SISTEMA PENALE

FASCICOLO

2/2024

ISSN 2704-8098

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale.
Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2023, p. 5 ss.

DECIFRARE, ACQUISIRE E UTILIZZARE LE COMUNICAZIONI CRIPTATE IN USO ALLA CRIMINALITÀ ORGANIZZATA: UNO SGUARDO EUROPEO, IN ATTESA DEL COUNT-DOWN ITALIANO (*)

di Simona Ragazzi e Filippo Spiezia

L'ingresso del digitale nella vita delle organizzazioni criminali ne ha cambiato i connotati, abilitandole, tra l'altro, al ricorso a sofisticate piattaforme telematiche criptate, in grado di preservare l'impenetrabilità delle comunicazioni.
Il fruttuoso sviluppo di tecnologie in grado di infiltrarne i server di appoggio, ad opera di alcuni Paesi della UE riuniti in più squadre investigative comuni, supportate da Europol, ha generato una copiosa mole di dati 'in chiaro', messi a disposizione di tutti i Paesi interessati, compresa l'Italia, tramite Eurojust. Ne è scaturito, tra l'altro, un sinergico lavoro del desk italiano di Eurojust di assistenza alle autorità giudiziarie italiane richiedenti tali dati con ordini europei di indagine. In molti Paesi europei ne è inevitabilmente derivato uno stimolante contenzioso giudiziario sulle 'giuste' forme di acquisizione dei dati e sui limiti di utilizzabilità di prove raccolte all'estero, dibattito approdato di recente anche alla Corte di Giustizia della EU.
In attesa dell'esito del ricorso pregiudiziale alla CGUE e a ridosso della decisione delle Sezioni Unite della Cassazione italiana su tali nodi critici, si propone una cronistoria del lavoro di disvelamento e condivisione tra Stati delle chat decriptate e una rassegna ragionata dei principali approdi giurisprudenziali a livello europeo, con lo sguardo rivolto alle possibili soluzioni interne e alle imminenti riforme sulle modalità di acquisizione della corrispondenza telematica.

1. Premessa.

La criminalità, specie organizzata, ha colto da tempo le opportunità offerte dalla evoluzione tecnologica, sia per utilizzare nuove modalità comunicative in ambito

(*) *Il presente lavoro costituisce il frutto di una riflessione congiunta dei due autori. Tuttavia, Filippo Spiezia ha redatto i paragrafi 1 e 2, mentre Simona Ragazzi i paragrafi 3, 4, 5 e 6; il paragrafo 7 sulle conclusioni costituisce frutto di redazione comune e condivisa; infine, anche le parti elaborate separatamente sono state oggetto di un comune lavoro di coordinamento*.

Editore Associazione "Progetto giustizia penale" | via Festa del Perdono 7, 20122 Milano
c/o Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria"
redazione@sistemapenale.it

criminale, sia commettendo reati sul web. Oggi i criminali hanno a "*portata di cloud*" un numero impressionante di informazioni ed hanno fatto ricorso al computer ed agli apparati di comunicazione digitale per commettere e sperimentare modalità inedite di consumazione delle attività illecite, anche "tradizionali", seppur lasciandone digitalmente traccia (si pensi alle forme di comunicazione anonima, su Dark Web o il ricorso a sistemi TOR ed a forme di comunicazioni criptate).

Il quadro complessivo ci restituisce il dato di organizzazioni criminali in continua evoluzione, grazie alla incredibile capacità di attingere al progresso tecnologico, esibendo un know how digitale che ha costituito l'indice evidente della loro trasformazione ed il fattore moltiplicatore del mutamento e del loro potenziamento operativo. *L'ingresso del digitale nella vita di organizzazioni e reti criminali ne ha cambiato i connotati*: esse esibiscono una straordinaria vitalità delle tecniche di elusione di ogni controllo collegata alla capacità, non solo del crimine organizzato mafioso, di dotarsi di tecnologie in grado di preservarne l'impenetrabilità: piattaforme criptate e ricorso al *dark web* per le ordinarie comunicazioni telematiche, sofisticati sistemi di sorveglianza elettronica delle aree di interesse, ossessiva cura della segretezza di movimenti e comunicazioni dei vertici dei gruppi criminali.

Si innesta, su tale avanzata capacità tecnologica, anche l'acquisita capacità senza precedenti di sviluppare dimensioni operative a rete (sinergie tra network criminali) e, dall'altro, economie di scala nella loro azione criminale, in grado di organizzare una suddivisione di compiti operativi nel quadro di un progressivo affinamento delle strategie criminali.

Queste ultime conoscono ormai il cambiamento del modello di business, che proietta le medesime in una dimensione affaristica su scala globale, privilegiando la dimensione imprenditoriale rispetto a quella di aperto e visibile contrasto armato e criminale, prevalendo l'esigenza dello sfruttamento delle enormi ricchezze illecite derivanti dai traffici di droga, con il coinvolgimento di esponenti di spicco in sofisiticare operazioni di ingegneria finanziaria, su scala nazionale, europea ed internazionale, ancora una volta con il ricorso allo strumento digitale.

Lo stesso dicasi per quanto riguarda la minaccia terroristica, dove l'uso del digitale è per certi versi ancora più marcato. L'utilizzo di siti web, di social networks o di forum e piattaforme online per lo scambio e diffusione di materiale propagandistico, di stampo terroristico, finalizzati al reclutamento, indottrinamento, finanziamento, promozione o incitamento ad atti terroristici e/o l'utilizzo di tecnologia informatica al fine di concretizzare attacchi verso sistemi informatici per scopi terroristici è attualmente uno degli strumenti più potenti in mano ai jihadisti, al pari di armi o esplosivi. Anche qui si può parlare di una modifica genetica**.**

2. Il disvelamento delle piattaforme di comunicazioni criptate e il supporto delle agenzie europee di cooperazione giudiziaria e di polizia.

Per comprendere la natura degli strumenti di cooperazione giudiziaria internazionale attraverso i quali si è dato ingresso ai materiali derivanti dalla

decriptazione dei flussi comunicativi in chat telefoniche criptate, è necessario risalire alle origini dei procedimenti penali esteri, nei quali l'attività investigativa è stata primariamente svolta e alle caratteristiche delle piattaforme di telecomunicazioni criptate che ne sono state oggetto.

Encrochat è il nome della società che vendeva il servizio di messaggistica criptata, denominato appunto Encrochat, utilizzato da numerose organizzazioni criminali in Europa e nel resto del mondo. Encrochat presentava il proprio servizio come inattaccabile e garantiva che le comunicazioni tra i suoi clienti non avrebbero potuto essere intercettate o violate in alcun modo. Il servizio e i relativi telefoni personalizzati erano emersi nell'ambito di indagini svolte nel 2017 da parte della Gendarmeria nazionale francese, la quale verificava che tale piattaforma operava da un server localizzato a Roubaix, Francia. Hotspots di utenti erano poi particolarmente diffusi nei Paesi di approvvigionamento e destinazione dei grandi mercati della cocaina e della cannabis, così come nei tipici siti di riciclaggio dei proventi.

Più in dettaglio, la piattaforma di telecomunicazioni EncroChat (analoghe caratteristiche presenterà anche Sky-Ecc, subentrata alla "scomparsa" della prima) proponeva agli utenti servizi di telecomunicazioni "sicuri", basati su criptofonini modificati nel software e nell'hardware, così da risultare insuscettibili di essere hackerati/intercettati da terzi.

Gli 'smartphone' EncroChat garantivano pieno anonimato e riservatezza dei contenuti comunicativi: nessuna correlazione tra un account del cliente e il dispositivo o una sim-card, non tracciabilità dell'acquisto (non possono essere acquistati presso punti vendita autorizzati, ma solo da speciali rivenditori e attraverso canali anonimi, all'elevato prezzo di circa 1.600 euro da pagarsi in contanti o in criptovalute), sistema operativo duale con una interfaccia criptata, rimozione di telecamera, microfono, GPS, porta usb; autodistruzione dei messaggi scambiati tra gli utenti mediante uno speciale codice pin o scrivendo più volte consecutivamente una password errata (con conseguente cancellazione immediata di tutti i dati della memoria) e, infine, centri assistenza da remoto o rivenditori in grado di cancellare tutti i dati del dispositivo, ove necessario. Profili di opacità avvolgevano la società apparentemente titolare della app, gli amministratori e la sede legale.

Solo nella prima metà del 2020 le forze dell'ordine sono riuscite a ottenere l'accesso ai messaggi scambiati tramite detto servizio. Gli inquirenti francesi sviluppavano un software del tipo *trojan horse*, che veniva caricato nel server di Roubaix in Francia nei primi mesi del 2020 e da lì installato nei dispositivi mobili degli utenti attraverso un simulato aggiornamento di sistema. La Gendarmeria costituiva una task force, la quale, sotto la supervisione della magistratura e dietro autorizzazioni del giudice istruttore di Lille, monitorava le comunicazioni di migliaia di sospetti criminali, portando all'apertura di un elevato numero di ulteriori sotto-procedimenti.

In precedenza, nel 2019, il Desk francese di Eurojust, su richiesta delle proprie autorità giudiziarie nazionali, aveva aperto un caso verso i Paesi Bassi a supporto dell'attività investigativa svolta con riguardo a organizzazioni criminali internazionali sospettate di utilizzare detta modalità di comunicazione per pianificare le proprie azioni. I dati acquisiti nel corso delle indagini dagli investigatori francesi sono stati condivisi

nell'immediato con i Paesi Bassi e nella primavera del 2020 Eurojust ha facilitato la creazione di una squadra investigativa comune (SIC) tra i due Stati, supportata da Europol.

Nei Paesi Bassi, l'indagine penale è stata condotta dalla Procura nazionale olandese e le informazioni ottenute sono confluite in numerose indagini penali.

Attraverso la squadra investigativa comune sono stati intercettati e identificati location, traffico e comunicazioni, inclusi i testi e le immagini, trasmessi all'interno di chat ad uso degli utenti della piattaforma[1].

All'esito dei primi mesi di investigazioni le autorità francesi verificavano che circa il 63,7% dei criptofonini attivi in Francia erano utilizzati per scopi criminali, mentre per il restante 36,3% sono parzialmente inattivi o non ancora scrutinati, concludendone che di fatto i telefonini Enchochat (ma analoghe verifiche valgono per la successiva piattaforma Sky-ecc) erano appannaggio di una clientela pressoché esclusivamente criminale.

Eurojust ha facilitato in modo decisivo la cooperazione giudiziaria, supportando la squadra investigativa comune, le richieste di cooperazione giudiziaria, la realizzazione di riunioni di coordinamento, la soluzione di problematiche investigative pratiche e tecnico-giuridiche riguardanti, ad esempio, la pendenza di procedimenti penali paralleli e questioni di giurisdizione.

È stato, così, possibile ricostruire in sede investigativa numerose e pericolose attività criminali di carattere nazionale e transnazionale e pervenire all'arresto di decine di indagati anche in Stati non partecipanti alla squadra investigativa comune. Molte di queste indagini hanno riguardato il traffico internazionale di droga e delitti commessi con l'uso di violenza.

Al luglio del 2020, in particolare, l'indagine ha condotto all'arresto di 60 sospettati, al sequestro di stupefacente (più di 10.000 kg. di cocaina, 70 kg di eroina, 12.000 kg di cannabis, 1.500 kg di droghe sintetiche e 160.000 litri di sostanze usate per la produzione di droghe sintetiche), allo smantellamento di 19 laboratori di droghe sintetiche, oltre che al sequestro di decine di armi da fuoco (automatiche), 25 automobili e circa 20 milioni di euro in contanti.

L'intercettazione dei messaggi di Encrochat si è conclusa il 13 giugno 2020, quando la società si è resa conto che gli investigatori erano riusciti a penetrare nella piattaforma. In quel momento Encrochat ha inviato un avviso a tutti i suoi utenti consigliando loro di disfarsi immediatamente dei telefoni.

Nel marzo 2021 con comunicato congiunto Europol - Eurojust veniva annunciato lo sblocco della crittografia e dunque il riuscito monitoraggio dell'ulteriore strumento di comunicazioni criptate Sky ECC[2], ad opera di una distinta squadra investigativa comune

---

[1] Comunicato congiunto delle due Agenzie in: https://www.eurojust.europa.eu/news/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

[2] https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

La nuova piattaforma di messaggistica elettronica era protetta da un programma di crittografia asimmetrica, denominato "Sky ECC", in quanto fondato sull'impiego della curva ellittica, che è un particolare tipo di

tra Belgio, Francia e Paesi Bassi, supportata dalle due agenzie europee. Le autorità giungevano a monitorare il flusso di informazioni di circa 70.000 utenti, rilevando, tra l'altro, che molti utenti di EncroChat, dopo la rivelazione della avvenuta decriptazione, erano passati alla nuova piattaforma.

Nel caso di Sky Ecc la società distributrice – la canadese "Sky Global" – aveva installato sofisticati software di crittografia su apparecchi nativi iPhone, Google Pixel, Blackberry e Nokia, permettendo anche in tal caso la comunicazione tra utenti su reti riservate, che si appoggiavano a server crittografati localizzati in Canada e Francia.

3. L'impegno di Eurojust e del Desk italiano nell'assistenza ai procedimenti penali interni.

Le due Squadre Investigative Comuni hanno reso possibile intercettare, condividere e analizzare milioni di messaggi scambiati fra membri di organizzazioni criminali, permettendo alle autorità di polizia e giudiziarie anche italiane, a seguito della esecuzione degli ordini di indagine europei inviati alla competente autorità giudiziaria francese, di arricchire il proprio patrimonio informativo e indagare in modo efficace le più diverse fattispecie criminose.

La straordinaria novità dell'operazione investigativo–giudiziaria in esame è scaturita proprio dal fatto che attraverso la diretta (e tecnicamente necessitata) intercettazione di *server* centrali, autorizzata secondo il diritto francese, è approdata al contestuale disvelamento di una mole copiosissima di dati comunicativi, afferenti a decine di migliaia di utenti, molti dei quali divenuti oggetto di specifico interesse investigativo in autonomi procedimenti penali intrapresi da Paesi 'terzi'.

Attraverso una videoconferenza del marzo 2020 Eurojust forniva informazioni ai Paesi UE riguardanti le misure di intercettazione su EncroChat in corso in Francia e la volontà delle Autorità francesi di mettere a disposizione e trasferire tali dati ai Paesi interessati. In altri termini, poiché questi dati non riguardavano solo le reti criminali localizzate in Francia o nei Paesi Bassi, le autorità francesi manifestavano la volontà di condividerli da allora con tutti i Paesi che ne avrebbero fatto formale richiesta.

Analogamente avveniva un anno dopo a seguito del disvelamento della piattaforma Sky ECC.

I dati comunicativi acquisiti sono stati dunque trasmessi nel quadro della JIT Francia - Paesi Bassi (e di quella successiva tra Francia – Paesi Bassi e Belgio) e sulla base di Ordini Europei di Indagine e Rogatorie emesse dai Paesi interessati. Le autorità francesi hanno ottenuto altresì l'assistenza di Eurojust nel monitorare le decisioni nazionali pertinenti e fornire un'analisi giuridica.

Per quanto concerne il nostro Paese, si è avviato un modulo operativo in virtù del quale il Desk italiano di Eurojust dal 2020 a oggi ha veicolato al corrispondente Desk francese ogni ordine di indagine europeo emesso dal pubblico ministero interessato e

---

crittografia, identificata dall'acronimo ECC: *Elliptic Curve Cryptography*.

finalizzato ad ottenere dall'autorità giudiziaria francese (tribunale di Lille o di Parigi, secondo il caso), l'autorizzazione ad acquisire e rendere utilizzabili processualmente i dati di proprio interesse nel procedimento penale italiano. L'autorizzazione e i dati così ottenuti sono stati poi trasmessi dal Desk italiano all'autorità giudiziaria italiana in forma di supporto digitale. Tale rilevante segmento del lavoro del Desk è sfociato nella apertura e proficua gestione di 373 casi Sky ECC e 150 casi Encrochat (corrispondenti, per lo più, ad altrettanti procedimenti penali interni).

Parallelamente, il Desk italiano ha partecipato a un lavoro collettaneo di Eurojust di continuo monitoraggio, raccolta e analisi dei ricorsi, degli argomenti presentati dalle difese o dai procuratori e delle decisioni prese da varie corti nazionali sul tema, e ha fornito e continua a fornire alle autorità giudiziarie italiane, tramite apposite note del Membro Nazionale, linee guida per l'acquisizione giudiziaria dei dati, report esplicativi integrativi (quali quelli, frutto di interlocuzione diretta con il Desk francese, contenenti i provvedimenti autorizzatori francesi, la dettagliata esposizione delle tecniche di intercettazioni adottata, la specificazione della natura dei dati trasmessi alla AG italiana, costituenti solo chat e non anche flussi comunicativi *attivi*, etc.), rassegne della giurisprudenza della CGUE e della Corte europea dei diritti dell'uomo relative all'ammissibilità delle prove e all'acquisizione di dati su larga scala e decisioni note delle corti nazionali.

4. Cenni sulle pronunce di altre corti superiori europee.

La graduale acquisizione con OIE verso la Francia e l'utilizzazione processuale dei dati ricavati dalla infiltrazione delle piattaforme EncroChat e Sky-Ecc in vari Paesi europei (in Italia riguardo, allo stato, con riferimento alla adozione di ordinanze applicative di misure cautelari personali) ha generato un'inevitabile contenzioso dinanzi alle corti nazionali.

In via generale, le corti finora adite hanno avallato l'utilizzo processuale dei dati acquisiti tramite ordini di indagini europei emessi da organi inquirenti nazionali verso la Francia, evidenziando la non sindacabilità del meccanismo di acquisizione della prova all'estero, ed escludendo che raccolta dei dati operata in tali casi sia assimilabile a una forma di "sorveglianza di massa" e che dunque possa ricadere nell'ambito applicativo della direttiva europea su e-privacy e service providers, e ciò anche in ragione delle caratteristiche operative delle piattaforme comunicative in esame e della loro strutturale funzionalità agli interessi della criminalità organizzata.

Si accennerà ad alcune delle decisioni più interessanti, senza pretesa di completezza. Non può che muoversi dalle pronunce delle corti superiori francesi. È essenziale premettere che il codice di procedura penale francese, all'art. 706-102-1 e ss., nel permettere il ricorso al captatore informatico per delitti di particolare gravità, tra cui quelli di criminalità organizzata, assoggetta le relative operazioni tecniche, ove

compiute con risorse dello Stato, al segreto di difesa nazionale[3]. Il provvedimento che autorizza l'uso del dispositivo tecnico, a pena di nullità, deve specificare il reato che motiva l'uso di tali operazioni, l'esatta ubicazione o la descrizione dettagliata dei sistemi automatizzati di trattamento dei dati, la durata delle operazioni (art. 706-102-3 c.p.p.). I dati raccolti nell'ambito delle indagini giudiziarie (intercettazioni di conversazioni, dati di connessione, geolocalizzazione, ecc.) sono poi centralizzati ed elaborati dall'Agenzia nazionale per le tecniche di indagine giudiziaria digitale (*Agence nationale des techniques d'enquêtes numériques judiciaires, Antenj*)[4].

Allo stesso modo sono soggette al segreto di difesa nazionale le operazioni di 'decriptazione' di dati informatici, ai sensi dell'art. 230-1 e ss. del c.p.p. Tale diversa fattispecie prevede che, salvo il segreto di difesa nazionale, i risultati delle attività di decriptazione siano accompagnati da informazioni tecniche utili alla comprensione e all'utilizzo dei risultati, unitamente a un certificato firmato dal responsabile dell'organismo tecnico che attesti la genuinità dei risultati trasmessi.

Il Consiglio costituzionale francese, adito dalla Corte di Cassazione (dinanzi alla quale era stata impugnata la decisione della Corte d'appello di Nantes che aveva rigettato le eccezioni difensive di mancato rispetto delle garanzie di cui all'art. 230-3 c.p.p. e comunque che aveva contestato la opposizione del segreto di difesa nazionale), con decisione dell'8.4.2022 statuiva che le previsioni del codice di procedura penale che consentono agli investigatori di porre il segreto di difesa nazionale[5] in relazione a determinate informazioni afferenti a speciali tecniche investigative, come quelle comportanti la infiltrazione di dispositivi elettronici e la decriptazione di dati informatici (artt. 230-1, 230-2, 230-3, e poi 706-102-1 c.p.p.) non vìolano i diritti degli accusati ad un rimedio giudiziario effettivo, né il diritto alla riservatezza, la libertà di espressione o qualsiasi altro diritto sancito dalla costituzione. Rientra, infatti, nei poteri del legislatore assicurare il bilanciamento tra i diritti di difesa e il principio del contraddittorio, da una parte, e le esigenze, di pari rango costituzionale, di accertamento dei reati e di salvaguardia degli interessi fondamentali della nazione, tra i quali rientra

---

[3] Articolo 706-102-1 (Traduzione non ufficiale, ricavata dal Dossier cit. in nota 7): «*Quando l'esigenza investigativa concernente un reato rientrante nel campo di applicazione dell'articolo 706-73 lo imponga, il giudice istruttore, previo parere del procuratore della Repubblica, può autorizzare con ordinanza motivata gli ufficiali e gli agenti di polizia giudiziaria incaricati del caso di mettere in atto un dispositivo tecnico avente per scopo, senza il consenso degli interessati, quello di accedere ovunque, ai dati informatici, registrarli, conservarli e trasmetterli, tal quali sono memorizzati in un sistema informatico, tal quali sono visualizzati su uno schermo per l'utente di un sistema di elaborazione dati automatizzato, tal quali sono inseriti da quest'ultimo mediante la digitazione di caratteri o così come sono ricevuti e trasmessi da periferiche.*

Il procuratore della Repubblica o il giudice istruttore possono nominare ogni persona fisica o giuridica abilitata e iscritta in una delle liste di cui all'articolo 157 per effettuare le operazioni tecniche che permettono la realizzazione del dispositivo menzionato nella prima linea del presente articolo. Il procuratore della Repubblica o il giudice istruttore possono altresì disporre l'impiego di risorse dello Stato sottoposte al segreto della difesa nazionale, secondo le forme previste al capitolo primo del titolo quarto del libro primo».

[4] Utili indicazioni si trovano nel Dossier del Senato della Repubblica: "Intercettazioni: profili di diritto comparato, aprile 2023, in: https://www.senato.it/service/PDF/PDFServer/BGT/01374063.pdf

[5] Sul segreto della difesa nazionale del diritto francese:
https://www.cortecostituzionale.it/documenti/convegni_seminari/CC_SS_SegretoStato_28032012.pdf

il segreto di difesa nazionale, dall'altra. Il Consiglio proseguiva ricordando che, è vero che le speciali tecniche di investigazione applicabili alla criminalità organizzata, tra i quali la captazione di dati informatici, sono sottoposti al segreto di difesa nazionale, ma si può ricorrere a tali strumenti solo previa autorizzazione del giudice della libertà e della detenzione o del giudice istruttore e solo se giustificati dalla necessità di una indagine relativa a crimini di particolare gravità e complessità; inoltre, restano versati al fascicolo del procedimento l'ordinanza motivata del giudice che ha autorizzato il dispositivo captatore contenente, a pena di nullità, un insieme di informazioni basilari, e ancora il processo verbale di intrapreso servizio e il processo verbale contenente l'insieme dei dati recepiti, accompagnato da un'attestazione della genuinità dei risultati trasmessi.

I successivi approdi della Corte di Cassazione francese (decisione del 10.5.2023 e decisione del 5.9.2023, quest'ultima nell'ambito del caso pilota approdato alla Corte d'Appello di Metz, che aveva deciso il 12.1.2023, su rinvio della Cassazione a seguito del Consiglio costituzionale) hanno poi operato un ulteriore distinguo, precisando che gli artt. 230-1 e ss. (che imporrebbero gli adempimenti supplementari del certificato attestante la veridicità dei dati e della specificazione dei dettagli tecnici delle operazioni di acquisizione dei dati) non vengono in rilievo rispetto all'acquisizione, a valle, dei dati EncroChat ad opera della polizia giudiziaria, poiché essa ha riguardato dati ormai in chiaro e non più criptati[6].

La Corte di giustizia federale tedesca (*Bundesgerichtshof)* con decisione del 2 marzo 2022, ha ritenuto valida l'utilizzazione delle chat acquisite dalle AG tedesche tramite OIE verso la Francia[7].

Essa ha, in sintesi, stabilito che: a) l'atto di indagine originario adottato dall'autorità giudiziaria francese non possa essere valutato secondo i parametri del diritto tedesco; pertanto non è dirimente stabilire se una certa misura investigativa adottata in Francia avrebbe potuto essere ordinata in Germania; il riesame del diritto straniero non è un prerequisito per il trasferimento di prove ottenute dall'autorità giudiziaria francese in base al diritto francese nei procedimenti penali in Germania; i differenti prerequisiti per adottare una misura tra Francia e Germania possono trovare il loro bilanciamento in base all'articolo 261 del codice di procedura penale tedesco (che definisce il principio del libero convincimento del giudice nella valutazione della prova); 2) non c'è violazione di diritti umani fondamentali o di principi fondamentali del diritto europeo o di quello dell'ordine pubblico, in quanto gli investigatori in Francia non hanno attuato una forma di 'sorveglianza di massa' di un largo numero di utenti di telefonia

[6] In altri termini, le relative operazioni si fondano sulla infiltrazione di dispositivi mediante captatore informatico sulla scorta dell'art. 706-102-1 del codice di procedura penale; non viene, perciò, in rilievo una attività di 'decriptazione' quale quella prevista dall'art. 230-1 e 230-2 (i dati sono stati acquisiti dalla PG in "forma non crittografata"), e dunque non vi è, a carico degli inquirenti, alcun onere di certificare la validità di quei dati né di fornire i dettagli tecnici delle operazioni compiute ai sensi dell'art. 230-3. Allo stesso modo la decisione della Corte di Metz, di cui tuttavia si conoscono soltanto lanci di stampa e non il testo, ha ritenuto che la sezione del codice di procedura penale francese che richiede la certificazione non si applichi alla operazione EncroChat.

[7] https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/EN/2022/2022038.html

mobile; piuttosto EncroChat si è rivelato un network appositamente studiato quale supporto ad attività criminali, ha operato in segreto e, stando ai primi risultati dell'investigazione, i suoi dispositivi sono stati appannaggio esclusivo di gruppi criminali organizzati, coinvolti in particolare nel traffico di stupefacenti, armi e nel riciclaggio, essi non erano disponibili nella normale rete di distribuzione e comportavano costi elevati; 3) non è vietata l'acquisizione preventiva degli elementi investigativi in parola attraverso un trasferimento di *intelligence* nel procedimento penale prima dell'adozione dell'ordine europeo di indagine, e ciò in virtù del consolidato principio che legittima la trasmissione spontanea di informazioni di polizia tra Stati.

Il Tribunale del Land di Berlino (Landgericht Berlin) con decisione del 19/10/2022 ha, tuttavia, poi attivato un rinvio pregiudiziale alla Corte di giustizia dell'unione europea, sotto il profilo della invocata interpretazione conforme della direttiva 2014/41 sull'ordine di indagine europeo.

Di notevole rilievo è la decisione adottata dal Corte Suprema *(Hoge Raad*) dei Paesi Bassi in data 13.6.2023 su domanda pregiudiziale della Corte distrettuale dei Paesi Bassi Settentrionali.

La decisione contiene innanzitutto un'accurata ricostruzione di tutti i passaggi dei procedimenti penali olandesi nei quali, nel contesto della di una squadra investigativa comune con la Francia nel caso EncroChat e con Francia e Belgio nel caso Sky ECC, sono state effettuate le operazioni di infiltrazione e intercettazione dei server delle due piattaforme[8]. Per tale ragione la situazione olandese è peculiare, poiché le autorità giudiziarie olandesi sono state investite fin dall'inizio delle indagini da attività investigative dirette, che sono sfociate anche in provvedimenti autorizzatori del giudice istruttore competente.

Nel caso Encrochat prima dell'installazione del dispositivo di intercettazione sul server di Roubaix da parte delle autorità francesi e con l'autorizzazione del giudice francese, il pubblico ministero (olandese) ha chiesto e ottenuto dal proprio giudice istruttore l'autorizzazione a emettere un ordine per penetrare e indagare su un lavoro automatizzato e registrare le (tele)comunicazioni; le informazioni così ottenute dalle autorità francesi sono state successivamente condivise (in diretta) con le autorità olandesi in base all'accordo concluso in relazione alla creazione della squadra investigativa comune.

Quanto all'indagine sugli utenti di SkyECC, prima che le autorità francesi collegassero e attivassero la tecnologia sviluppata nei Paesi Bassi che consentiva di decriptare il traffico di messaggi, la procura (olandese) ha richiesto un mandato al giudice istruttore per emettere un ordine di registrazione delle telecomunicazioni. Sono state inoltre richieste autorizzazioni per l'emissione di un ordine di penetrazione e perquisizione di un'opera automatizzata.

La Hoge Raad olandese, muovendo dai ricorsi proposti, ha tuttavia sviluppato conclusioni articolate e più generali, di seguito sintetizzate, che tengono conto di tutte le

[8]Per la lettura integrale della sentenza in inglese:
https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:HR:2023:913

possibili opzioni, anche relative all'ipotesi in cui, analogamente al caso italiano, i Paesi Bassi non facessero parte delle investigazioni in cui i risultati sono stati raccolti (par. 6.21 – 6.28):

a) se l'esecuzione di una misura investigativa all'estero avviene sotto la responsabilità di un'autorità straniera, i requisiti previsti dal diritto processuale penale olandese per l'applicazione del relativo potere in un'indagine nazionale sui reati devono essere soddisfatti solo se l'applicazione del potere investigativo avviene su iniziativa delle autorità olandesi. Ciò significa: su richiesta dei Paesi Bassi – in relazione o meno alle azioni di una squadra investigativa comune – o sulla base di un OIE emesso dai Paesi Bassi. Se in base al codice processuale penale olandese è richiesta l'autorizzazione del giudice istruttore, tale autorizzazione deve essere ottenuta prima che all'autorità straniera venga richiesto di esercitare un potere investigativo o che venga emesso un OEI in vista dell'esecuzione di un atto investigativo;
b) il requisito dell'autorizzazione del giudice istruttore non si applica nel caso in cui l'indagine in questione si svolga o si sia già svolta su iniziativa delle autorità straniere, dopo di che queste ultime – su richiesta o meno delle autorità olandesi o dopo che le autorità olandesi hanno emesso un OIE a tal fine – rendono disponibili i risultati dell'indagine. La legge non richiede il rilascio di un'autorizzazione da parte del giudice istruttore per l'utilizzo esclusivo in un procedimento penale nei Paesi Bassi dei risultati di una ricerca svolta o già svolta su iniziativa e sotto la responsabilità dell'autorità straniera.
c) le decisioni dell'autorità giudiziaria straniera su cui si basano le misure investigative di raccolta dei dati vanno rispettate e non possono essere sindacate, salvo che siano state ritenute illegali nell'ambito del procedimento penale in cui originano;
d) il giudice dello Stato che acquisisce tali atti deve partire dall'assunto che la raccolta di tali dati sia avvenuta in maniera affidabile nello Stato richiesto, mentre è tenuto a esercitare un vaglio di affidabilità solo quando, a prescindere dai rilievi delle parti, emergano concrete indicazioni di inaffidabilità;
e) il giudice dovrà solo "prestare attenzione" alle modalità con cui i risultati delle indagini condotte all'estero sono stati conseguiti, laddove tali modalità siano rilevanti per la valutazione della prova ai fini del rispetto delle garanzie del giusto processo (e – precisa dopo – sempre con i limiti della valutazione di prove raccolte sotto l'egida di AG straniera);
f) allo stato della legislazione olandese non è richiesta un'autorizzazione giudiziaria preventiva per raccolta di dati acquisiti in un autonomo procedimento penale straniero salva l'ipotesi in cui le intercettazioni si svolgano nei confronti di bersagli allocati sul territorio olandese e pur sempre nei limiti di cui all'articolo 31 della direttiva OIE ovvero nei termini del codice di procedura penale olandese in caso di rapporti con Stati che non riconoscono l'OIE;
g) il pubblico ministero è, tuttavia, libero di chiedere al giudice un'autorizzazione, ancorché non prevista e non imposta dal codice, tenuto conto delle peculiari circostanze del caso; ciò, per esempio, lì dove in un contesto di investigazioni

transfrontaliere si ricorra a tecnologie non conosciute all'ordinamento olandese; così, nel contesto della raccolta su larga scala di dati relativi alle cripto-comunicazioni, i motivi per richiedere tale autorizzazione potrebbero scaturire dal fatto che: (1) le autorità straniere hanno già proceduto o procederanno di propria iniziativa a raccogliere i dati sotto la loro responsabilità; (2) sono state ottenute o saranno ottenute grandi quantità di dati che, da un lato, possono essere di grande valore non solo per l'indagine in cui viene richiesta l'autorizzazione, ma anche in vista di altre (future) indagini penali e, d'altra parte, i dati possono includere persone che, al momento della loro acquisizione, non sono (ancora) identificate come sospette dalle autorità investigative; (3) è stato concordato che i dati così ottenuti saranno ampiamente condivisi con le autorità olandesi in vista del trattamento di tali dati per l'indagine in corso e per eventuali altre indagini.

h) Infine, citando la sentenza della CGUE - Grande Sezione, 6 ottobre 2020, *La Quadrature du Net*, C. 511-18, quando gli Stati membri attuano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche (via intercettazioni, etc.), senza imporre obblighi di trattamento ai fornitori dei relativi servizi di comunicazione (c.d. service providers), la protezione dei dati delle persone interessate non ricade nell'ambito della direttiva 2002/58/UE sul trattamento dei dati personali nel settore delle comunicazioni elettroniche, bensì unicamente in quello del diritto nazionale, fatta salva l'applicazione della diversa direttiva (UE) 2016/680, relativa alla protezione delle persone fisiche nel trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento di reati o esecuzione di sanzioni penali, e i requisiti della CEDU (par. 102). Nel presente caso l'autorità giudiziaria francese non ha dovuto rivolgersi a EncroChat e SkyECC per ottenere dati personali dei rispettivi utenti, poiché le captazioni sono state autonomamente effettuate dagli investigatori. Inoltre, i gestori delle piattaforme hanno offerto un servizio di messaggistica criptata nel quale gli utenti non dovevano rivelare la loro identità e dunque conferire i loro dati personali e dove le comunicazioni si svolgevano solo tra utenti del medesimo servizio per cui non vengono in rilievo le previsioni normative sugli obblighi di conservazione dei dati personali gravanti sui fornitori di *pubblici* servizi di comunicazione elettronica[9].

[9] Un altro caso è stato sollevato da alcune corti della Gran Bretagna e pende dinanzi alla Corte europea dei diritti dell'uomo (C. 44715/20: il 3 gennaio 2022 la Corte europea ha chiesto alle parti, tra l'altro, se hanno contestato le intercettazioni davanti alle competenti corti francesi).
Di seguito un richiamo alla decisione della Corte suprema norvegese:
https://www.domstol.no/en/supremecourt/rulings/rulings-2022/supreme-court-criminal-cases/HR-2022-1314-A/

5. Il dibattito nella giurisprudenza italiana.

La Corte di Cassazione tra il 2022 e il 2023 ha reso numerose pronunce sulla utilizzabilità dei dati estrapolati dalle piattaforme EncroChat e Sky-ecc via OIE dalla Francia, tutte derivanti da procedimenti cautelari.

Le pronunce precedenti alle sentenze n. 44154 e 44155 del 26.10.2023, che hanno segnato un momento di discontinuità, avevano univocamente ritenuto che la messaggistica scambiata con i sistemi Sky Ecc ed EncroChat, acquisita mediante ordine europeo di indagine da autorità giudiziaria straniera che ne aveva eseguito la decriptazione, costituisse dato informativo documentale conservato all'estero, utilizzabile ai sensi dell'art. 234-*bis* cod. proc. pen., e non flusso comunicativo, non trovando applicazione la disciplina delle intercettazioni di cui agli artt. 266 e 266-bis cod. proc. pen. (*ex multis*, Sez. I, n. 6363 e 6364 del 13/10/2022 Cc. -dep. 15/2/2023; Sez. IV, n. 16347 del 05/04/2023, Papalia).

In tali pronunce (per tutte, Sez. IV, n. 18514, cc. 04.04.2023, dep. 4.5.2023, Puzella), è stata superata l'eccezione di inutilizzabilità del materiale acquisito tramite l'autorità giudiziaria francese per dedotta lesione del diritto di difesa per non essere stati messi a disposizione i provvedimenti della autorità giudiziaria francese né ivi spiegate le modalità di raccolta, rilevando che: a) si trattava di dati autonomamente acquisiti dalla autorità giudiziaria francese nell'ambito di procedimenti penali ivi aperti; b) trattandosi di informazioni che la legislazione di quello Stato consente di tenere segrete, la autorità giudiziaria francese non ha trasmesso la documentazione relativa alle modalità di acquisizione dei dati; c) i diritti della difesa devono necessariamente modularsi sulla legge dello Stato che ha eseguito l'OIE, per cui, poiché, nel caso di specie, quello Stato può legittimamente opporre il segreto sul punto, la legittimità delle modalità di acquisizione e decrittazione dei dati deve ritenersi garantita dal controllo che su quella attività è stato compiuto dall'autorità giudiziaria francese; d) si è comunque attestata – con processo verbale redatto e sottoscritto dall'ufficiale di polizia giudiziaria francese incaricato dell'adempimento – la regolarità del trasferimento di quei dati su supporto informatico non modificabile e l'acquisizione è avvenuta con regolari O.I.E. messi a disposizione delle parti […].

Le sentenze della Sez. VI, n. 44154/23 e 44155/23 del 26/10/2023 (di annullamento con rinvio di corrispondenti decisioni del tribunale del riesame di Milano e Reggio Calabria) hanno invece escluso l'operatività dell'art. 234-bis c.p.p., ritenendola giustificata solo per l'acquisizione di documenti e dati informatici "dematerializzati", cioè preesistenti all'avvio delle indagini da parte dell'autorità giudiziaria francese ovvero che erano stati formati al di fuori di quelle investigazioni: nei casi in esame, di contro, gli elementi sono stati raccolti attraverso le indagini della autorità straniera e in forma di apprensione occulta del contenuto archiviato in un server. Tale attività acquisitiva, pertanto, andrebbe inquadrata nelle disposizioni su perquisizione e sequestri, in specie nell'art. 254-*bis* c.p.p., riguardante il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni. Quindi, in linea con gli interventi sulla acquisizione dei dati "esterni" al traffico telefonico o telematico (nuovo art. 132 d.lgs. 196/2003, alla luce della sentenza CGUE 2.3.2021 C -746/18), le due

pronunce hanno concluso che: a) l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione, quali quelle in esame, debba essere sempre autorizzata da un giudice; b) sebbene attraverso gli OIE in esame si acquisisca una prova precostituita – nella specie esiti di intercettazioni – il mero richiamo all'articolo 270 c.p.p. non esaurisce la verifica della sussistenza delle condizioni di ammissibilità della prova che la direttiva OIE riserva allo Stato di emissione: la natura del mezzo di prova (intercettazioni) attivato nel Paese richiesto impone pertanto che il giudice italiano (il GIP e, in mancanza, il riesame) verifichi, ai fini della utilizzabilità dei materiali informativi acquisiti, se sussistevano le condizioni per la autorizzabilità in sede giurisdizionale delle relative attività investigative oggetto dell'OIE.

Una successiva sentenza (Sez. VI, n. 46482 del 27/9/2023, dep. 17/11/2023, e simile la n. 46833 del 26/10/2023, dep. 21/11/2023) ha adottato un indirizzo ulteriormente diverso, recependo, dalle due ultime decisioni sopra richiamate, la qualificazione dei dati raccolti all'estero come corrispondenza telematica, ma traendone conclusioni diverse in termine di necessità o meno di autorizzazione preventiva del giudice e su altri profili. La Corte muove dalla sentenza della Corte costituzionale n. 170/2023, secondo cui anche la messaggistica – informatica o cartacea – conservata dopo la consegna non ha natura di generico documento, bensì mantiene il suo carattere di "corrispondenza", dovendosi ritenere permanere l'interesse alla riservatezza *«almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento storico»*. Osserva dunque che la messaggistica sulle chat criptate in esame, costituendo del pari registrazione di conversazioni già avvenute e, quindi, di dati "statici", è assimilabile alla corrispondenza, la quale [giova qui aggiungere, allo stato della legislazione] non necessita di un provvedimento del giudice, potendo essere acquisita con decreto motivato di sequestro probatorio disposto dal pubblico ministero.

La Corte puntualizza che non può invece invocarsi l'art. 234-*bis* c.p.p. sui "documenti informatici"; vero è che tanto la corrispondenza quanto i documenti informatici rientrano nel fuoco dei documenti (art. 234 c.p.p.), ma l'art. 234-*bis* cod. proc. pen., introdotto con la normativa antiterrorismo legata al fenomeno dei *foreign fighters*, e costituente trasposizione nell'ordinamento dell'art. 32 della Convenzione sul cybercrime, ratificata con la legge n. 48 del 2008, come prevede testualmente *(«è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico»)*, fa riferimento a una specifica e diversa gamma di documenti, appunto, che intende rendere acquisibili al di fuori di qualsiasi formalità: ovvero, qualsiasi materiale disponibile in rete, con il limite che, quando si tratti di documentazione non liberamente accessibile al pubblico (per accesso protetto), il "legittimo titolare" autorizzi l'uso.

Conclude la Corte che l'OIE con cui venga richiesto il trasferimento di intercettazioni di conversazioni già disposte dal giudice straniero può, dunque, essere emesso dal pubblico ministero, poiché gli atti *di indagine richiesti nell'O.E.I. avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo"*, segnatamente nella forma del sequestro probatorio di documentazione/corrispondenza con provvedimento del pubblico ministero.

Ciò non dovrebbe significare che l'OIE in questione debba essere preceduto da un decreto di sequestro probatorio del pubblico ministero e finalizzato alla sua esecuzione, con tutte le conseguenze che ne derivano, in quanto si verte in materia di trasferimento di prove fra diversi procedimenti penali, trasferimento (di documenti e corrispondenza già acquisita in un procedimento straniero) che non deve soffrire di limiti superiori rispetto a quelli dell'acquisizione diretta che opererebbe tra procedimenti penali interni e che quindi si può effettuare con un semplice provvedimento del pubblico ministero. Significativamente, infine, la Corte sottolinea che anche ove si trattasse di trasferimento di contenuti di intercettazioni tra procedimenti penali, le quali nell'ordinamento interno circolano sulla base di un mero provvedimento del pubblico ministero, non sarebbe richiesta una distinta e autonoma autorizzazione del GIP, salvi i limiti dell'art. 270 c.p.p.

È, in definitiva, ultronea una verifica giudiziale di utilizzabilità da parte del giudice nazionale, perché non prevista dall'art. 270 cod. proc. pen. neppure per il trasferimento di intercettazioni nei procedimenti interni. Infine, l'indisponibilità della tecnologia di "hackeraggio" utilizzata per estrarre e mettere in chiaro la messaggistica criptata non determina lesione dei diritti di difesa, poiché l'ordinamento interno non obbliga alla ostensione degli attrezzi virtuali con cui si sia ottenuta la decodifica di contenuti telematici, salva la possibilità per l'imputato di allegare anomalie tecniche che facciano fondatamente dubitare della correttezza delle acquisizioni, e che depongano per l'inquinamento del risultato.

La sentenza n. 46390 del 26/10/2023, dep. 16/11/2023, sulla allegata inaccessibilità della difesa ai meccanismi usati dalle forze di polizia per la decodifica digitale delle piattaforme, ha poi precisato che neanche il diritto interno garantisce alla difesa l'accesso agli algoritmi per la decodifica dei dati criptati, ma si limita a dettare garanzie procedurali a protezione della cd. "catena di custodia" nell'ottica dell'integrità probatoria, quali la necessità di un atto autorizzativo da parte di attori giudiziari qualificati, l'individuazione dei soggetti che possono acquisire e ritenere i dati e la disciplina della conservazione e consultazione degli stessi.

Dinanzi ad interpretazioni in tutto o in parte difformi su molteplici profili di rilievo, quali appena ripercorse, la Sezione III con decisione del 3/11/2023 ha a sua volta rimesso alle Sezioni Unite la duplice questione: se i flussi comunicativi acquisiti abbiano natura di documento informatico *ex* art 234-*bis* c.p.p. e se debbano essere preceduti da una verifica preventiva o successiva dell'autorità giudiziaria.

Infine, con ordinanza n. 2329/24 della Sez. VI, 15.1.2024, dep. 18.1.2024, la Corte di Cassazione ha rimesso alle Sezioni Unite una duplice ulteriore questione, vertente su seguenti punti: a) quale sia lo strumento processuale "interno" da porre a parametro per l'importazione delle *"chat"* decrittate e richieste con gli OEI, tra la normativa in tema di sequestro di corrispondenza informatica (art. 254-bis c.p.p. o quella in tema di intercettazioni da altro procedimento ex art. 270 c.p.p.; b) se e quale sia l'ambito del controllo giurisdizionale (e se preventivo o successivo) da svolgere nell'ordinamento interno sulla utilizzabilità dei dati probatori raccolti all'estero, con particolare riferimento ai risultati di intercettazioni disposte dall'Autorità giudiziaria estera attraverso l'inserimento di un captatore informatico sul "server" di una piattaforma

criptata. La Corte si chiede, tra l'altro, se, per es., qualificando l'acquisizione come corrispondenza informatica e in ossequio al parametro della proporzionalità nella emissione di un OIE, l'autorità giudiziaria italiana possa sindacare il carattere "massivo" (e così potenzialmente non "proporzionato e adeguato") della raccolta generalizzata di flussi comunicativi ottenuti tramite intercettazione diretta del server siccome disposto dall'autorità giudiziaria francese, ovvero, ove si qualificasse come acquisizione di intercettazioni da altro procedimento *ex* art. 270 c.p.p., se l'autorità giudiziaria italiana possa svolgere un autonomo apprezzamento dei presupposti applicativi delle intercettazioni, come consentito nell'ordinamento interno italiano, o ancora se possa ritenere illegittima in quanto prova atipica l'intercettazione ottenuta tramite inoculazione di virus intrusore nel server, posto che nell'ordinamento italiano l'agente captatore è consentito solo nella forma della inoculazione in dispositivi elettronici portatili[10].

6. L'attesa prossima pronuncia della Corte di Giustizia dell'Unione europea. Le conclusioni dell'Avvocato generale.

Le questioni relative alla conformità alla Direttiva 2014/41/UR degli OIE emessi dal pubblico ministero per l'acquisizione dei contenuti delle chat criptate di interesse di un procedimento penale, alla necessità di un preventivo vaglio giurisdizionale dello Stato emittente l'OIE e alle ricadute in termini di utilizzabilità delle prove sono state portate all'attenzione della Corte di Giustizia dell'Unione europea su rinvio pregiudiziale della Corte regionale di Berlino, dinanzi al quale pende un procedimento originariamente incardinato presso la procura di Francoforte e poi oggetto di separazione trasmissione verso plurime procure locali (Causa C 670-22).

Il procuratore tedesco, avendo interesse alla raccolta di dati relativi agli utenti tedeschi di EncroChat, apriva un'indagine per traffico di sostanze stupefacenti di ingente quantità nei confronti di persone non ancora identificate, ma ragionevolmente parte di un gruppo criminale organizzato operante in Germania. Il procuratore richiese successivamente, tramite più ordini di indagine europei, l'autorizzazione alle autorità francesi all'uso dei dati raccolti sulla piattaforma per il proprio procedimento penale. La

[10] La copiosa attività di veicolazione degli OIE italiani e di costante interlocuzione con la AG francese, svolta dal Desk italiano di Eurojust, può già offrire un contributo al primo punto posto da ultimo dalla Cassazione: la natura delle prove acquisite tramite OIE, ovvero se corrispondenza telematica (art. 254-bis c.p.p.) o intercettazioni disposte in altro procedimento (art. 270 c.p.p.), è suscettibile di dipendere da quanto sia stato acquisito, caso per caso, via OIE dal procedimento penale francese, in seno al quale per un verso si è svolta un'attività di intercettazione di flussi comunicativi in corso e per altro verso si è acquisita la mole delle chat già registrate. Ebbene, alla stregua di quanto precisato dalla autorità giudiziaria francese a seguito di richieste di informazioni integrative da parte della AG italiana, tutti gli ordini di indagini europei eseguiti per l'Italia sono consistiti unicamente in scambi comunicativi già cristallizzati al momento della acquisizione e non anche in flussi *live* propri della fase di intercettazione, così da dover ragionevolmente ricadere nell'ambito del sequestro di corrispondenza telematica.

Corte di Lille autorizzò la trasmissione dati e l'utilizzo di dati EncroChat relativi agli utenti tedeschi.

La corte tedesca, autrice del rinvio pregiudiziale alla CGUE, nell'invocare un'interpretazione conforme degli articoli 6(1) (a), 6 (1) (b), 31(1) e (3) della Direttiva si è chiesta, in sintesi:

- se la Autorità Giudiziaria deputata a emettere l'OIE in base all'articolo 6 (1) della direttiva OIE in combinato disposto con l'articolo 2 (c), ove detto OIE sia rivolto ad ottenere prove già esistenti nello stato di esecuzione (Francia), debba essere il giudice, [quanto meno] nella ipotesi in cui, secondo il diritto dello Stato richiedente (Germania) la sottostante forma di raccolta delle prove (ovvero le intercettazioni) avrebbe dovuto essere ordinata da un giudice in un corrispondente caso di diritto interno;
- alternativamente, se l'OIE debba essere emesso da un giudice, quantomeno nel caso in cui lo Stato di esecuzione ha attuato la sottostante misura investigativa nel territorio dello Stato richiedente con lo scopo successivo di rendere quegli elementi probatori disponibili alle autorità investigative delle autorità richiedente interessata (Germania) perché possa utilizzarli in un proprio procedimento penale;
- se un OIE rivolto ad ottenere delle prove debba essere comunque emesso da un giudice, indipendentemente dalle regole giurisdizionali dello Stato richiedente, quando la misura investigativa in parola implichi una grave interferenza in diritti fondamentali di elevato rango;
- se l'articolo 6 (1)(a) della direttiva 2014/41 precluda la trasmissione di dati già disponibili allo Stato di esecuzione via OIE, laddove tali dati siano stati ottenuti attraverso la intercettazione di forme di comunicazione o di traffico dati tale da coprire *tutti* gli utenti sottoscrittori di un determinato servizio comunicativo e all'epoca della intercettazione o della emissione dell'OIE non vi era una concreta evidenza della commissione di gravi reati da parte degli utenti medesimi;
- se l'articolo 6 (1) (a) precluda l'OIE lì dove l'integrità dei dati raccolti attraverso le intercettazioni non possa essere verificata dalle autorità giudiziarie dello Stato di esecuzione a causa della apposizione del segreto assoluto;
- se la trasmissione dati via OIE sia preclusa dalla direttiva sull'OIE, laddove le misure investigative di intercettazione adottate dallo Stato di esecuzione (Francia) non sarebbero consentite secondo il diritto dello Stato emittente (Germania) in un caso domestico similare;
- se una misura che coinvolga l'infiltrazione dei dispositivi [degli utenti] finali, con lo scopo di raccogliervi dati traffico dati location e scambi comunicativi per via telematica, costituisca intercettazione di comunicazioni ai sensi dell'art. 31 della direttiva OIE;
- se la notifica in base all'articolo 31 (1) della direttiva OIE [c.d. allegato C] debba essere sempre indirizzata a un giudice, quantomeno quando la misura pianificata dallo Stato intercettante possa essere ordinata solo da un giudice, secondo lo Stato destinatario della notifica.

Meritano di essere qui sintetizzate le conclusioni dell'Avvocato generale della CGUE, rese note il 26 ottobre 2023, le quali, pur non potendo necessariamente prefigurare quale sarà la futura decisione della Corte, sviluppano un'analisi assai approfondita del tema in tutti i suoi profili e giungono all'esito di un procedimento nel quale sono stati auditi i contributi di numerose parti e intervenienti[11].

L'Avvocato Generale evidenzia come svariate alte corti di Paesi europei si stiano in questi mesi interrogando sul processo di acquisizione della prova relativo alle chat decriptate e tra queste anche la Corte di giustizia della UE, ma ricorda che il focus del procedimento del rinvio pregiudiziale è dato non già dalla legittimità o validità delle attività investigative di intercettazione svolte dalle autorità francesi, materia di esclusiva pertinenza dell'Autorità Giudiziaria francese, ma dalla compatibilità con la direttiva 2014/41/UE di ordini di indagini europei emessi da *uffici giudiziari inquirenti* – come nel caso di specie la Procura di Francoforte o, come in Italia, il pubblico ministero procedente – allo scopo di acquisire i dati ricavati dalla attività di intercettazione di flussi comunicativi avvenuta in Francia e lì esauritasi, prima e indipendentemente dagli ordini di indagine europei.

L'OIE di cui infatti viene contestata la validità dinanzi al giudice remittente tedesco non mirava a raccogliere in Francia dati *ex novo* attraverso un autonomo servizio di intercettazione di comunicazioni, ma solo a richiedere il *trasferimento di prove già raccolte* nell'ambito del procedimento penale francese.

Tale tipo di OIE ricade, pertanto, nell'articolo 1 (2), seconda parte, della Direttiva 2014/41, essendo rivolto non già a compiere atti investigativi [o a formare una prova) in un altro Stato membro, ma ad ottenere *prove che siano già in possesso delle competenti autorità dello Stato di esecuzione*.

L'Avvocato generale prosegue ricordando che in base all'articolo 6 (1) della direttiva 2014/41 l'autorità emittente l'OIE deve verificare che esso sia necessario e proporzionato allo scopo da raggiungere e che la misura richiesta avrebbe potuto essere emessa alle medesime condizioni in un caso di diritto interno similare. In sintesi, l'autorità emittente deve svolgere una verifica astratta ed una concreta: quella astratta (art. 6 (1), lett. b) volta ad appurare che la misura investigativa richiesta nell'OIE esista nel proprio diritto interno e a quali condizioni possa essere disposta; quella concreta (art. 6 (1), lett. a) volta ad appurare che quel particolare ordine sia necessario e proporzionato agli scopi perseguiti nel procedimento penale interno.

Punto cruciale è stabilire chi possa essere l'autorità emittente.

Secondo l'articolo 2 (c) della direttiva, può essere "un giudice, una Corte, un giudice investigativo o un pubblico ministero competente nel caso di interesse".

L'art. 6(1)(b) della Direttiva 2014/41/UE recita che «*L'autorità di emissione può emettere un OEI solamente quando ritiene che […] l'atto o gli atti di indagine richiesti nell'OEI*

[11] Per il comunicato di sintesi:
https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-10/cp230163it.pdf;
per il testo integrale:
https://curia.europa.eu/juris/document/document.jsf;jsessionid=EEF3F45D476085A9ADBA8A86C66FF78D?text=&docid=279144&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=100225

avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo». Pregiudiziale è pertanto definire cosa si intenda per "Caso domestico analogo": con ciò deve qui ritenersi il trasferimento di prove da un procedimento penale ad un altro nell'ambito del medesimo sistema giudiziario (ovvero nel caso in esame, da un procedimento penale tedesco ad un altro pendente davanti altra autorità giudiziaria tedesca), e ciò tenuto conto del lessico dell'articolo 6 (1)(b) della direttiva per cui "*l'atto di indagine indicato nell'OIE*" deve essere quello che un'autorità interna deve essere abilitata ad adottare a livello interno; in tal caso si tratta con ogni evidenza del trasferimento di una prova già in possesso delle autorità giudiziarie francesi. Pertanto, se il diritto tedesco, per ipotesi, proibisse il trasferimento interno di comunicazioni intercettate da un procedimento penale ad un altro, l'autorità emittente non potrebbe chiedere via OIE nemmeno un tipo di trasferimento transfrontaliero.

La Corte remittente tedesca evidenziava, però, come un OIE destinato al trasferimento di prova preesistente non possa essere emesso indipendentemente dalla disamina di come quella prova fu originariamente raccolta; pertanto, la Corte tedesca si interrogava sulla proporzionalità e dunque legalità delle misure investigative originarie adottate dall'autorità francese.

L'Avvocato generale ribadisce che l'autorità che emette l'OIE non può sindacare la legalità e la proporzionalità delle misure attraverso le quali lo Stato di esecuzione ha raccolto le prove. Il principio del mutuo riconoscimento, cardine della cooperazione in materia penale all'interno dell'unione europea, preclude all'autorità che emette l'OIE di verificare se il sottostante atto investigativo attraverso il quale la prova è stata raccolta sia stato legalmente intrapreso nello Stato membro di esecuzione. Sebbene infatti i sistemi giuridici europei possano differire in modo significativo tra loro, la cooperazione giudiziaria penale in ambito UE si fonda sull'assunzione per cui tutti gli Stati membri rispettano i diritti fondamentali dell'individuo.

Perciò, a meno che le sottostanti misure investigative fossero ritenute illegali nell'ambito del procedimento penale francese, l'autorità emittente non è nelle condizioni di poterne sindacare la legittimità.

Le circostanze del caso in esame non inducono, peraltro, il sospetto di un abuso nelle procedure di indagine transfrontaliera da parte della Francia. La Francia ha acquisito le prove in questione nel corso di un suo proprio procedimento penale e, sebbene tali prove siano risultate di interesse per la Germania, la Francia non ne ha intrapreso la raccolta in vista di una indagine tedesca e dunque, anche a ritenere che un giudice tedesco non avrebbe utilizzato un tale tipo di intercettazione nel diritto tedesco, le autorità francesi hanno adottato tali atti di indagine in conformità al loro diritto interno, previa autorizzazione di un giudice francese.

Quindi, e sempre al fine di chiarire quale sia l'autorità competente deputata ad emettere un OIE nel diritto interno, nel richiamare la decisione della Corte di giustizia *Traffic and local data* (ove si rimarca che l'OIE deve essere emesso da un organo giudicante se così prevede la legge dello Stato richiedente in relazione al tipo di atto di indagine o di prova richiesto nel contesto domestico), si conclude che il parametro è dato qui non già dalla intercettazione di comunicazioni, ma dal trasferimento di prove preesistenti e acquisite nell'ambito del Paese richiesto, per cui ci si deve chiedere se il trasferimento di

prove da un procedimento penale ad un altro nel diritto interno sia competenza soltanto del giudice o anche del pubblico ministero.

Nei successivi paragrafi (64-66) le conclusioni dell'Avvocato generale affrontano il cruciale tema se, a monte dell'emissione di un OIE in tale contesto, sia necessario un provvedimento o comunque uno scrutinio del giudice dello Stato richiedente circa i presupposti di ammissibilità delle intercettazioni di cui il pubblico ministero intende chiedere l'acquisizione alla Francia, ovvero se, laddove la prova oggetto di trasferimento (v. le intercettazioni) nel diritto interno tedesco fosse soggetta ad autorizzazione di un giudice, l'OIE dovrebbe comunque essere emesso da un giudice o previa autorizzazione di un giudice. L'Avvocato generale risponde che, se il trasferimento di prove esistenti fosse avvenuto a livello interno, da un pubblico ministero a un altro, la misura di intercettazione di telecomunicazioni sottostante sarebbe stata certamente disposta, nel diritto tedesco, da un giudice. Pertanto, la proporzionalità dell'ingerenza nei diritti fondamentali sarebbe stata controllata da un giudice. Ciò rende accettabile, dal punto di vista della protezione dei diritti degli indagati e degli imputati, consentire l'utilizzo di tali prove in un altro procedimento penale senza un ulteriore intervento di un giudice. Quando il trasferimento di prove si svolge da uno Stato all'altro, la normativa opera diversamente. Poiché qui le intercettazioni sono state autorizzate dal giudice francese, il principio del riconoscimento reciproco esige che le autorità tedesche attribuiscano a tale fase procedurale lo stesso valore che esse attribuirebbero ad essa a livello interno. Ciò anche quando, in un caso concreto, un giudice tedesco deciderebbe in modo diverso.

Tale valutazione non cambia per il fatto che alcuni utenti di EncroChat erano localizzati in territorio tedesco, perché la raccolta delle prove in Francia è avvenuta per le ragioni proprie dell'investigazione francese, mentre la scoperta che alcuni utenti fossero in territorio di altro Paese è solo la conseguenza e non la ragione delle intercettazioni disposte.

Altro passaggio cruciale dell'analisi è quello in cui si valuta se, come ritenuto nel rinvio pregiudiziale, l'emissione di un OIE rivolto al trasferimento di prove che consistano nella intercettazione di telecomunicazioni richieda sempre l'autorizzazione di un giudice, sulla scorta della sentenza della Corte di Giustizia dell'Unione europea - Grande Sezione del 02/03/2021 nel caso 746/2018[12].

Ora, osserva l'Avvocato generale come la direttiva 2002/58/UE sulla e-privacy e la pertinente giurisprudenza non si applicano alla situazione in esame. Esse si applicano solo quando i fornitori di servizi di telecomunicazioni sono richiesti dal diritto interno di conservare i dati del traffico e di localizzazione associati alle telecomunicazioni e

[12] È noto che la Corte ha in quella sede affermato che l'articolo 15, paragrafo 1, della direttiva 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, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali della UE, deve essere interpretato nel senso che l'accesso ai fini di un'istruttoria penale ai dati relativi al traffico (telefonico e telematico) e ai dati relativi all'ubicazione, conservati da service provider, deve essere compiuto mediante autorizzazione di una Corte o di un altro organismo imparziale, e non anche di un pubblico ministero. L'ordinamento italiano si è conformato attraverso l'art. 1 Decreto-Legge 30.9.2021 n. 132, conv. L. 23.11.2021 n. 178, che ha novellato l'art. 132 del D. Lgs. n. 196/2006.

quando le pubbliche autorità chiedono di accedere ai dati così conservati. Quando, invece, l'intercettazione è attuata direttamente dagli Stati membri senza che passi da obblighi posti ai service provider, la direttiva sulla privacy non si applica. Si applica solo il diritto interno.

Se peraltro – spiega il parere – si vuole entrare nella logica più profonda della decisione della CGUE 2/3/2021, ovvero del perché il pubblico ministero è ritenuto lì inidoneo a svolgere una valutazione imparziale di proporzionalità nell'accesso ai dati delle telecomunicazioni, allora bisogna osservare che nel contesto della direttiva sulla e-privacy i dati ai quali si accede sono in possesso degli operatori delle telecomunicazioni e attengono alla *generalità della popolazione* [cioè degli utenti di un servizio]; i dati conservati non sono oggetto di un caso specifico, ma costituiscono piuttosto una forma di "sorveglianza di massa"; perciò la richiesta accesso del pubblico ministero è la prima occasione nella quale circostanze specifiche e individuali vengono in rilievo, ed è pertanto, giustificato esigere che un *soggetto terzo e imparziale* valuti la proporzionalità di tale accesso, per evitare abusi da richieste potenzialmente indiscriminate e massicce di dati conservati.

Ciò distingue profondamente il caso della intercettazione dei flussi comunicativi sulle chat qui in esame. I dati da trasferire non sono raccolti indiscriminatamente dall'intera popolazione, ma nel quadro di indagine penale in Francia sotto il controllo di un giudice che li ha autorizzati. Il livello di intrusione nella privacy e nella protezione dati nei due casi è ben diverso: i dati oggetto dell'OIE erano limitati agli utenti di EncroChat in Germania in un contesto nel quale vi erano fondati elementi per ritenere che tale servizio di telecomunicazione fosse utilizzato per commettere reati. Ciò non vuol dire che l'intrusione nella vita privata di tali utenti sia irrilevante, ma non è comparabile a quella sorveglianza di massa sulla popolazione generale in cui si sostanzia la materia della conservazione dei dati ad opera dei *service provider*[13].

Infine, l'Avvocato generale rileva che il diritto dell'Unione non disciplina, nella fase attuale del suo sviluppo, l'ammissibilità di prove raccolte tramite un OEI emesso in violazione dei requisiti previsti dalla direttiva OEI. L'ammissibilità delle prove è una materia che rientra nel diritto nazionale, il quale deve tuttavia essere conforme ai requisiti dei diritti della difesa di cui agli articoli 47 e 48 della Carta dei Diritti fondamentali della UE[14].

---

[13] L'ultimo punto delle conclusioni è dedicato all'obbligo di notifica ex articolo 31 della direttiva sull'OIE.

[14] In un ideale dialogo tra corti europee in tema di comunicazioni crittografate, vale, infine, la pena segnalare la recente sentenza della Corte Europea dei Diritti dell'Uomo del 13/2/2024 nel caso 33696/19 Podchasov c. Russia. Il caso origina nel 2017, quando il servizio di sicurezza FSB russo chiese all'applicazione di messaggistica Telegram di fornire tutte le informazioni tecniche per decrittografare le comunicazioni degli utenti per sospetto impiego, da parte di alcuni utenti, in attività di terrorismo; al rifiuto di Telegram, motivato dal fatto che l'ordine di disvelamento avrebbe imposto di creare una backdoor che avrebbe indebolito il meccanismo crittografia indistintamente nei confronti di tutti gli utenti del servizio end-to-end, una Corte distrettuale di Mosca dispose il sequestro della società e il blocco della app, consentendo al FSB di ottenere le chiavi di crittografia e dunque di accedere a tutti i dati comunicativi degli utenti.
Uno degli utenti impugnò l'ordinanza giudiziaria in Russia, ma la sua richiesta fu respinta, così dando luogo nel 2019 a ricorso alla CEDU. La Corte ha statuito che «*la legislazione contestata, che prevede la conservazione di*

7. Tirando le fila…

Le tensioni interpretative registrate dinanzi alle corti superiori di numerosi Paesi europei (e non) e davanti a Corti sovranazionali[15] danno la misura di una trasformazione in atto nella giurisdizione in forza, da una parte, della irruzione del digitale nella vita delle organizzazioni criminali e, dall'altra, della messa in campo di sofisticati sistemi intrusivi sviluppati da alcuni Paesi europei e resi ancora più efficaci dall'agire in squadre investigative comuni. Esse hanno anche il pregio di avere così generato e di continuare ad alimentare un ricco dibattito sugli strumenti della cooperazione giudiziaria europea soprattutto nel cruciale settore dei mezzi di prova che impattano sulla riservatezza delle comunicazioni telematiche.

Gli arresti giurisprudenziali finora noti, come pure l'autorevole parere dell'Avvocato generale della CGUE (in attesa della pronuncia della Corte), sembrano tracciare un primo, temporaneo assestamento del contenzioso su alcuni passaggi chiave e permettono di trarre spunti di riflessione utili al dibattito nella giurisprudenza italiana:

- L'acquisizione, con ordine di indagini europeo dei flussi comunicativi svoltisi sulle piattaforme EncroChat e Sky-ecc costituisce legittimo trasferimento di prove preesistenti negli originari procedimenti penali francesi di dati ivi acquisiti;
- L'autorità giudiziaria dello Stato richiedente i dati non può sindacare la correttezza del procedimento penale francese in virtù del principio di mutuo riconoscimento, cardine degli strumenti di cooperazione giudiziaria europea e frutto della *mutual trust* che ispira i rapporti tra ordinamenti e sistemi giudiziari dell'Unione; tale acquisizione è, peraltro, avvenuta previa autorizzazione motivata dell'autorità giudiziaria francese nelle forme della intercettazione di comunicazioni e della decriptazione;
- né dovrebbe necessitare (salva la peculiare ipotesi di cui all'art. 31 della Direttiva sull'OIE ed entro stretti limiti) una *preventiva* autorizzazione del giudice per l'acquisizione dei dati (se essa non è richiesta per il trasferimento di mezzi di prova tra un procedimento e l'altro nell'ordinamento interno), salvo il libero convincimento nella valutazione dei gravi indizi prima e della prova poi nelle decisioni giudiziarie interne, nelle quali i dati così acquisiti verranno in rilievo (v. anche Corte Federale tedesca) o la verifica delle modalità acquisitive se, ai fini

---

tutte le comunicazioni internet di tutti gli utenti, l'accesso diretto – su base generalizzata e senza adeguate garanzie contro gli abusi – dei servizi di sicurezza ai dati archiviati e l'obbligo di decriptare le comunicazioni crittografate, come applicato alle comunicazioni crittografate da punto a punto, non possono essere considerate necessarie in una società democratica, compromettendo il diritto al rispetto della vita privata ex art. 8 della Convenzione Europea dei diritti dell'uomo. La decisione, meritevole di autonoma analisi e ferma la diversità tra le piattaforme qui coinvolte rispetto a quelle tipo Encrochat e Sky ECC», rimanda all'importanza di un vaglio giurisdizionale *ad hoc* a fondamento di attività decriptative e captative e a parametri di pertinenza e proporzionalità dell'accesso ai dati rispetto all'obiettivo di contrasto al crimine.

[15] Pende anche una questione dinanzi alla Corte europea dei diritti dell'uomo.

della prova, rileva per il rispetto del principio del giusto processo (Hoge Raad olandese); sul punto, alle considerazioni già svolte in tema di ragionevole inquadramento delle chat decriptate nell'alveo della "corrispondenza" e di riconducibilità dell'acquisizione interna a un trasferimento di prove piuttosto che al compimento di attività di indagine *ex novo*, può affiancarsi il rilievo per cui nel sistema interno i poteri di intervento del GIP sono tipizzati e definiti secondo precisi presupposti, di talché è difficile fare ricadere entro gli artt. 266 e seguenti c.p.p. (o in altre previsioni codicistiche) una sorta di avallo apparentemente preventivo, ma in realtà postumo, a un'attività di intrusione sulla libertà e riservatezza delle comunicazioni che già è stata già disposta e svolta dall'autorità giudiziaria estera nel procedimento 'madre';

- sposando la tesi per cui si verte in materia di trasferimento di prove da altro procedimento penale, trasferimento che dovrebbe operare dall'estero alle medesime condizioni che in Italia, e qualificando i dati in esame come "corrispondenza", non dovrebbe parimenti occorrere – a fondamento dell'ordine di indagine europeo – un preventivo decreto di sequestro probatorio del pubblico ministero (che non è richiesto per travasare corrispondenza *già in sequestro* da un procedimento interno all'altro)[16];
- pare, infine, ultroneo in questo ambito il richiamo alla disciplina delle tutele di cui alla Direttiva 2002/58/UE, sia per la natura del processo di raccolta dei dati qui in rilievo, che è autonomamente avvenuto attraverso intercettazione, senza bisogno di richiesta di dati a terzi detentori, sia perché non si tratta di una operazione di sorveglianza di massa di utenti di servizi comunicativi, sia infine per la intrinseca diversità tra servizi di comunicazioni offerti da *service providers* operanti sul mercato pubblico e regolato e piattaforme strutturalmente concepite per soddisfare esigenze di impenetrabilità della criminalità organizzata, senza conferimento dei reali dati identificativi degli utenti.
- sulla possibilità, poi, di attivare un sindacato giurisdizionale più o meno penetrante, anche postumo, di utilizzabilità degli esiti dell'attività captiva acquisita dall'estero sulla base della differenza tra i presupposti legittimanti tali attività di indagine nei due ordinamenti (Stato emittente e Stato di esecuzione), come si chiede la Corte di Cassazione nella ordinanza di remissione n. 2329/24, si possono offrire i seguenti spunti di riflessione:
  - quanto al parametro della proporzionalità, menzionato nell'ordinanza di remissione n. 2329/24 (punto 6) con riferimento al sequestro eventualmente 'massivo' di corrispondenza telematica disposto dall'autorità giudiziaria francese, la verifica di proporzionalità investe solo l'ordine disposto dalla

[16] Di diversa opinione M. Daniele, *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite*, in Sistema Penale, 11.12.2023 (https://www.sistemapenale.it/it/scheda/daniele-ordine-europeo-di-indagine-penale-e-comunicazioni-criptate-il-caso-sky-ecc-encrochat-in-attesa-delle-sezioni-unite), ad avviso del quale occorrerebbe un previo decreto di sequestro probatorio del PM, cui conseguirebbe la possibilità di invocare l'esclusione delle comunicazioni dal materiale probatorio a disposizione del giudice di merito tramite il riesame del sequestro.

Autorità emittente l'OIE nell'ambito del *proprio* procedimento penale (*ex* art. 6.1 della direttiva 2014/41 l'autorità emittente l'OIE deve verificare che esso sia necessario e proporzionato allo scopo da raggiungere ai fini del procedimento di cui all'articolo 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata)[17], e non anche l'attività autonomamente disposta dall'autorità giudiziaria dello Stato di esecuzione per le proprie esigenze investigative e processuali, il sindacato sulla quale risulterebbe ultroneo e non consentito;

- quanto ai presupposti dell'attività captativa (e fermo il rilievo per cui nel caso italiano, si è più ragionevolmente trattato di chat già cristallizzate e non di flussi in atto), è ancora il principio del mutuo riconoscimento, come declinato nel diritto e nella giurisprudenza euro-unitari, a indicare la strada. Come si evince dal considerando 19 della Direttiva 2014/41[18], tale principio non pretende coincidenza piena delle regole processuali e probatorie dei singoli Stati aderenti alla direttiva, facendo piuttosto leva su una loro omogeneità complessiva, fermo il rispetto dei diritti fondamentali dell'individuo, derivante dalla comune soggezione degli Stati membri al sistema della Carta dei diritti fondamentali dell'Unione europea, alla Convenzione europea dei diritti dell'uomo e alla relativa giurisprudenza delle corti superiori europee.
- Nonostante, infatti, tale principio, codificato dall'articolo 82 TFUE, propugni un progressivo e sempre più elevato ravvicinamento tra le legislazioni nazionali[19], permane una oggettiva e fisiologica divergenza tra ordinamenti anche sul piano degli istituti processuali penali, mentre non è stata ancora adottata (né in seno alla direttiva OIE né in seguito) una sorta di tavola dei principi generali condivisi, ossia di più specifiche disposizioni calibrate sulle diverse tipologie di prova[20]. Perciò, il legislatore sovranazionale ha stabilito

---

[17] Considerando n. 11 alla Direttiva OIE: «*L'autorità di emissione dovrebbe pertanto accertare se le prove che si intende acquisire sono necessarie e proporzionate ai fini del procedimento, se l'atto di indagine scelto è necessario e proporzionato per l'acquisizione di tali prove, e se e opportuno emettere un OEI affinché un altro Stato membro partecipi all'acquisizione di tali prove. [….]. L'esecuzione di un OEI non dovrebbe essere rifiutata per motivi diversi da quelli previsti nella presente direttiva. Tuttavia l'autorità di esecuzione dovrebbe avere la facoltà di optare per un atto di indagine meno intrusivo di quello richiesto nell'OEI interessato qualora consenta di ottenere risultati analoghi*».

[18] «*La creazione di uno spazio di libertà, di sicurezza e di giustizia nell'Unione 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. Tuttavia, tale presunzione è 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 i suoi obblighi in materia di protezione dei diritti fondamentali riconosciuti nella Carta, l'esecuzione dell'OEI dovrebbe essere rifiutata*».

[19] A norma dell'art. 82, § 1, TFUE, «la cooperazione giudiziaria in materia penale nell'Unione deve fondarsi sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e include il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri nei settori di cui al paragrafo 2 e all'articolo 83» […].

[20] *Libro Verde sulla ricerca della prova in materia penale* adottato dalla Commissione europea l'11 novembre 2009, i nuovi strumenti di assistenza avrebbero dovuto darsi carico dell'adozione di "*norme comuni per la raccolta delle prove in materia penale*", citato nel par. 23 della Circolare del Ministero della Giustizia 26.10.2017 in tema di attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale – Manuale

una presunzione soltanto *relativa* di conformità di ciascun ordinamento al diritto dell'Unione europea e, in particolare, ai diritti fondamentali, presunzione – come ricorda la Corte di Giustizia della UE nella sentenza 11.11.2021 del caso Gavanozov (C-852/19)[21] – che può essere superata nel caso concreto [solo] di fronte a fondati motivi per ritenere che l'esecuzione dell'atto indicato nell'OEI comporti una lesione dei diritti fondamentali[22];

- ora, differenze tra i presupposti legittimanti, per esempio, l'intercettazione o il sequestro di corrispondenza o i dati del traffico telefonico e telematico (quale l'adozione di criteri diversi di selezione dei reati legittimanti l'attività di captazione/apprensione, ovvero la facoltà di uso di un meccanismo, come il virus intrusore, per una o per un'altra tipologia di dispositivo), potrebbero ragionevolmente non costituire motivo di sospetta violazione dei diritti umani fondamentali, ma rientrare nella fisiologia della diversa regolamentazione della medesima materia, fermo il rispetto di alcune garanzie fondamentali (quali la previa autorizzazione giudiziaria, l'onere motivazionale, la funzionalità degli strumenti alla prova di reati di una certa gravità, l'obbligo di conservazione dei supporti originali e di verbalizzazione delle operazioni *nel procedimento originario*, etc.). Si ricordino le riflessioni dell'Avvocato generale della Corte di giustizia sulla esclusione di *fumus* di abuso nelle procedure di indagine ad opera dell'autorità giudiziaria francese nel presente caso; riguardo, peraltro, all'originaria inoculazione di *trojan horse* sui server piuttosto che sui singoli dispositivi mobili, la soluzione adottata dalla Francia su tecnologia olandese, anche sulla scorta dei chiarimenti via via forniti alle autorità giudiziarie italiane, pare costituire non già il riflesso di una maggiore intrusività nelle comunicazioni interpersonali, bensì il portato di un avanzamento tecnologico e di una modalità operativa rivelatasi *imprescindibile* per giungere alla captazione dei flussi comunicativi incorporati sui singoli dispositivi portatili degli utenti di interesse. La autorità giudiziaria francese non ha indiscriminatamente usato i dati di tutti gli utenti nei propri procedimenti penali, mettendo piuttosto quei dati a disposizione delle Autorità Giudiziarie dei Paesi interessati, i quali nei relativi OIE ne hanno dovuto evidenziare la pertinenza rispetto alle proprie indagini.

---

operativo.

[21] Punto 54: «…*Tuttavia, occorre ricordare che discende, segnatamente, dai considerando 2, 6 e 19 di detta direttiva che l'ordine europeo di indagine è uno strumento che rientra nella cooperazione giudiziaria in materia penale di cui all'articolo 82, paragrafo 1, TFUE, che si fonda sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie. Tale principio, che costituisce la «pietra angolare» della cooperazione giudiziaria in materia penale, è a sua volta fondato sulla fiducia reciproca nonché sulla presunzione relativa che gli altri Stati membri rispettino il diritto dell'Unione e, in particolare, i diritti fondamentali [v., in tal senso, sentenza dell'8 dicembre 2020, Staatsanwaltschaft Wien (Ordini di bonifico falsificati), C-584/19, EU:C:2020:1002, punto 40*]».

[22] C. DE LUCA, *La Corte di giustizia si pronuncia nuovamente sull'ordine europeo di indagine penale: la tutela dei diritti fondamentali prevale sull'efficienza investigativa*, in questa Rivista, 9 marzo 2022.

In attesa della pronuncia delle Sezioni Unite della Cassazione italiana e della Corte di Giustizia della UE, le sfide aperte sono, comunque, ancora molte e importanti.

Un primo terreno di verifica sarà costituito dalla capacità di resistenza nel contraddittorio del processo delle acquisizioni già compiute e, pertanto, dalla capacità di soddisfare l'esigenza delle parti e del giudice della cognizione di comprendere metodi di selezione dei dati di interesse nel singolo procedimento interno, completezza della raccolta e garanzie adottate[23].

Per questo è auspicabile che fin da ora le produzioni dei flussi comunicativi acquisiti con OIE siano corroborate, da parte del pubblico ministero, da una disamina analitica del procedimento penale originario nel quale tali dati sono stati acquisiti, delle procedure e delle tecniche utilizzate e dei provvedimenti autorizzativi.

Un esempio paradigmatico è rappresentato dall'ordinanza del Tribunale del Riesame di Reggio Calabria del 23/11/2023, la quale, decidendo sul rinvio della Cassazione di cui alla sentenza n. 44155/23 del 26/10/2023, ha nuovamente confermato l'ordinanza genetica, dando atto delle più articolate produzioni effettuate dal pubblico ministero, contenenti una rassegna organica e puntuale dei provvedimenti autorizzatori francesi, delle tecniche di intercettazione dei server, delle modalità di conservazione dei dati e della identificazione dei dati di rilievo per i procedimenti interni.

Ne discende anche la necessità di selezionare correttamente i dati comunicativi raccolti per permettere alla autorità giudiziaria italiana di vagliare la pertinenzialità, completezza e utilità alle fattispecie oggetto dei procedimenti penali interni[24].

Ma non si può tacere che il passaggio all'era digitale, la natura transfrontaliera dei flussi comunicativi nelle chat criptate in uso alla criminalità organizzata e la necessità per gli attori delle indagini di tenere il passo rispetto a tali innovazioni, oltre a generare trasformazioni della giurisdizione, delle tecniche intrusive, della cooperazione internazionale, hanno segnalato asimmetrie, disallineamenti e inadeguatezze tra apparati investigativi di diversi Paesi, anche europei, nel fronteggiare la sfida.

«*I mafiosi avranno sempre una lunghezza di vantaggio su di noi*». Così – non a caso – il Procuratore Nazionale Antimafia e Antiterrorismo, Giovanni Melillo, citava Giovanni Falcone il 31 gennaio 2023, nel corso dell'audizione al Senato sul tema delle intercettazioni, per sottolineare quella che ha definito «*una caratteristica costante della criminalità mafiosa: la sua capacità di agire avvalendosi di straordinarie capacità di adattamento,*

---

[23] Per una proiezione sull'utilizzazione dei dati acquisiti in dibattimento M. DANIELE, *Ordine europeo di indagine penale*, cit.

[24] L'ordinanza è stata resa nell'ambito del procedimento penale c.d. "Eureka", relativo a fattispecie di associazione mafiosa di tipo 'ndranghetistico, associazione finalizzata al traffico di stupefacenti, riciclaggio e reati collegati, istruito dalla Direzione Distrettuale Antimafia di Reggio Calabria e che ha visto l'agire, con il coordinamento di Eurojust, di più Squadre Investigative Comuni, tra la DDA italiana e le Procure tedesche di Monaco I, Coblenza, Saarbrücken e Düsseldorf e, ancora, l'Ufficio del Giudice Istruttore presso il Tribunale di Limburg e il Procuratore Federale di Bruxelles, lavoro sfociato in mandati di arresto europeo e ordini di congelamento di beni, eseguiti in Germania, Belgio, Francia, Portogallo, Romania e Spagna. https://www.eurojust.europa.eu/news/ndrangheta-mafia-members-arrested-investigation-belgium-italy-and-germany

ma anche di conoscenza della modernità e delle sue tecnologie»[25], per poi constatare come sia «*in gioco persino il tradizionale primato di professionalità ed efficacia dei nostri apparati di polizia, di fatto pressoché esclusi da ambiti di cooperazione che esigono la condivisione di eccezionali risorse tecnologiche e di nuovi strumenti operativi, come l'impiego a fini investigativi, pur rigidamente controllato attraverso la fissazione di rigorosi presupposti e limiti, di nuove tecniche intrusive e di quei medesimi hackers etici che anche lo Stato ha per fortuna, sia pure solo in tempi recentissimi, imparato ad utilizzare per sottoporre i propri sistemi informati a stress test necessari per saggiarne la resistenza ad attacchi interni ed esterni; oggi le indagini più importanti in materia di narcotraffico e di riciclaggio si nutrono di acquisizioni probatorie rese possibili da quadri normativi e strumenti investigativi più avanzati di quelli disponibili per la magistratura e le forze di polizia italiane*».

EncroChat, Sky Ecc ed Exclu (l'ultima giunta tra le piattaforme ad essere decriptate, nel febbraio 2023) sono state chiuse. Ma le piattaforme criptate (e non ancora decifrate) *tuttora in uso* alla criminalità organizzata, compresa quella italiana, sono ancora molteplici e in continuo sviluppo. Gli apparecchi criptati sono poi precipuamente in dotazione ai segmenti più elevati dei network criminali. La capacità di intervenire in modo tempestivo e pieno (possibilmente su flussi comunicativi in corso e non solo su dati freddi a distanza di anni dal loro svolgersi) impatta, dunque, fortemente sulla qualità e l'incisività dell'azione di contrasto al crimine organizzato.

Occorre allora pensare a robusti investimenti in innovazione tecnologica applicata alle tecniche di indagine e a forme di cooperazione interstatuale, giudiziaria e di polizia, ancora più efficaci e idonee a permettere un'acquisizione più tempestiva e partecipata, anche da parte degli apparati investigativi e degli organi giudiziari italiani, dei flussi comunicativi criptati attuali e prossimi.

È opportuno, infine, accennare al disegno di legge, allo studio al Senato, in tema di *Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute* (nuovo art. 254-*ter* c.p.p., il quale prevede che, nel corso delle indagini preliminari, il giudice per le indagini preliminari, a richiesta del pubblico ministero, disponga con decreto motivato il sequestro di dispositivi e sistemi informatici o telematici, o di memorie digitali, necessari per la prosecuzione delle indagini in relazione a circostanze e modalità dei fatti e nel rispetto del criterio di proporzione[26].

Qualora il pubblico ministero, poi, intenda procedere al sequestro dei dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute (chat *et sim.*), lo richiede al giudice per le indagini preliminari, che provvede con un distinto e ulteriore decreto motivato, disponendo il sequestro in presenza dei presupposti di cui al primo periodo e agli articoli 266, comma 1, e 267, comma 1, c.p.p.

---

[25] https://www.giustiziainsieme.it/it/processo-penale/2644-audizione-al-senato-della-repubblica-del-procuratore-nazionale-antimafia-giovanni-melillo-sul-tema-delle-intercettazioni-del-31-gennaio-2023

[26] https://www.senato.it/leg/19/BGT/Schede/FascicoloSchedeDDL/ebook/57039.pdf, contenente il dossier dei due disegni di legge in tema (n. 690 e n. 806), aggiornato al 16/2/2024.

(come nelle intercettazioni). Inoltre, copia del decreto di sequestro è notificata all'avente diritto alla restituzione del dispositivo […].

La riforma, ove a breve approvata, non inciderebbe sulle acquisizioni di dati comunicativi delle piattaforme criptate qui in esame, nel senso di determinare la necessaria autorizzazione preventiva del GIP, e ciò sia per una chiara disposizione transitoria (secondo la quale le norme in via di introduzione si applicano alle perquisizioni e ai sequestri la cui esecuzione ha avuto inizio in data successiva alla sua entrata in vigore), sia perché, ove si propendesse per l'indirizzo che rimarca trattarsi di trasferimento di prove precostituite all'estero quand'anche l'atto sottostante fosse qualificato come intercettazione, esso può avvenire con un mero provvedimento del pubblico ministero. Occorrerebbe un provvedimento autorizzatorio del GIP ove si chiedesse la raccolta di dati comunicativi che non sono stati invece ancora acquisiti dalla autorità giudiziaria straniera.

In uno scenario diverso, in cui, per ipotesi, apparati investigativi italiani fossero autonomamente in grado di intercettare una piattaforma criptata (riconducibile alla nozione di sistema informatico o telematico), al fine di decifrarne e acquisirne i flussi comunicativi sia in divenire sia nella corrispondenza telematica già storata, esattamente come ha fatto l'autorità giudiziaria francese nei casi Encrochat e Sky Ecc, invece, rispetto ai flussi comunicativi in corso si applicherebbe l'art. 266-*bis* c.p.p., mentre rispetto agli archivi di comunicazione "freddi" dovrebbe applicarsi la disciplina del nuovo sequestro *ex* art. 254-*ter* c.p.p., comprensiva delle comunicazioni agli indagati; ai possibili effetti negativi di discovery anticipata potrebbe ovviarsi in base alle norme esistenti in tema di ritardato sequestro (quali l'art. 98 DPR 309/90 e l'art. 9, comma 7, l. 146/2006).

Editore

ASSOCIAZIONE
"PROGETTO GIUSTIZIA PENALE"