PIÙ OMBRE CHE LUCI NELLE SENTENZE DELLE SEZIONI UNITE IN TEMA DI CRIPTOFONINI

Ottavia Murro - Wanda Nocerino

SOMMARIO: 1. Le (esplicite) domande e le (velate) risposte. – 2.Le indagini francesi e i riflessi sui procedimenti nazionali. – 3. Le decisioni delle Sezioni Unite, il reflusso della Corte di Lussemburgo e le questioni devolute alla Corte di Strasburgo. – 4. I frastagliati precedenti nazionali. – 5. Nodi sciolti e grovigli irrisolti. – 5.1. Le condizioni di ammissibilità dell'O.E.I. – 5.2. L'utilizzabilità dei dati raccolti all'estero nei procedimenti interni. **–** 6. La necessaria tipizzazione delle "nuove" indagini: un appello al legislatore.

ABSTRACT

Con le pronunce in commento, le Sezioni Unite delineano le regole per procedere all'acquisizione dei dati criptati ("freddi" o flussi in transito) acquisiti all'estero. Pur ammettendo un vaglio postumo del giudicante sull'utilizzabilità degli elementi di prova raccolti dall'autorità giudiziaria straniera, escludono categoricamente la necessità di un'intermediazione preventiva dell'organo della giurisdizione per richiedere l'O.E.I. Ciò che rimane avvolto nell'ombra è la qualificazione giuridica da attribuire all'attività di indagine consistente nell'acquisizione di dati comunicativi raccolti all'estero, moltiplicando le perplessità degli interpreti che si trovano a confrontarsi con principi di diritto non perfettamente sovrapponibili nel sistema nazionale. Lo scopo della ricerca è comprendere se e in che termini i dati acquisiti all'estero possano trovare impiego nel processo penale, individuando la corretta cornice giuridica nella quale le attività possono essere sussunte.

The United sections of the Court of Cassation outline the rules for proceeding with the acquisition of encrypted data ("cold" or transit flows) acquired abroad. While admitting a posthumous scrutiny by the judge on the usability of the evidence collected by the foreign judicial authority, they categorically exclude the need for preventive intermediation by the body of jurisdiction to request the O.E.I. What still remains shrouded in shadow is the legal qualification to be attributed to the investigative activity consisting in the acquisition of communication data collected abroad, multiplying the perplexities of interpreters who find themselves dealing with principles of law that are not perfectly superimposable in the national system. The aim of the research is to understand whether and in what terms the data acquired abroad can be used in criminal proceedings, identifying the correct legal framework in which the activities can be subsumed.

1. Le (esplicite) domande e le (velate) risposte.

Nel solco segnato da una giurisprudenza in fermento in tema di utilizzabilità della messaggistica scambiata su sistema cifrato *Sky Ecc* ed *Encrochat*[1], la VI Sezione presenta all'esame dell'organo riunito due distinti ricorsi[2] che, seppur formalmente separati, vertono su tre quesiti tendenzialmente sovrapponibili che così possono essere schematizzati:

a) definire la natura giuridica dell'attività di acquisizione, mediante Ordine Europeo di Indagine (O.E.I.), del contenuto di comunicazioni effettuate attraverso i criptofonini, già decriptate dall'autorità giudiziaria estera in un proprio procedimento penale;

b) verificare la sussistenza delle condizioni per legittimare il p.m. ad acquisire, per il tramite dell'O.E.I., dati informatici all'estero;

c) delineare i confini entro cui è possibile esperire un sindacato giurisdizionale nello Stato di emissione dell'O.E.I. circa l'utilizzabilità degli esiti investigativi di attività svolte all'estero.

I percorsi motivazionali che caratterizzano le pronunce in esame sono pressoché identici e le risposte alle questioni sollevate – riscritte ed ampliate rispetto alle massime provvisorie[3], anche in considerazione degli approdi della Corte di Lussemburgo[4] – si integrano e si completano vicendevolmente, salvo con riferimento al primo quesito per cui le sentenze sembrano giungere a conclusioni parzialmente difformi.

Se la Corte non ha alcun dubbio nell'escludere la necessità dell'intermediazione preventiva dell'organo della giurisdizione per richiedere l'O.E.I. (ammettendo esclusivamente un vaglio di utilizzabilità postumo degli elementi di prova acquisiti all'estero), sul presupposto per cui «rientra nei poteri del p.m. disporre l'acquisizione di atti di altro procedimento penale»[5], quello che invece rimane avvolto nel mistero è la qualificazione giuridica da attribuire all'attività di indagine consistente nell'acquisizione di dati comunicativi raccolti all'estero.

In effetti, le due sentenze – redatte dal medesimo Collegio, decise lo stesso giorno, vertenti sulle stesse questioni – riflettono posizioni pressoché divergenti: secondo la pronuncia n. 23755, «la trasmissione [...] del contenuto di comunicazioni [...] già acquisite [...] dall'autorità giudiziaria estera [...] rientra nella disciplina relativa alla circolazione delle prove tra procedimenti penali, quali desumibile dagli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p.»; secondo il provvedimento n. 23756, invece, tale acquisizione è assoggettata esclusivamente alla disciplina di cui all'art. 270 c.p.p.

Ciò significa che se per la prima sentenza (in ordine di deposito) la qualificazione giuridica delle investigazioni svolte all'estero sulle piattaforme criptate dipende dal tipo di atto condotto e, dunque, varia in base all'oggetto e alle modalità acquisitive dell'elemento probatorio, al contrario, per la seconda pronuncia l'attività di indagine condotta dall'autorità straniera è sussumibile unicamente nell'alveo delle intercettazioni e, dunque, può essere utilizzata in Italia solo alle condizioni delineate dall'art. 270 c.p.p.

Da questa prospettiva, sembra che le statuizioni del Collegio riunito hanno moltiplicato le perplessità degli interpreti che si trovano a confrontarsi con due principi di diritto non perfettamente sovrapponibili.

Senza contare, poi, che, in entrambe le pronunce, la Corte sembra porre l'accento solo su alcuni dei

complessi aspetti che involgono il tema delle indagini sulle piattaforme criptate; di conseguenza, si ha la sensazione che i principi di diritto enucleati potranno risolvere solo in parte le criticità derivanti dalla necessità (tutt'altro che remota) di svolgere investigazioni su *server* ubicati sul territorio nazionale[6].

2. Le indagini francesi e i riflessi sui procedimenti nazionali.

Prima ancora di analizzare il contenuto delle pronunce, risulta imprescindibile soffermarsi brevemente sui meccanismi di funzionamento dei criptofonini e sulle peculiari indagini svolte dalle autorità estere per acquisire le informazioni transitanti e/o giacenti sulle piattaforme criptate.

Sotto il profilo tecnico, un *cryptophone* – anche definito *Dedicated Encrypted Communication Devices* (DECD) – è un tipo di *smartphone* specificamente progettato per fornire comunicazioni sicure e proteggere da *hacking* e sorveglianza. Nei criptofonini, infatti, vengono disabilitati tutti quei servizi che possono essere facilmente intercettati, quali: la localizzazione GPS, i servizi *Google*, il *Bluetooth*, la fotocamera, i microfoni, la porta USB (che rimane in funzione solo per la carica della batteria). Rimangono attive le chiamate ma solo in modalità VoIP (*Voice over IP*), senza l'uso della rete GSM; anche la messaggistica è abilitata ma si serve di applicazioni proprietarie e crittografate che rendono, di fatto, il dispositivo impenetrabile[7].

Tali *devices* si servono delle *Hardened Secure Communication Platforms* (HSCP), più comunemente definite piattaforme di comunicazioni criptate, ossia di sistemi operativi e applicazioni installate su dispositivi di comunicazione sicuri e protetti fisicamente. Le più note sono *Encrochat*[8] e *Sky Ecc*[9], anche se in commercio ne esistono numerose e con differenti caratteristiche[10].

Sotto il profilo operativo, va detto che – pur non essendo ufficialmente noti i singoli passaggi investigativi che hanno portato all'apprensione degli elementi di prova mediante accesso ai *server* sulla piattaforma *Sky Ecc* – l'indagine si è sviluppata con l'istituzione di una squadra investigativa comune, composta dalle autorità giudiziarie e da rappresentanti delle forze di polizia di Belgio, Francia e Olanda, con il coordinamento di *Europol*[11].

Materialmente, l'acquisizione del contenuto della messaggistica è avvenuta per il tramite delle autorità francesi – luogo in cui il *server Sky Ecc* è ubicato – che hanno disposto sia intercettazioni "tradizionali", di cui

agli artt. 100 ss. del *code de procédure pénale*, sia l'acquisizione di comunicazioni archiviate su sistemi informatici, secondo la previsione dell'art. 706-102-1 c.p.p. francese.

I dati appresi, però, non sono risultati immediatamente intelligibili: l'attività di indagine, infatti, ha progressivamente svelato l'architettura informatica del sistema di comunicazione impiantato dalla società canadese di *Sky Global*, facendo emergere l'utilizzo di ben quattro chiavi di cifratura, due presenti nel *server* e due nel dispositivo del fruitore del servizio.

Di conseguenza, per poter raccogliere dati comprensibili, gli investigatori si sono visti costretti ad acquisire l'algoritmo di decodifica ricorrendo all'uso di un captatore informatico (tipo *Trojan*) funzionale ad asportare le chiavi nascoste sia sul *server* che sui criptofonini.

A questo punto, la polizia giudiziaria francese è riuscita a decodificare i messaggi già registrati e giacenti sulla piattaforma e a conoscere il significato delle comunicazioni in transito.

Come era prevedibile, l'operazione non è rimasta confinata ai Paesi direttamente interessati dall'indagine: infatti, in diversi procedimenti penali nazionali è emersa (e, con molta probabilità, continuerà ad emergere) la necessità di acquisire, mediante O.E.I., la trascrizione dei messaggi scambiati da soggetti operanti su territorio italiano dopo che gli stessi sono stati decriptati dall'autorità estera.

3. Le decisioni delle Sezioni Unite e il reflusso della Corte di Lussemburgo.

Delineati i tratti tecnici delle operazioni investigative, diviene necessario approfondire il punto di approdo a cui giunge il Supremo Consesso con le due "sentenze gemelle", nell'ottica di una analisi sistematica anche alla luce di una terza pronuncia, definita "sentenza cugina"[12], ovvero la sentenza della Corte di Giustizia del 30 aprile 2024 (*Encrochat*)[13].

Sicuramente, lo si dice già in premessa, il tema su cui la Corte si confronta non appare inedito, poiché da tempo gli operatori e gli interpreti si interrogano sul rapporto tra esigenze collettive di sicurezza e tutela dei diritti soggettivi di garanzia[14].

Ciò che, invece, sembra innovativo è il contesto in cui si inseriscono le pronunce in commento, ovvero la dimensione della criminalità contemporanea che non è più confinata all'interno di uno o più Stati, ma è diventata, ormai, globale e interconnessa[15]. Circostanza che si riverbera sul tema dei criptofonini che, come noto, ha coinvolto, quasi simultaneamente, le giurisdizioni di numerosissimi Paesi europei.

In tale scenario, le questioni rimesse alle Sezioni Unite attengono alla legittimità dell'agire investigativo, e quindi all'utilizzabilità degli esiti di indagine, nonché alla tipologia degli atti trasmessi agli organi investigativi italiani in relazione alle garanzie da riservare agli indagati[16].

Più precisamente, è proprio l'individuazione della natura dell'atto ad incidere, a cascata, sulle garanzie e sulla utilizzabilità delle prove nel processo interno.

Per tale ragione, il primo quesito che viene posto al Supremo Collegio attiene alla qualificazione dell'attività di acquisizione dei dati giacenti o transitanti su *server*, al fine di individuare il regime processuale attivabile.

In tale contesto, la norma che è venuta in rilievo è stata quella che disciplina le acquisizioni di documenti e dati informatici (art. 234-*bis* c.p.p.)[17]. Norma che, stando ai presupposti applicativi, non è apparsa applicabile al caso di specie, atteso che, si legge nelle sentenze in commento, «la sua operatività prescinde da ogni forma di collaborazione da parte dello stato estero di esecuzione», essendo attuata direttamente dall'autorità giudiziaria italiana.

Non solo. Si potrebbe anche aggiungere che, ai sensi dell'art. 234-*bis* c.p.p., è sempre consentita l'acquisizione di elementi probatori nel caso in cui documenti o dati informatici siano disponibili al pubblico, ovvero vi sia il consenso del legittimo titolare allorquando essi non si trovino sulle c.d. fonti aperte. Presupposti che, nell'attività acquisitiva di *chat* criptate, non risultano sussistenti[18].

Diversamente, lo strumento dell'O.E.I., nel regolare le modalità di acquisizione di elementi di prova transfrontalieri, presuppone dei rapporti di collaborazione tra autorità giudiziarie di diversi Stati membri dell'UE[19].

Considerati tali presupposti, viene anche in rilievo il rapporto di esclusione reciproca[20] sussistente tra

l'Ordine Europeo di Indagine e la disciplina delineata dall'art. 234-*bis* c.p.p., discipline ritenute dal Supremo Collegio come alternative.

Più precisamente, i due istituti attengono ad ipotesi e presupposti diversi, nei quali gioca un ruolo dirimente la sussistenza o meno di una collaborazione tra Stati.

Nel contempo, l'O.E.I. può essere emesso anche per ottenere prove già in possesso delle autorità competenti dello stato di esecuzione (art. 1, direttiva 2014/41/UE) e tale strumento di indagine risulta prevalente rispetto agli altri (*Considerando* n.35 della suddetta direttiva)[21].

Dalla questione così delineata, emerge che nel caso di specie ci si è trovati al cospetto di elementi di prova autonomamente raccolti dalle autorità straniere prima dell'emissione dell'O.E.I., e, dunque, di informazioni preformate sulla base della *lex loci* ed acquisite con la collaborazione tra autorità giudiziarie di diversi Stati UE[22].

Peculiarità che hanno spinto le Sezioni Unite a ritenere applicabile la disciplina dell'Ordine di Indagine Europeo e a parametrare il criterio dell'equivalenza non con la disciplina nazionale relativa alla formazione della prova, quanto piuttosto con quella della circolazione di queste ultime fra procedimenti diversi.

Nel solco di tale ragionamento, esclusa l'applicabilità dell'art. 234-*bis* c.p.p., le regole probatorie che vengono in rilievo sono rinvenibili, per le Sezioni Unite, nel combinato disposto degli artt. 238 c.p.p. e 78 disp. att. c.p.p., ovvero, qualora le prove fossero state acquisite con le forme delle intercettazioni di comunicazioni, negli artt. 270 c.p.p. e 78 disp. att. c.p.p.[23].

Bisognerà poi verificare sia se sussistono, nel caso di specie, le condizioni per l'emissione dell'O.E.I., con riguardo al versante della necessarietà e proporzionalità (*infra*, § 5.1.)[24], sia se è stata chiarita la natura dell'attività investigativa sulle piattaforme criptate (*infra*, § 5).

Il secondo tema affrontato attiene alle garanzie che devono governare l'utilizzabilità dei dati trasmessi e, in tale contesto, il quesito che la Corte ha sciolto attiene a eventuali controlli giurisdizionali[25].

Con riferimento a tale quesito, le sentenze "gemelle" sembrano risentire della sentenza della Corte di Giustizia relativa al caso *Encrochat*, nella quale si è precisato che il pubblico ministero figura tra i soggetti che possono costituire un'autorità di emissione dell'O.E.I.

Più nel dettaglio, i giudici di Lussemburgo hanno chiarito che l'autorità di emissione, quando intenda ottenere la trasmissione di prove già in possesso delle competenti autorità dello Stato di esecuzione, non è autorizzata a controllare la regolarità del distinto procedimento con il quale lo Stato membro di esecuzione ha raccolto le prove di cui essa chiede la trasmissione.

Nel trasportare a livello nazionale la prospettiva europea, si rileva come, ai sensi degli artt. 238 e 270 c.p.p., nel caso di circolazione di prove da un procedimento ad un altro, tale autorizzazione preventiva non è necessaria; pertanto, in applicazione del principio di equivalenza, il corrispondente O.E.I. può emessodirettamente dal pubblico ministero.

Principio che per la Corte è valevole anche in riferimento a prove che a livello nazionale richiedono la preventiva autorizzazione del giudice, quali le attività di intercettazione e l'acquisizione di tabulati di traffico telefonico e telematico. Per queste ultime, infatti, il controllo ha operato *ex ante*, in fase di acquisizione da parte giudice nello stato di esecuzione, pertanto non deve più ricorrere in caso di richiesta di O.E.I. da parte del pubblico ministero.

Conclusione che rischia di collidere con un ordinamento nel quale il provvedimento del giudice è necessario per le attività di intercettazioni e per acquisire i tabulati di traffico telefonico e telematico[26] ma – di contro – nessun controllo giurisdizionale viene previsto per compiere un sequestro di dati informatici che attengono alle comunicazioni[27].

Delineate le questioni, le Sezioni Unite approdano a due soluzioni: da un alto, l'utilizzabilitàdei dati comunicativi acquisiti dalle piattaforme criptate; dall'altro, l'esclusione di un controllo giurisdizionale da parte del giudice italiano, salvo che questi rilevi una violazione dei diritti fondamentali. Soluzione che risulta conforme alla consolidata elaborazione giurisprudenziale, in tema di rogatoria internazionale, per la quale l'atto investigativo gode di una presunzione relativa di conformità ai diritti fondamentali, con conseguente onere, gravante sulla difesa, di allegare e provare fatti da cui inferire la violazione di detti diritti fondamentali[28].

4. I frastagliati precedenti nazionali.

Una volta enucleato il principio di diritto espresso dalle Sezioni Unite, sembra imprescindibile analizzare il contesto nel quale si insinua l'intricata *querelle.*

I giudici di legittimità – sollecitati dai difensori degli imputati talvolta per violazione delle norme in materia di intercettazione[29], talaltra per lesione del contraddittorio sulle modalità di apprensione delle *chat* allocate su *server* esteri[30] – sono stati chiamati più volte a decidere sui limiti di impiego processuale dei dati criptati appresi dall'autorità giudiziaria di altri Paesi e acquisiti nei procedimenti nazionali per il tramite dell'O.E.I.

Più nel dettaglio, le Corti si sono trovate ad affrontare la questione da un duplice angolo di visuale: da un lato, sono intervenute per definire il corretto inquadramento giuridico delle attività di acquisizione del contenuto delle *chat* sulle piattaforme criptate e, dall'altro, per determinare le modalità attraverso cui i dati ottenuti all'estero possono transitare nel processo penale.

Con riferimento al primo aspetto, alcune pronunce[31] chiariscono che l'attività di acquisizione e di decifrazione dei dati comunicativi allocati su *server* esteri non possa rientrare nel novero delle intercettazioni informatiche o telematiche *ex* art. 266-*bis* c.p.p., trattandosi invece di documenti informatici pienamente utilizzabili in conformità alle previsioni di cui all'art. 234-*bis* c.p.p., posta l'assenza di contestualità tra la trasmissione della comunicazione e l'atto acquisitivo[32].

In questi casi, a parere della Corte, trova applicazione il dettato di cui all'art. 234-*bis* c.p.p., dal momento che il dato informatico "in chiaro" è una «rappresentazione comunicativa incorporata in una base materiale con metodo digitale».

Secondo un diverso e minoritario orientamento[33], non è sempre possibile applicare il dettato di cui all'art. 234-*bis* c.p.p., dal momento che il ricorso alla norma in esame può ritenersi giustificato esclusivamente nell'ipotesi di acquisizione di dati e documenti informatici – intesi come elementi informativi "dematerializzati" – che preesistono rispetto all'avvio delle indagini.

In quest'ottica, qualora l'attività investigativa si concretizzi nell'apprensione occulta del contenuto archiviato

nel *server* nel corso dell'investigazione, la relativa acquisizione va inquadrata nella disposizione di cui all'art. 254-*bis* c.p.p.; qualora, poi, l'attività consista nella captazione e registrazione del messaggio cifrato nel mentre lo stesso è in transito dall'apparecchio del mittente a quello del destinatario, il mezzo di ricerca della prova più congeniale è quello dell'intercettazione telematica, *ex* art. 266-*bis* c.p.p.[34].

Secondo una diversa impostazione teorica, sostenuta da sole due pronunce[35], l'acquisizione mediante O.E.I. di messaggi scambiati con sistema cifrato è sussumibile nel novero della prova documentale, individuando nell'art. 234 c.p.p., e non nella disposizione successiva, il parametro normativo di riferimento. A parere della Corte, infatti, l'art. 234-*bis* c.p.p. consente l'acquisizione all'estero di documentazione digitale accessibile al pubblico (o con il consenso del titolare del documento, se non in libera disponibilità) senza ricorso alle procedure di collaborazione con lo Stato in cui i documenti sono collocati. Nella specie, invece, i dati sono stati acquisiti all'esito di una attività di collaborazione internazionale.

Nemmeno può farsi ricorso, secondo i giudici, alle previsioni di cui all'art. 266-*bis* c.p.p., posto che «la disciplina delle intercettazioni non è applicabile per l'acquisizione, con ordine europeo di indagine, di specifici "dati freddi", cioè di documenti costituenti l'esito delle comunicazioni memorizzate su *server*, già acquisiti e decriptati dai giudici stranieri, in un loro procedimento autonomamente avviato e concluso».

In una isolata pronuncia[36], la Corte di cassazione – pur ribadendo l'impossibilità di ricorrere tanto alle previsioni di cui all'art. 234-*bis* c.p.p. (non trattandosi di meri documenti e di dati digitali ma di corrispondenza informatica) quanto a quelle di cui all'art. 266-*bis* c.p.p. (stante l'assenza di contestualità tra la trasmissione della comunicazione e l'atto acquisitivo) – chiarisce che il trasferimento dei dati decriptati all'estero soggiace alle previsioni di cui all'art. 270 c.p.p., sussistendone tutti i presupposti legittimanti (ossia la rilevanza e l'indispensabilità per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza).

Con riferimento alle modalità acquisitive, la giurisprudenza sembra concorde nel ritenere che dati informatici acquisiti all'estero possono essere ottenuti e impiegati nel processo penale nazionale per il tramite dell'O.E.I.[37], strumento di cooperazione investigativa cui ricorrere per favorire la circolazione delle prove nei Paesi *intra*-unionali[38].

In quest'ottica, lo scrutinio sulla compatibilità del processo di acquisizione del dato probatorio con il diritto di difesa non risulta frustrato dalla scelta della procura di mettere a disposizione i soli esiti dell'attività svolta

all'estero e non anche il percorso di acquisizione di quei dati[39], posto che l'autorità giudiziaria estera si è resa garante del rispetto delle corrette procedure acquisitive del dato informatico volte ad impedirne l'alterazione[40].

5. Nodi sciolti e grovigli irrisolti.

Al di là di posizioni più o meno critiche nei confronti della decisione in commento, ci si può ritenere soddisfatti di alcune innovative riflessioni di metodo contenute nel ragionamento delle Sezioni Unite, sicuramente "facilitate" dalla completezza espositiva che caratterizza la memoria della Procura generale[41].

Intanto, è meritevole l'attenzione posta dal Procuratore generale, prima, e dalle Sezioni unite, poi, all'uso di nuove tecniche investigative assai efficaci per la repressione del crimine: progredendo, infatti, con straordinaria velocità tanto le tecnologie di captazione – che diventano sofisticate ed invasive – quanto le modalità di elusione delle captazioni – che si affidano all'impenetrabilità degli apparecchi utilizzati, all'inaccessibilità di particolari reti di captazione ovvero all'adozione di sistemi di criptazione dei messaggi scambiati –, risulta imprescindibile ricorrere a nuove metodologie di indagine ad alto potenziale tecnico per penetrare canali criminali di comunicazione o scambio di informazioni utilizzati per la commissione di reati di particolare allarme sociale.

Altrettanto apprezzabile è l'interesse mostrato per l'analisi delle caratteristiche tecniche dell'attività investigativa condotta sui *server* esteri. La suprema Corte coglie, infatti, l'importanza del dato tecnico ai fini della comprensione dei risultati giuridici che dall'utilizzo dello stesso possono derivare. Per troppo tempo il mondo del diritto ha peccato di miopia nel ritenere che l'analisi giuridica potesse prescindere dalla conoscenza tecnico-scientifica che permea molti mezzi di ricerca della prova.

La motivazione (e prima ancora la memoria della Procura generale) chiarisce cosa sono i criptofonini e i sistemi di comunicazione criptati, dà conto della complessa indagine svolta e, nell'evidenziare l'importanza di tali strumenti ai fini investigativi, la Corte ne individua gli enormi rischi in punto di lesione di diritti. La motivazione sottolinea come il loro utilizzo potrebbe dar luogo ad una serie indefinita di atti investigativi *de facto* non autorizzati.

A rigor di onestà, i potenziali rischi sono molti di più e vanno enunciati ai non addetti ai lavori per

comprendere a fondo la portata della lesività di tali tecniche di indagine.

In primis, i giudici sembrano giustificare la trasmigrazione di dati raccolti all'estero nei procedimenti penali nazionali senza definire con chiarezza la categoria probatoria in cui ascrivere l'attività investigativa condotta che continua a rimanere avvolta dal mistero, fluttuando – senza peraltro sovrapporsi – tra differenti istituti processuali più o meno noti al sistema.

Dunque, la Corte sembra disinteressarsi della natura delle attività di indagine che, a monte, avevano consentito di penetrare all'interno delle piattaforme di comunicazione criptate: non è dato sapere in che modo si sia giunti all'acquisizione dei messaggi criptati, se attraverso la captazione di flussi in fase dinamica ovvero mediante l'acquisizione di dati telematici freddi, cioè già archiviati nella memoria del *server,* oppure procedendo ad un'apprensione "*omnibus*".

In una delle due sentenze "gemelle"[42], la Corte sembra qualificare l'attività investigativa richiamando le previsioni di cui agli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p., facendo così presumere che l'attività condotta all'estero sia prova documentale o intercettazione.

Anche in questo caso emergono delle perplessità perché se il riferimento all'art. 270 c.p.p. significa acquisizione del risultato delle intercettazioni disposte in un diverso procedimento (anche se iniziato e concluso all'estero), non si riesce agevolmente a comprendere quali potrebbero essere i verbali di un diverso procedimento ai quali si riferiscono gli artt. 238 c.p.p. e 78 disp. att. c.p.p., posto che potrebbe trattarsi di *chat* acquisite, di verbali e brogliacci di p.g. *ex* art. 268 c.p.p., ma anche di verbali allo stato non conosciuti.

Inoltre, nel qualificare l'attività acquisitiva, non può non rilevare come ci si trovi al cospetto di una situazione tanto innovativa, quanto ibrida, e comunque in bilico tra diverse operazioni investigative, individuabili, per i dati in transito, negli artt. 266 e 266-*bis* c.p.p. mentre, per quelli statici, negli artt. 234, 234-*bis*, 254 c.p.p., coinvolgendo finanche la disciplina in materia dei tabulati telefonici e telematici (art. 132 d.lgs. n. 196 del 2003); attività, queste, che interferiscono con la complessa ed ampia tematica delle garanzie da riservare all'acquisizione dei dati comunicativi[43].

Sotto tale profilo, la questione si intreccia con plurime decisioni che hanno segnato, negli ultimi anni, la complessa tematica delle comunicazioni: in un primo versante, con riguardo all'acquisizione presso il *server*

dei dati esterni delle telecomunicazioni, la giurisprudenza della Corte di Giustizia UE[44] fissa limiti stringenti, in forza del principio di proporzionalità, avendo riguardo al criterio della stretta necessità in relazione ai fini dell'indagine e al controllo giurisdizionale sulla esistenza delle condizioni sostanziali e procedurali per l'accesso ai dati[45].

Sempre la Corte di Giustizia UE[46] – e poi il legislatore italiano[47] – intervengono in tema di tabulati di traffico telefonico e telematico, prevedendo, oltre alla riserva di legge, anche un provvedimento autorizzativo del giudice. Sotto altro profilo, è intervenuta la Corte costituzionale, in tema di tutela della libertà e segretezza della corrispondenza, con la nota sentenza n. 170 del 2023[48], che ha esteso l'ombrello protettivo dell'art. 15 Cost. alla corrispondenza elettronica, anche dopo la sua ricezione da parte del destinatario, almeno fino a quando non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza. In tale scenario, si aggiunge anche la giurisprudenza della Corte EDU, la quale ha ricondotto sotto il cono di protezione dell'art. 8 CEDU (ove pure si fa riferimento alla corrispondenza *tout court*), i messaggi di posta elettronica[49], gli s.m.s.[50] e la messaggistica istantanea inviata e ricevuta tramite internet[51].

Sulla base di tale quadro giurisprudenziale, in ordine alla natura dell'attività di acquisizione delle comunicazioni elettroniche, emerge una perplessità che attiene al *vulnus* di tutele che governa l'assetto normativo interno e, più precisamente, all'assenza di una disciplina che individui limiti e garanzie dell'agire investigativo.

Aspetti che però, anche dopo le sentenze gemelle, restano ancora irrisolti, atteso che non viene chiarita la tassonomia dell'atto investigativo e, nel contempo, si nega la necessità di una autorizzazione preventiva del giudice per acquisire dati comunicativi digitali. Soluzione che, sulla base delle norme oggi vigenti, può apparire condivisibile poiché – allo stato – nessuna norma legittima una riserva di giurisdizione nell'attività di sequestro di dati comunicativi. Ed infatti, la preventiva autorizzazione del giudice ai fini dell'emissione dell'O.E.I. è necessaria, in forza del criterio di equivalenza, solo per le intercettazioni, non anche per il sequestro.

Il risultato, però, è un "cortocircuito" sistemico: per le intercettazioni e per l'acquisizione dei dati esterni del traffico telefonico e telematico è necessario il preventivo provvedimento autorizzativo dell'organo della giurisdizione, mentre per il sequestro dei comunicativi è sufficiente un semplice provvedimento del p.m.

A ben vedere, la soluzione prescelta dalla Corte svela la fragilità dell'assetto normativo che governa la materia e – più ampiamente – l'inconsistenza di una disciplina, quale quella ad oggi esistente, che non appare idonea a disciplinare la versatilità della comunicazione, oggi estremamente potenziata dalla Rete.

Soprattutto non convince la semplicità con cui il Supremo Collegio ha consentito il ricorso all'O.E.I. ritenendo soddisfatti sia le condizioni per l'emissione, sia il complesso di regole che garantiscono l'utilizzabilità probatoria dei dati raccolti.

5.1. Le condizioni per l'emissione dell'O.E.I.

In primo luogo, si osserva come non sembrano sussistere nel caso di specie le condizioni per l'emissione dell'O.E.I., nè sul versante della "necessarietà", nè sotto il profilo della "equivalenza".

Con riferimento al primo requisito, occorre precisare che, secondo quanto previsto dagli artt. 1, § 4 e 6, § 1 lett. *a,* Direttiva 2014/41/UE e dall'art. 7, d.lgs. n. 108 del 2017, l'Ordine è attivabile solo quando proporzionato e necessario per il procedimento penale interno allo Stato richiedente.

Lo scopo è evitare che singole autorità giudiziarie possano abusarne quando gli stessi atti non sarebbero giustificati nell'ordinamento interno per la tipologia di procedimento, entità della pena eventualmente da irrogare e rilevanza dei fatti[52].

Proprio su questo aspetto si aprono scenari a dir poco inquietanti: nel caso di specie, infatti, una volta "bucato" il *server* all'estero, l'acquisizione non ha ad oggetto esclusivamente le comunicazioni e le conversazioni ritenute potenzialmente rilevanti nel procedimento ove l'attività investigativa è stata "ordinata" ma anche tutti i flussi comunicativi (in atto o giacenti sulla piattaforma) intercorsi tra gli abbonati al servizio.

Di qui, «cadute le barriere protettive, davanti agli investigatori si apre quindi una distesa sterminata di materiale probatorio acquisito attraverso il monitoraggio di una moltitudine di utenze di cui, nel provvedimento autorizzativo, non era però stata fatta alcuna menzione e rispetto alle quali, dunque, non era stato compiuto il doveroso vaglio circa la necessità di sacrificarne la riservatezza»[53].

Pur non trattandosi di attività investigative rientranti nel *genus* della c.d. sorveglianza di massa[54], è evidente

che l'acquisizione indiscriminata di tutti i dati giacenti o transitanti su un sistema non soddisfa il requisito della necessità e proporzione; conseguentemente, fino a quando dal punto di vista strettamente tecnico non sarà possibile limitare il controllo solo ai dati rilevanti per il procedimento per cui è richiesta l'acquisizione, le apprensioni su larga scala non sembrano poter trovare cittadinanza nell'ordinamento giuridico nazionale[55].

Come anche precisato, «[S]e, la legge consente di violare la riservatezza di quelle comunicazioni rispetto alle quali sussistono determinati presupposti giustificativi, non si vede come un giudice possa autorizzare un'attività di intercettazione (telematica) nella consapevolezza che, così facendo, sta automaticamente consentendo la captazione a tappeto di tutti i flussi comunicativi veicolati dal *server* infettato e tutto questo in assenza dei necessari requisiti stabiliti dalla legge»[56].

Anche con riferimento al principio di equivalenza si evidenziano criticità.

Come è noto, ai sensi dell'art. 6, § 1, lett. *b,* Direttiva 2014/41/UE, l'atto di indagine oggetto dell'O.E.I. deve essere compiuto nel rispetto delle stesse condizioni che si sarebbero attuate se fosse stato realizzato nello stato richiedente o, come specificamente prevede la direttiva, «alle stesse condizioni in un caso analogo».

Lo scopo è evitare che l'autorità giudiziaria possa aggirare le regole di acquisizione probatoria interna chiedendo ad altre autorità di procedere – appunto – attraverso diverse modalità[57].

Di conseguenza, il problema della qualificazione giuridica dell'attività svolta all'estero si pone come essenziale perché da essa dipende la validità degli O.E.I. emessi in Italia[58].

Circoscrivendo l'analisi all'ipotesi in cui l'azione acquisitiva di messaggistica sia "*live*" – e, dunque, la captazione estera sia avvenuta nel momento stesso in cui la comunicazione transita nell'etere digitale –, si ricorre (a dire della Corte) alla categoria delle intercettazioni telematiche, regolate dall'art. 266-*bis* c.p.p.[59], che, come noto, hanno ad oggetto un «flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi», ossia tra *computer* collegati tra loro in Rete, via *modem*, via radio (se i dispositivi sono connessi con tecnologia *wireless*) o con qualsiasi altra forma di interconnessione.

Sicuramente, sotto il profilo tecnico-operativo, l'accesso ad un *server* per captare comunicazioni in atto

potrebbe essere ricompreso nell'alveo delle intercettazioni telematiche, venendo in rilievo il carattere della contestualità della captazione di un flusso comunicativo tra sistemi collegati in Rete.

Tuttavia, pur volendo assimilare tali forme captative alle intercettazioni "classiche", non si può negare che le prime siano caratterizzate da significative peculiarità, risultando molto più intrusive per chi vi è sottoposto e, al contempo, assai più efficaci per i loro esiti istruttori.

Si converrà che un conto è captare flussi telematici intercorrenti tra due o più sistemi oggetto di intercettazione, ben altro è accedere direttamente al *server* sul quale transitano tutte le comunicazioni di tutti gli utenti che utilizzano quel servizio.

Seppur si arrivasse a ritenere – sulla scorta dell'interpretazione "evolutiva" del dettato normativo suggerita dalla giurisprudenza della Corte EDU[60] – che tale captazione rappresenti un'evoluzione dell'intercettazione telematica "tradizionale" avente ad oggetto flussi comunicativi transitanti su un nuovo "sistema informatico" (ossia il *server*) "monitorato" perché è sul nuovo ambiente virtuale che (presumibilmente) si consuma il fatto di reato, non va dimenticato che l'attività svolta dall'autorità giudiziaria francese rappresenta un'attività "ibrida", un misto tra intercettazione, sequestro, acquisizione di documenti o di corrispondenza[61], oltre che ad un'intrusione a fini esplorativi.

L'approdo sembra trovare conferme negli atti di indagine francesi che richiamano sia le norme in materia di intercettazione "tradizionale" (artt. 100 ss. c.p.p. francese) sia le previsioni "speciali", in materia di captazione e acquisizione delle comunicazioni attraverso nuove tecniche di indagine (art. 706.95 c.p.p. francese), giungendo finanche ad includere le previsioni in materia di controllo continuativo e occulto delle comunicazioni che consentono di registrare, conservare, apprendere e trasmettere dati informatici (art. 706.102.1 c.p.p. francese)[62].

Che non si tratta di pure intercettazioni o di mere acquisizioni documentali lo si evince anche dall'O.E.I. con cui l'autorità italiana procede ad «acquisire ogni eventuale informazione in possesso in ordine ai *target* riportati, anche con riferimento a tutte le comunicazioni in entrata/uscita, immagini, *file* audio e video»[63].

E non è tanto la realizzazione delle azioni investigative plurime e combinate a destare perplessità quanto l'inesistenza di una normativa in materia che specifichi le potenzialità, i casi e i limiti delle attività in

questione o, meglio, le modalità con cui esse vengono svolte nel pieno rispetto del principio di legalità[64].

Da ultimo, merita di essere sottolineato anche un altro aspetto relativo al *modus procedendi* dell'autorità francese per acquisire i dati dal *server* criptato; aspetto che finisce per allontanare definitivamente l'attività investigativa *de qua* dagli atti di indagine esperibili in Italia.

Come si è avuto modo di anticipare, gli investigatori francesi si servono di un captatore informatico (tipo *Trojan*) per acquisire gli algoritmi di decodifica dei dati criptati.

A ben riflettere, il *virus* informatico, nell'ordinamento nazionale, può essere ammesso solo per scopi captativi e non certo per accedere a sistemi con scopi esplorativi[65]; il che testimonia l'illegittimità dell'ordine italiano a fronte del *deficit* di legalità dell'acquisizione della messaggistica oggetto della richiesta di trasmissione[66].

5.2. L'utilizzabilità dei dati raccolti all'estero nei procedimenti interni.

Altro aspetto che appare strettamente connesso alle questioni sopra analizzate, attiene alla utilizzabilità degli atti acquisiti mediante tecniche investigative che permettono di accedere ad informazioni digitali "da remoto"[67] e alla eventuale verifica dei presupposti di ammissibilità vagliati nel rispetto della *lex fori*[68].

Proprio per questo, il versante più complesso della questione rimane – ancora una volta – strettamente legato alla fisionomia dell'agire investigativo che, come detto sopra, fluttua tra plurimi atti di indagine (intercettazioni, acquisizione dati esteriori delle comunicazioni, sequestro comunicazioni) ed impatta comunque sui dati comunicativi, mirando ad apprendere messaggistica sia "*live*", sia giacente nella piattaforma.

Per tale ragione, appare innegabile che l'attività deve essere circondata da cautele in grado di assicurare legalità e proporzionalità, nel rispetto dei diritti fondamentali[69].

Da qui, a cascata, le questioni si spostano sul conseguente coinvolgimento dell'organo giurisdizionale e sull'utilizzabilità dei dati nei procedimenti interni.

In questa prospettiva, seppure – ai fini dell'emissione dell'O.E.I. – non è necessaria l'autorizzazione preventiva di un giudice, sotto altro versante, non sembra che si possa prescindere, nello Stato di emissione, da un vaglio giurisdizionale *tout court*[70]. Più precisamente, lo stato di emissione – indipendentemente dai rimedi esperibili in quello di esecuzione – deve consentire alla difesa di contestare, attraverso un mezzo di impugnazione appropriato, le ragioni di merito dell'emissione dell'ordine europeo di indagine[71].

Le Sezioni Unite, infatti, ritengono che l'assenza di un controllo giurisdizionale preventivo sulle condizioni di ammissibilità della prova,non preclude al giudice nazionaledi valutare, *ex post*, se vi siano i presupposti per ammettere ed utilizzare tali prove e, tale controllo equivale ad assicurare il diritto all'impugnazione nello Stato di emissione[72]. Si assiste così ad una sorta di equiparazione tra il mezzo di impugnazione e il vaglio di ammissibilità operato dal giudice dello Stato di emissione chiamato ad utilizzare le prove.

Quello che però non viene chiarito attiene ai limiti di tale controllo e ai criteri che devono governare l'utilizzabilità delle prove acquisite con l'emissione dell'O.E.I., atteso che il parametro valutativo, enucleato dall'art.14, § 7, direttiva 2014/41/UE, richiede il rispetto dei diritti della difesa e delle garanzie del giusto processo[73], ma non anche l'osservanza, da parte dello Stato di esecuzione, delledisposizioni previste dall'ordinamento giuridico interno in tema di formazione ed acquisizione di tali atti.

In altre parole, «la portata delle limitazioni all'uso dei contributi irritualmente acquisiti mediante l'O.E.I. è resa particolarmente ardua nel nostro ordinamento dal silenzio serbato sul punto dalla disciplina di recepimento interna, che obbliga a dirimere l'interrogativo ricorrendo alle categorie generali»[74].

In tale scenario si innestano plurime vedute che portano, alcuni, ad intravedere, quando l'ordine è illegittimo, la sussistenza di patologie che si riflettono sul procedimento penale di destinazione, decretando la inutilizzabilità della prova[75]; altri, a decretare l'irrilevanza delle irregolarità nella raccolta transfrontaliera, essendo questa una violazione non espressamente sanzionate da inutilizzabilità[76].

In tale complesso scenario, la Corte garantisce un controllo giurisdizionale postumo sui limiti di utilizzabilità degli esiti investigativi raccolti all'estero, nel pieno rispetto dei diritti fondamentati, ma non chiarisce come l'atto investigativo condotto su piattaforme criptate – che ha comportato l'acquisizione generalizzata ed indifferenziata di dati di massa – sia conforme alle regole relative all'ammissibilità e alla valutazione di

prove[77] e, più ampiamente, rispetti il principio di legalità della prova[78].

A ben riflettere, la criticità attiene proprio all'assenza di un controllo sull'ammissibilità e sulla utilizzazione della prova conformi alla legislazione italiana[79], controllo che non può prescindere da una verifica sul rispetto dei requisiti previsti a pena di inutilizzabilità dagli artt. 270 e 271 c.p.p., tra i quali figura l'esistenza di una autorizzazione rilasciata dall'organo di garanzia.

Alla luce di ciò, si concorda con chi ha intravisto la violazione dall'art. 8 della C.e.d.u. e dagli artt. 7 e 8 della Carta di Nizza in forza del mancato coinvolgimento di un'autorità sufficientemente indipendente nel procedimento di autorizzazione del controllo[80].

A tali considerazioni deve aggiungersi un ulteriore aspetto, attinente al controllo – operato dal giudice e dalle parti – sulle modalità di raccolta delle prove da parte dell'autorità straniera.Più precisamente, il problema coinvolge la peculiarità delle operazioni investigative condotte non solo con elevate tecniche informatiche, ma anche utilizzando specifici algoritmici. Ed appare innegabile come quest'ultimo, impiegato per decrittare i flussi comunicativi captati o comunque sequestrati all'interno del *server* debba essere messo a disposizione delle parti congiuntamente alla stringa informatica non ancora decriptata. Il tema è infatti il diritto dell'accusato a confrontarsi con l'accusatore (in tal caso le *chat*) al fine di verificare la piena corrispondenza tra il testo originario (la stringa informatica) e il testo intellegibile introdotto come prova nel giudizio[81].

La necessità di tale *discovery* rappresenta il fulcro del diritto di difesa e del contraddittorio al fine di consentire all'interessato di interloquire sulle modalità di acquisizione delle prove digitali. Ma, al contrario, si può anche sostenere come la conoscenza delle tecniche di indagine può interferire con esigenze di sicurezza nazionale, tali da giustificare l'apposizione del segreto di Stato.

In tale contesto vengono in rilievo le possibili conseguenze di un mancato accesso all'algoritmo.

Potrebbe derivare una nullità a regime intermedio – *ex* art. 187, comma 1, lett. c), c.p.p., per violazione del diritto di difesa; oppure, alcuna patologia potrebbe investire gli atti, non essendo rinvenibile nel nostro sistema un divieto probatorio volto a sanzionare questo tipo di situazioni.

Anche tale questione, affrontata dalle Sezioni Unite, si presta ad osservazioni critiche in quanto si è ritenuto che l'impossibilità per la difesa di conoscere gli algoritmi utilizzati per la decriptazione delle comunicazioni «non determina, almeno in linea di principio, una violazione di diritti fondamentali».

Scelta che, tuttavia, pare contrastare anche con la sentenza della Corte di Giustizia nel caso *Encrochat*[82], nella parte in cui impone al giudice penale nazionale di espungere, nell'ambito di un procedimento penale, informazioni ed elementi di prova se l'imputato non è in grado di svolgere efficacemente le proprie osservazioni su tali informazioni ed elementi di prova e questi ultimi siano idonei ad influire in modo preponderante sulla valutazione dei fatti[83].

6. La necessaria tipizzazione delle "nuove" indagini: un appello al legislatore.

Alla luce delle considerazioni svolte possono trarsi alcune prime considerazioni sistematiche.

Intanto, dal quadro prospettato emerge che la questione non è di facile composizione in considerazione del forte impatto sui principi costituzionali e sulle categorie probatorie del processo penale che difficilmente riescono a reggere l'urto della modernità.

Più precisamente, il bilanciamento tra aspettative di riserbo e ingerenze investigative del potere pubblico deve confrontarsi con plurimi profili: *in primis*,con l'era tecnologica che stiamo vivendo, nella quale le indagini digitali svolgono un ruolo centrale nella lotta contro il crimine.

In secondo luogo, non può non rilevare come la dimensione di dette indagini stia mutando a fronte di una criminalità che agisce sempre di più a livello globale; infine, le attività investigative si orientano, ormai frequentemente, verso l'acquisizione massiccia di dati di ogni tipo.

In tale scenario, le investigazioni digitali impongono al giurista l'onere di ricercare, costantemente, quel difficile punto di equilibrio tra tecnica e diritto, nel rispetto delle garanzie, del principio di proporzionalità e di legalità.

Temi tanto attuali quanto cogenti, che hanno coinvolto, ad esempio, le attività investigative sui dati di

geolocalizzazione[84], sui dati comunicativi[85], ovvero – in un'ottica di prospettive di riforma – sulla più ampia questione del sequestro dei dispositivi elettronici[86].

Ciò posto, conviene dirlo senza ritrosie, l'attività di acquisizione e conservazione di *big data* raccolti all'estero travalica i confini tassonomici dello schema normativo dei tradizionali mezzi investigativi, rischiando di trasformarsi in una sorveglianza perpetua ritenuta illegale perché in contrasto con le norme costituzionali (artt. 14 e 15 Cost.) e convenzionali (artt. 6 e 8 Cedu)[87].

Se da un lato risulta evidente l'altissimo potenziale probatorio dell'attività investigativa in esame, sotto altro profilo, il substrato normativo attualmente in vigore (l. n. 48 del 2008)[88], appare non solo inconsistente ed obsoleto[89], ma anche «scarsamente congruente rispetto alle potenzialità espressive dell'agire investigativo»[90], facendo sbilanciare il sistema sulle esigenze dell'accertamento, a discapito dei diritti di difesa e di riservatezza.

Nonostante le visibili difficoltà, l'interprete non può arrendersi all'idea che le nuove indagini finiscano per rimanere improficue, dovendo compiere lo sforzo ermeneutico per adeguare la disciplina vigente alle sfide dell'era moderna. Dunque, posta l'irrinunciabilità degli strumenti offerti dalla tecnologia, occorre ragionare su soluzioni alternative funzionali ad offrire un compromesso tra le esigenze investigative e la tutela delle prerogative individuali.

In primo luogo, sembra indispensabile prevedere una regolamentazione dei servizi di comunicazione cifrata attraverso l'aggiornamento del Codice delle comunicazioni elettroniche[91]: l'obiettivo è fornire un elenco di piattaforme criptate autorizzate a rilasciare il servizio, i cui gestori si impegnano a collaborare con le autorità di *law enforcement* per sviluppare soluzioni che permettano di individuare e bloccare gli utenti che utilizzano le piattaforme per commettere reati.

Inoltre, i peculiari connotati dell'ingerenza dovrebbero spingere il legislatore ad inquadrare il trattamento normativo da riservare alle più evolute misure di sorveglianza investigativa e, in una prospettiva sovranazionale, sarebbe auspicabile la predisposizione di una normativa uniforme sulla circolazione dei dati digitali comunicativi (sia "freddi" che "caldi"), superando le incertezze poste dalla confusa disciplina in materia di O.E.I.

In questo senso, sarebbe indispensabile l'introduzione di una norma costruita sul modello del dettato di cui art. 270 c.p.p. italiano che individui limiti e prospettive comuni per acquisire risultati di captazioni in Stati diversi da quelle per cui sono state autorizzate, la cui cornice dovrebbe strutturarsi sull'individuazione dei principi a cui corredare le fasi del procedimento probatorio, a partire dalla raccolta degli elementi. Nel dettaglio, appare doverosa la previsione di casi, modi e limiti entro cui perimetrare l'agire investigativo, appendo necessaria una disposizione normativa che soddisfi nell'*an* e nel *quomodo* la riserva di legge e di giurisdizione[92]. Diversamente detto, «perché non si possa abusare del potere, occorre che il potere arresti il potere»[93]. Nel contempo, va rafforzato – ove possibile – il ruolo della difesa già in fase investigativa.

In ultima analisi, occorre soffermarsi su un aspetto che, pur non rappresentano un'emergenza contingente, potrebbe destare enormi preoccupazioni nel prossimo futuro. Se è vero che ad oggi l'Italia ha svolto un ruolo di "osservatore passivo" rispetto alle attività condotte da altri Paesi, non è inverosimile immaginare che, di qui a qualche tempo, le autorità nazionali si troveranno a ricoprire il ruolo di "attori" nelle investigazioni sulle piattaforme criptate, svolgendo "in prima persona" indagini su *server* magari ubicati in territorio nazionale.

Non essendo ipotizzabile lasciare alla disponibilità degli inquirenti la scelta di ricorrere indiscriminatamente a nuovi strumenti investigativi e nemmeno legittimare il loro impiego in sede giurisprudenziale attraverso interpretazioni estensive in una materia governata da un rigido principio di legalità, si avverte l'esigenza di un intervento repentino del legislatore, chiamato a tipizzare il complesso di attività esperibili attraverso inedite tecniche investigative[94].

In quest'ottica, si potrebbe propendere per l'introduzione di un nuovo mezzo di ricerca della prova (accesso e acquisizione di *big data* su sistemi informatici o telematici, potrebbe chiamarsi) per regolare le attività di accesso, osservazione e acquisizione di dati e informazioni rinvenuti sui nuovi spazi virtuali: in questi casi, non sarebbe tipizzato lo strumento con cui condurre le indagini informatiche, quanto piuttosto le regole cui ricorrere ogni qual volta si proceda ad attività di sorveglianza occulta e continuativa da remoto, predisponendo le garanzie fondamentali che devono essere sempre riconosciute all'indagato e ai soggetti terzi occasionalmente coinvolti, a prescindere dalla tecnica investigativa impiegata.

In altre parole, l'obiettivo potrebbe essere quello di introdurre una nuova categoria probatoria con la quale verrebbero individuati i "casi" e i "modi" dell'ingerenza nella sfera privata degli individui, così da ritenere il sacrificio dei diritti inviolabili assolutamente rispettoso del principio di stretta legalità e del principio di proporzione.

[1] Per un'analisi dei precedenti, si rinvia a § 4.

[2] Cass., Sez. VI, 15 gennaio 2024, n. 2329, in *Sist. pen.,* 11 dicembre 2023; Cass., Sez. III, 2 novembre 2023, n. 47798, *ivi,* 11 dicembre 2023.

[3] Cass., Sez. Un., 29 febbraio 2024, informazione provvisoria n. 3 con riferimento all'ordinanza di rimessione n. 47798/2023; Cass., Sez. Un., 29 febbraio 2024, informazione provvisoria n. 4 del 2024, riferita all'ordinanza di rimessione n. 2329/2024.

[4] Ci si riferisce alla sentenza della Corte giust. UE, Grande Camera, 30 aprile 2024, *M.N.*, C-670/22. La Corte, pur attribuendo al p.m. il potere di adottare un O.E.I. teso a ottenere la trasmissione delle prove già in possesso delle autorità competenti nello Stato di esecuzione, in ossequio alle previsioni di cui all'art. 6, § 1 della Direttiva 2014/41/UE, chiarisce che «l'art. 14, § 7 della Direttiva [...] deve essere interpretato nel senso che esso impone al giudice penale nazionale di espungere [...] informazioni ed elementi di prova se [la persona sottoposta alle indagini] non è in grado di svolgere efficacemente le proprie osservazioni su informazioni ed elementi di prova e questi ultimi siano idonei ad influire in modo preponderante sulla valutazione dei fatti».. Sul punto, per tutti, RAZZI-SPIEZIA, *Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del* count-down *italiano,* in *Sist. pen.,* 26 febbraio 2024. Sul punto, si veda pure Corte giust. UE, Grande Camera, 4 ottobre 2024, *CG,* C-548/21, per cui l'accesso degli inquirenti ai dati contenuti in un telefono cellulare non è una misura da riservare necessariamente alla lotta contro i reati gravi. Deve, però, essere disposta da un giudice (o da un'autorità indipendente), con provvedimento motivato, e resta soggetta al principio di proporzionalità. Così, la Corte di giustizia ha interpretato gli artt. 4, par. 1, 13 e 54 della direttiva 2016/680/UE, individuando un punto di equilibrio tra le esigenze di accertamento del reato e il diritto alla riservatezza dei dati personali e, più in generale, alla libertà di comunicazione dei privati. D'altra parte, parallelamente a quanto accaduto negli Stati nei quali è rifluito il materiale probatorio francese, sono stati presentati alcuni ricorsi individuali alla Corte di Strasburgo in relazione ad analoghi trasferimenti di materiale investigativo. Cfr. Corte EDU, *A. L. c. Francia*, n. 44715/20; Corte EDU, *E. J. c. Francia*, n. 47930/21.

[5] Cass., Sez. Un., 14 giugno 2024, n. 23755, in *C.E.D. Cass.,* n. 286573; Cass., Sez. Un., 14 giugno 2024, n.

23756, non massimata. Per i primi commenti, si vedano, DANIELE, *La mappa del controllo giurisdizionale quando l'OEI ha ad oggetto prove già in possesso dell'autorità straniera,* in *Sist. pen.,* 17 luglio 2024; GUAGLIARDI, *Utilizzo nel processo penale di messaggi criptati ottenuti tramite una operazione di* hacking *massiva all'estero e acquisiti in Italia tramite Ordine Europeo di Indagine. Il fine giustifica i mezzi?,* in *Giur. pen.,* 2024, 6, 1; PIGNATA, *Le Sezioni unite sull'utilizzabilità della messaggistica criptata acquisita mediante ordine europeo di indagine,* in *Penale. Diritto e procedura,* 1 luglio 2024; SPANGHER, *Le Sezioni Unite precisano le condizioni di utilizzabilità della messaggistica dei criptofonini,* in *Dir. e giust.,* 18 giugno 2024; ID., *Criptofonini: le sentenze delle Sezioni Unite,* in *Giust. insieme,* 20 giugno 2024.

[6] Dello stesso avviso DANIELE, *La mappa del controllo giurisdizionale quando l'OEI ha ad oggetto prove già in possesso dell'autorità straniera,* cit., 3.

[7] Per un approfondimento sugli aspetti tecnici, si vedano CURTOTTI, RIZZI, NOCERINO, RUSSITTO, GILIBERTI, SCARPA, *Piattaforme criptate e prove penali,* in *Sist. pen.,* 2023, 6, 173.

[8] *Encrochat* era una Rete di comunicazioni e un fornitore di servizi con sede in Europa che offriva *smartphone* modificati consentendo comunicazioni crittografate tra gli abbonati (circa 60 mila utenti). Si trattava di un *App* di messaggistica basata su OTR che instradava le conversazioni attraverso un *server* centrale con sede in Francia, *EncroTalk*, un servizio di chiamate vocali basato su ZRTP e *EncroNote*s, che consentiva agli utenti di scrivere note private crittografate. Il servizio di messaggistica crittografata *EncroChat* e i relativi telefoni personalizzati sono stati scoperti dalla gendarmeria francese nel 2017 che, poco dopo, ha provveduto a disattivare la piattaforma.

[9] *Sky Global* era una rete di comunicazioni e un fornitore di servizi con sede a Vancouver, in Canada: uno dei suoi prodotti più importanti era l'applicazione di messaggistica sicura *Sky Ecc* e i criptotelefoni. nel 2021 erano oltre 171.000 gli apparati registrati, principalmente in Europa, Nord America, diversi Paesi del Centro e Sud America – principalmente Colombia – e Medio Oriente. Un quarto degli utenti attivi si trovava in Belgio (6.000) e nei Paesi Bassi (12.000). Una delle sue caratteristiche era l'autodistruzione dei messaggi dopo un periodo di scadenza definito dall'utente. Il 9 marzo 2021 Francia, Belgio ed Olanda, attraverso un'attività di indagine svolta a seguito della costituzione, sul canale giudiziario, di una squadra investigativa comune, sono riusciti a violare i *server* sui quali sono conservate le comunicazioni.

[10] Si pensi, solo per citarne alcuni, ad *Ennetcom, Exclu, Silent phone, Zphone*, *X1 e X1 black* della *Secure Group* e le piattaforme dall'azienda *Sikur*.

[11] Sui dettagli dell'indagine, per tutti, PROCURA GENERALE DELLA CORTE DI CASSAZIONE, *Memoria per l'udienza delle Sezioni Unite penali del 29 febbraio 2024,* disponibile su *Sist. pen.,* 1 marzo 2024.

[12] Utilizza le espressioni "sentenze gemelle" e "sentenza cugina", DANIELE, *Le "sentenze gemelle" delle Sezioni Unite sui criptofonini*, in *Sist. pen.*, 17 luglio 2024.

[13] Corte giust. UE, 30 aprile 2024, *M.N.*, cit. Sul tema, si veda pure Corte giust. UE, 4 ottobre 2024, *CG,* cit.

[14] Sul tema, NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, 3. Sul tema anche, CAIANIELLO, *Diritti, libertà e garanzie sostanziali e processuali*, in, *Introduzione al diritto penale europeo. Fonti, metodi, istituti, casi*, di Manes, Caianiello Torino, 2020, 285; FERRAJOLI, *Costituzionalismo principialista e costituzionalismo garantista*, in *Giur. cost.*, 2010, 2781.

[15] Per un esame delle questioni rimesse alle Sezioni unite e del delicato tema della sicurezza globale, SPANGHER, *Criptofonini: sono "in gioco" diritti fondamentali*, in *Cass. pen.*, 2024, 173.

[16] Analizza tale aspetto, NOCERINO, *Ancora in tema di criptofonini: nuovi arresti giurisprudneziali in attesa delle Sezioni unite*, in *Questa rivista*, 29 novembre 2023; SPANGHER, *Chat. Saranno le Sezioni Unite a decriptare le questioni giuridiche*, in *Giustizia insieme*, 13 novembre 2023.

[17] Tale inquadramento viene proposta, tra le molte, da Cass., Sez. III, 19 ottobre 2023, n. 47201, in *C.E.D. Cass.*, n. 285350.

[18] Cfr., LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate nella fucina dell'ordine europeo di indagine penale*, in *Cass. pen.*, 2024, 182.

[19] DANIELE, *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite*, in *Sist. pen.,* 11 dicembre 2023.

[20] DANIELE, *Ordine europeo di indagine penale*, cit., 3.

[21] Per un approfondimento, CAIANELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Proc. pen. giust*., 2015, 3, 5-6.

[22] «Al riguardo, è stato premesso che l'ordine europeo d'indagine - disciplinato dal d.lgs. 27 giugno 2017, n. 108, emanato per dare attuazione alla direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 - può anche essere emesso per ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione (art. 1, par. 1, della direttiva), proprio come è avvenuto nella specie, perché il provvedimento del pubblico ministero italiano ha avuto ad oggetto l'acquisizione degli esiti documentali di attività d'indagine precedentemente svolta dall'autorità francese»; PROCURA GENERALE DELLA CORTE DI CASSAZIONE, *Memoria per l'udienza delle Sezioni Unite penali del 29 febbraio 2024,* disponibile su *Sist. pen.,* 1° marzo 2024, 16.

[23] Sull'utilizzabilità degli esiti delle intercettazioni nel procedimento diverso, con riferimento alla disciplina vigente per effetto delle modifiche recate dalla L. 9 ottobre 2023, n. 137, su tutte, Cass., Sez. I, 14 novembre 2023, n. 48622, in *C.E.D. Cass.*, n. 2855579.

[24] Sul tema, LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate*, cit., 182.

[25] Il quesito posto alle Sezioni unite è stato: "se per l'emissione di un O.E.I. finalizzato all'acquisizione di comunicazioni criptate già autonomamente raccolte all'estero, sia necessaria l'autorizzazione preventiva di un giudice dello Stato di emissione".

[26] Sulla l. 23 novembre 2021, n. 178, che introduce una doppia riserva in materia di acquisizione dei tabulati di traffico telefonico e telematico si rinvia a DEMARTIS, *La nuova disciplina sui tabulati: un completo adeguamento agli standard europei?*, in *Dir. pen. proc.*, 2022, 299; DINACCI, *L'acquisizione dei tabulati telefonici*

tra anamnesi, diagnosi e terapia: luci europee e ombre legislative, in *Proc. pen. giust.*, 2022, 2, 301; nonché, volendo, MURRO, *Dubbi di legittimità costituzionale e problemi di inquadramento sistematico della nuova disciplina dei tabulati*, in *Cass. pen.*, 2022, 2440.

[27] DANIELE, *Ordine europeo di indagine penale*, cit.

[28] Tra le molte, Cass., Sez. II, 22 dicembre 2016, n. 2173, in *C.E.D. Cass.*, n. 269000, dove si precisa che l'unico limite all'acquisizione di un atto compiuto all'estero è la violazione dei diritti fondamentali dell'ordinamento giuridico italiano e del diritto di difesa. Nel contempo, come chiarito dalla Corte di Giustizia, l'impiego dell'O.E.I., ai fini della trasmissione di prove già autonomamente raccolte all'estero, non può avere l'effetto di eludere le condizioni previste dalla *lex fori*; così, DANIELE, *Le "sentenze gemelle" sui criptofonini*, cit. L'Autore precisa che se da un lato rivive il criterio di "*no inquiry*" nei confronti delle attività istruttorie compiute negli altri Stati; sotto altro aspetto, c'è il pericolo di prassi eccessivamente lassiste, ovvero il rischio «che si consolidi, l'idea per cui le prove già autonomamente raccolte all'estero sulla base della *lex loci* potrebbero essere automaticamente ed acriticamente recepite nel nostro sistema, fidandosi ciecamente dell'operato delle autorità straniere».

[29] Cass., Sez. IV, 5 aprile 2023, n. 16347, in *C.E.D. Cass.,* n. 284563; Cass., Sez. I, 1 luglio 2022, n. 34059, non massimata; Cass., Sez. I, 13 ottobre 2022, n. 6364, in *Cass. pen.,* 2023, 2786, con nota di NOCERINO, *L'acquisizione della messaggistica su sistemi criptati: intercettazioni o prova documentale?.*

[30] Cass., Sez. VI, 25 ottobre 2022, n. 48330, in *C.E.D. Cass.,* n. 284027.

[31] Cass., Sez. IV, 5 aprile 2023, n. 16347, cit.; Cass., Sez. I, 13 gennaio 2023, n. 19082, in *C.E.D. Cass.,* n. 284440; Cass., Sez. I, 13 ottobre 2022, n. 6364, cit.; Cass., Sez. I, 1 luglio 2022, n. 34059, cit.

[32] Non è superflua la precisazione per cui i dati sono ubicati in uno Stato estero (ossia la Francia) e sono "di proprietà" dello Stato che presta il proprio consenso all'acquisizione degli stessi.

[33] Cfr. Cass., Sez. VI, 26 ottobre 2023, n. 44154, in *Cass. pen.,* 2024, 173, con nota di SPANGHER, *L'acquisizione all'estero di comunicazioni criptate nella fucina dell'ordine europeo di indagine penale*; Cass., Sez. VI, 26 ottobre

2023, n. 44155, *ivi,* 2024, 162, con commenti di LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali* criptate, cit.; nonchè SPANGHER, *Criptofonini: sono "in gioco" diritti fondamentali*, cit.

[34] Tale differenza è stata sottolineata, tra le altre, anche da Cass., Sez. IV, 15 ottobre 2019, n. 49896, in *C.E.D. Cass.*, n. 277949; Cass., Sez. III, 26 settembre 2019, n. 47557, *ivi*, n. 277990.

[35] Cass., Sez. VI, 26 ottobre 2023, n. 46833, in *C.E.D. Cass.,* n. 285543; Cass., Sez. VI, 27 settembre 2023, n. 46482, *ivi,* n. 285363.

[36] Cass., Sez. VI, 11 ottobre 2023, n. 48838, in *C.E.D. Cass.*, n. 285599.

[37] Cass., Sez. VI, 25 ottobre 2022, n. 48330, cit.; Cass., Sez. I, 13 ottobre 2022, n. 6364, cit.

[38] Sui rapporti tra O.E.I. e acquisizione di *chat* decriptate all'estero, per tutti, DANIELE, *Ordine europeo di indagine penale e comunicazioni criptate: il caso* Sky ECC/Encrochat *in attesa delle Sezioni Unite*, in *Sist. pen.,* 11 dicembre 2023.

[39] Nello specifico la difesa lamenta che il p.m. ha messo a disposizione della difesa solo gli esiti dell'attività di polizia svolta, senza condividere il percorso (ovvero gli atti di indagine) che ha portato all'acquisizione delle *chat* decriptate e, in particolare, la documentazione di *Europol* (con i file decriptati) con l'indicazione precisa delle modalità di acquisizione dei dati nel *server* e gli annessi verbali di polizia. Cfr. Cass., Sez. VI, 25 ottobre 2022, n. 48330, cit.

[40] In una isolata pronuncia (Cass., Sez. IV, 15 luglio 2022, in. 32915, in *Giur. pen.,* con nota di BARBIERI, *I limiti di utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine*), la Corte sostiene che l'acquisizione del dato probatorio (le *chat* decriptate) è inutilizzabile, poiché non è stato rispettato il diritto di difesa. Precisamente, la Corte afferma che il principio del contraddittorio implica una dialettica procedimentale non solo sugli esiti del materiale acquisito, ma anche sulle modalità con cui è stato acquisito detto materiale. Ne consegue che, *ex* art. 191 c.p.p., una prova è inutilizzabile se viola i divieti stabiliti dalla legge. In conclusione, per i giudici di legittimità, la difesa gode del diritto di accedere alla documentazione dell'attività investigativa svolta e di conoscere le modalità con cui erano state

acquisite tali messaggi criptati, in virtù dell'osservanza del diritto di difesa e di contraddittorio.

[41] Cfr. PROCURA GENERALE DELLA CORTE DI CASSAZIONE, *Memoria per l'udienza delle Sezioni Unite penali del 29 febbraio 2024,* cit.

[42] Cass., Sez. Un., 14 giugno 2024, n. 23755, cit.

[43] Sulle garanzie da riservare agli strumenti investigativi finalizzati a sequestrare di *chat*, *email* e – più ampiamente – dati comunicativi, sia consentito, MURRO, *Lo* "smartphone" *come fonte di prova. dal sequestro del dispositivo all'analisi dei dati*, Padova, 2024, 195.

[44] Corte giust. UE, Grande Sezione, 2 marzo 2021, *H.K./Prokuratuur,* C-746/18.

[45] Il principio viene ripreso anche dalla giurisprudenza interna che ha ritenuto come l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione de[ve] essere sempre autorizzata da un giudice: sarebbe davvero singolare ritenere che per l'acquisizione dei dati esterni del traffico telefonico e telematico sia necessario un preventivo provvedimento autorizzativo del giudice, mentre per compiere il sequestro di dati informatici riguardanti il contenuto delle comunicazioni oggetto di quel traffico sia sufficiente un provvedimento del pubblico ministero; così, Cass., Sez. IV, 26 ottobre 2023, n. 44154, cit.

[46] Corte giust. UE, 2 marzo 2021, C- 746/18*, H.K.,* cit.

[47] L. 23 novembre 2021, n. 178, cit.

[48] Per un commento della sentenza, CHELO, *Davvero legittimo il sequestro di messaggi e-mail già letti?*, in *Giur. cost.*, 2023, 296; FILIPPI, *Il cellulare "contenitore" di corrispondenza anche se già letta dal destinatario*, in *questa Rivista*, 6 settembre 2023.

[49] Corte EDU, 05 settembre 2017, *Barbulescu c. Romania*; § 72; Corte EDU, 03 aprile 2007, *Copland c. Regno Unito*, § 41.

[50] Corte EDU, 17 dicembre 2020, *Saber c. Norvegia.*

[51] Corte EDU, 05 settembre 2017, *Barbulescu*, cit., § 74.

[52] In questo senso, CAIANELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale*, cit., 6.

[53] Così, LUDOVICI, *I criptofonini: sistemi informatici criptati e* server *occulti,* in *questa Rivista,* 2023, 3, 420.

[54] In effetti, le investigazioni sulle piattaforme criptate sono lontane dal rappresentare il prototipo delle tecniche di sorveglianza "non mirata" (o di massa), per cui «la persona, l'organizzazione o la caratteristica tecnica cui la raccolta dei dati è indirizzata non possono essere specificate preventivamente», rientrando, per converso, nell'ambito delle tecniche investigative di *surveillance* "mirata", ossia quelle «applicate dalle autorità competenti nel contesto di indagini penali [o prima del loro formale inizio] allo scopo di individuare e indagare su reati gravi e sospetti, e mirano a raccogliere informazioni in modo tale da non avvisare le persone bersaglio». In questi casi, infatti, pur se l'investigazione non è diretta ad acquisire flussi comunicativi di sistemi informatici "determinati" ma tutti i flussi che transitano (o sono transitati) sulla piattaforma, esiste un *target* di riferimento, così come esiste ed è sufficientemente individuato un "sistema" da attenzionare, sia pur virtuale ed etereo, quale è il *server*. In questo senso, CURTOTTI, RIZZI, NOCERINO, RUSSITTO, GILIBERTI, SCARPA, *Piattaforme criptate e prove penali,* cit., 177. Analogamente, PROCURA GENERALE DELLA CORTE DI CASSAZIONE, *Memoria per l'udienza delle Sezioni Unite penali del 29 febbraio 2024,* cit.

[55] L'assunto sembra ancor più pertinente in un momento in cui la giurisprudenza nazionale pone particolare attenzione alla questione relativa alla proporzione tra quanto "richiesto" e quanto "appreso". Cfr., da ultimo, Cass., Sez. VI, 21 maggio 2024, n. 31180, non massimata.

[56] LUDOVICI, *I criptofonini: sistemi informatici criptati e* server *occulti,* cit., 420.

[57] Cfr. ALLEGREZZA, *Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality,* in Aa. Vv., *Transnational Evidence and Multicultural Inquiries in Europe. Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, a cura di Ruggeri, Cham, 2014, 59-60. Sul principio di proporzionalità nel contesto dell'O.E.I., cfr. DANIELE, *I chiaroscuri dell'OEI e la bussola della proporzionalità,* in Aa. Vv., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017,* a cura di Kostoris-Daniele, Torino, 2018, 55 ss. Con precipuo riferimento al caso in esame, LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate*, cit., 162; NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla* querelle *giurisprudenziale sull'acquisizione della messaggistica criptata dell'estero,* in *Sist. pen.,* 2024, 2, 189.

[58] In questo senso, NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti,* cit., 190.

[59] Per tutti, TORRE, *L'intercettazione di flussi telematici (art. 266* bis *c.p.p.),* in Aa. Vv., Cybercrime, *Trattato di diritto penale,* a cura di Cadoppi, Canestrari, Manna, Papa, Torino, 2019, 1472 ss.

[60] Secondo la giurisprudenza della Corte EDU, «deve ritenersi sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti ove questa viene condotta». Sul punto Corte EDU, Grande Camera, 4 dicembre 2015, *Roman Zakharov c. Russia*. Così ragionando, il *server* potrebbe essere considerato come un contenitore (*rectius:* spazio) su cui transitano flussi comunicativi da attenzionare, non dissimile dallo *smartphone* o dal *computer*.

[61] Il Giudice delle leggi (cfr. Corte cost., 27 luglio 2023, n. 170; Corte cost., 28 dicembre 2023, n. 227 del 2023; Corte cost.,12 gennaio 2023, n. 2), specifica che il concetto di corrispondenza comprende qualsiasi comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, realizzata in modo diverso dalla conversazione in presenza e che prescinde dal mezzo tecnico utilizzato e, pertanto, si estende anche alla posta elettronica e ai messaggi inviati tramite l'applicativo *WhatsApp* o sms o sistemi simili, in quanto «del tutto assimilabili a lettere o a biglietti chiusi», perché accessibili soltanto mediante codici di accesso o altri meccanismi di identificazione. Di conseguenza, in tali ipotesi, trova applicazione la tutela prevista dall'art. 15 Cost., che assicura la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, consentendone la limitazione sulla base delle riserve di legge e di giurisdizione, ovvero con le garanzie previste dalla legge e soltanto con atto motivato dell'autorità giudiziaria. Sul tema, *ex multis,* CURTOTTI, *La sentenza costituzionale n. 170 del 2023 e le*

comunicazioni "apparenti": quando un eccesso di garanzie non sempre è un moltiplicatore di garanzie, in *Dir. inf. inform*., 2023, 4/5, 708; BACCARI, *Lo scambio di messaggi WhatsApp costituisce "corrispondenza",* in *Proc. pen. giust.,* 2024 4, 862. Per dovere di completezza, si precisa che il principio viene recepito dalla giurisprudenza di legittimità. Cfr. Cass., Sez. VI, 21 maggio 2024, n. 31180, non massimata.

[62] In particolare, il giudice della libertà e della detenzione di Lille che autorizza per primo le investigazioni su piattaforme criptate il 14 giugno 2019 dispone sia le intercettazioni e sia accesso a distanza per captare le comunicazioni in transito e acquisire i dati contenuti nei dispositivi (OEI); il giudice istruttore di Parigi autorizza le attività di intrusione informatica che travalicano i confini della mera captazione del flusso in transito avendo come scopo l'acquisizione di dati informatici "freddi" e "caldi".

[63] Cfr. Ordine Europeo di Indagine, 13 aprile 2021, 3.

[64] In questo senso, NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti,* cit., 183; SPANGHER, *Criptofonini: le sentenze delle Sezioni Unite,* cit., 3.

[65] Sul tema, volendo, NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere,* Padova, 2021.

[66] In questo senso NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti,* cit., 196.

[67] SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, 161.

[68] SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. pen. giust*., 2017, 178.

[69] DANIELE, I chiaroscuri dell'OEI e la bussola della proporzionalità, in DANIELE - KOSTORIS (a cura di), L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017, Torino, 2018, 55.

[70] In questo senso, DANIELE, *Le "sentenze gemelle" delle Sezioni Unite*, cit. L'A. ritiene che il vaglio giurisdizionale «nel sistema dell'OEI, costituisce un tassello ineludibile. Lo si ricava *in primis* dal già ricordato obbligo di rispettare i diritti fondamentali nei limiti del principio di proporzionalità, rispetto a cui il controllo giurisdizionale rappresenta un prerequisito essenziale».

[71] Corte giust. UE, 11 novembre 2021, *Gavanozov*, C-852/19, in *Cass. pen.*, 2022, 883.

[72] Corte giust. UE, 11 novembre 2021, *Gavanozov*, cit.

[73] In tema, DE LUCA, *La Corte di giustizia si pronuncia nuovamente sull'ordine europeo di indagine: la tutela dei diritti fondamentali prevale sull'efficienza investigativa*, in *Sist. pen.*, 9 marzo 2022.

[74] Cfr., NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti,* cit., 197.

[75] Cfr., Cass., Sez. VI, 26 ottobre 2023, n. 44154, in *C.E.D. Cass.,* n. 285284.

[76] CONTI, Accertamento del fatto e inutilizzabilità nel processo penale, Padova, 2007, 150. Per una completa disamina della questione si rinvia a NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti,* cit., 198; l'A. precisa anche come in tale caso l'inutilizzabilità «discenderebbe poi in questo caso dal mancato rispetto di prescrizioni dettate dalle *lex fori* a fronte di un Ordine di indagine cui è stato comunque dato corso e che costituisce il formale canale acquisitivo dei contributi raccolti all'estero, e vi sarebbe perciò da superare la difficoltà connessa all'affermazione di una inutilizzabilità derivata verso cui la giurisprudenza continua a dimostrarsi marcatamente ostile».

[77] NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti,* cit., 200.

[78] Sia l'art. 1, § 4 della direttiva 2014/41/UE, sia l'art. 1, d.lgs. n. 108/2017 sanciscono il dovere di rispettare i principi dell'ordinamento costituzionale e della Carta dei diritti fondamentali dell'Unione Europea. Inoltre ai sensi dell'art. 14, § 7, «[...]. Fatte salve le norme procedurali nazionali, gli Stati membri assicurano che nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto

processo nel valutare le prove acquisite tramite l'OEI».

[79] Cfr., Cass., Sez. VI, 26 ottobre 2023, n. 44154, in *C.E.D. Cass*., n. 285284.

[80] NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti,* cit., 201, per cui «l'invalidità discenderebbe nella specie in questo caso dall'incostituzionalità affermata attraverso il parametro interposto di cui all'art. 117 Cost.38. Del resto anche lo Stato che riceve il materiale intercettato è pur sempre tenuto al rispetto delle prerogative affermate dalla Convenzione quantunque l'ingerenza originaria non si sia materialmente verificata all'interno del suo territorio».

[81] Così, LUDOVICI, *I criptofonini: sistemi informatici criptati e* server *occulti*, cit., 421.

[82] Corte giust. UE., 30 aprile 2024, *M.N.*, cit.

[83] **Sul tema, MASSARI,** *Il diritto di difesa, questo sconosciuto: il caso dei criptofonini e degli ordini europei di indagine***, in** *Diritto difesa***, 11 settembre 2024.**

[84] Cass., Sez. VI, 14 aprile 2023, n. 15836, in *Giur. it.*, 2023, 1678, con nota, volendo di MURRO, *L'utilizzabilità dei dati di geolocalizzazione: le risposte della giurisprudenza vs il roboante silenzio normativo*, nella quale pronuncia si precisa che i dati presenti sui tabulati, relativi alla geolocalizzazione, sono inutilizzabili se non sono acquisiti con provvedimento del p.m. Anche nel contesto europeo, le numerose pronunce sono state mosse dalla *ratio* di limitare abusi nella vita privata dell'individuo attraverso un utilizzo incontrollato e non disciplinato degli strumenti di investigazione digitale, *ex multis*, Corte EDU, Sez. I, 25 maggio 2021, *Big Brother Watch & Altri c. Regno Unito*

[85] C. Cost., 27 luglio 2023, n. 170, in *questa Rivista*, 6 settembre 2023, con nota di FILIPPI, *Il cellulare "contenitore" di corrispondenza anche se già letta dal destinatario*.

[86] Il d.d.l. A.S. n. 806 del 2024 – approvato dal Senato nell'aprile 2024 – mira ad introdurre una disciplina *ad*

hoc per il sequestro di *smartphone* e altri dispositivi. Sul tema, sia consentito, MURRO, *Lo* smartphone *come fonte di prova*, cit., 261.

[87] Come precisa la Corte EDU, sussiste una violazione dell'art. 6, comma 2, Cedu tutte le volte in cui l'autorità giudiziaria non ha indicato in maniera esaustiva i motivi che hanno determinato la compressione delle libertà fondamentali. Corte EDU, 26 giugno 2016, *Mugosa c. Montenegro*; Corte EDU, 10 novembre 2015, *Slavov e altri c. Bulgaria*. Inoltre, sussiste una violazione dell'art. 8 Cedu ogniqualvolta il provvedimento con cui vengono disposte le intercettazioni non viene corredato da una solida motivazione quanto ai suoi presupposti; nondimeno, è compito dell'autorità monitorare con costanza la permanenza delle ragioni che, ai tempi, imponevano la captazione occulta. Da ultimo, Corte EDU, 12 gennaio 2023, *Potoczka and Adamco c. Slovacchia*

[88] Per un approfondimento in dottrina, tra i molti, AA.VV., *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul* cybercrime, a cura di Luparia, Milano, 2009; LUPARIA, Computer crime *e procedimento penale*,in AA.VV., *Modelli differenziati di accertamento*, a cura di Garuti, in *Trattato di procedura penale*,diretto da Spangher, Torino, 2011, 369.

[89] Sulle carenze della normativa, BERGONZI PERRONE, *Il mancato rispetto delle disposizioni della l. 48/2008 in tema di acquisizione probatoria informatica: per una ipotesi sanzionatoria non prevista esplicitamente dal dato normativo,* Stem Mucchi Editore, 2013.

[90] Così, LA REGINA, *Il sequestro dei dispositivi di archiviazione digitale*, in *questa Rivista,* 2023, 429.

[91] D. lgs. 1° agosto 2003, n. 259.

[92] WEBBER, *On the Loss of Rights*, in *Proportionality and the Rule of Law. Rights, Justification, Reasoning*, a cura di Huscroft - Miller - Webber, Cambridge, 2014, 123.

[93] MONTESQUIEU, *Lo spirito delle leggi*, Ginevra, 1748, trad. it., Milano, 1989.

[94] Secondo SPANGHER, *Criptofonini: le sentenze delle Sezioni Unite,* cit., 3, «occorre riscrivere lo statuto delle prove penali stante l'inadeguatezza dell'attuale disciplina sia sotto il profilo della necessita di accrescere la riserva di giurisdizione, sia alla luce a questa collegata delle implicazioni dello sviluppo scientifico e tecnologico, anche nella prospettiva dell'IA». Secondo NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti,* cit., 201, non bisogna per forza "salvare" la prova (e quindi lo strumento di cooperazione con cui questa circola), risultando più opportuno stimolare il legislatore ad intervenire in materia.

Cass_23756_24Download

Cass_23755_24Download