PENALE

La Corte di giustizia dell'UE sui criptofonini

Fonte: C. Giustizia UE grande sezione, 30 aprile 2024, n. 670

Luigi Giordano
09 Maggio 2024

Con la pronuncia in esame la Corte di giustizia dell'Unione Europea si è occupata di risolvere le cinque questioni pregiudiziali sollevate dal tribunale di Berlino sulla legittimità degli ordini europei di indagine alla luce delle previsioni della direttiva 2014/41.

Massima

Ai sensi degli artt. 1, par. 1, 2, par. 1, lett. c) e 6 della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, un ordine europeo di indagine inteso a ottenere la trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione – nella specie, i risultati di intercettazioni relativi a telefoni che permettevano conversazioni criptate – può essere emesso anche dal pubblico ministero, non dovendo essere adottato necessariamente dal giudice, pure se, in forza del diritto dello Stato di emissione, in un procedimento interno a tale Stato, la raccolta originaria di tali prove avrebbe dovuto essere ordinata da un giudice, sempre che la competenza a disporre l'acquisizione di prove raccolte in un diverso procedimento sia attribuita al pubblico ministero.

Il caso

Nell'ambito di un'indagine condotta dalle autorità francesi, è emerso l'utilizzo di telefoni cellulari funzionanti mediante un applicativo denominato EncroChat per commettere reati concernenti principalmente al traffico di sostanze stupefacenti. Questi telefoni permettevano, per mezzo di un *software* speciale ed un *hardware* modificato rispetto a quelli normalmente in commercio, passando per un *server* installato a Roubaix (Francia), **comunicazioni cifrate non intercettabili con metodi di indagine tradizionali**.

La polizia francese, previa autorizzazione giurisdizionale, è riuscita a salvare alcuni dati contenuti in tale server nel 2018 e nel 2019. Tali dati hanno consentito lo sviluppo, da parte esperti anche dei Paesi Bassi, di un *software* di tipo *trojan*. Il *software* è stato caricato su detto server nella primavera del 2020, previa autorizzazione del *Tribunal correctionnel de Lille* (Tribunale penale di Lille, Francia) e, da lì, sui predetti telefoni cellulari tramite un aggiornamento simulato.

Il *trojan* avrebbe interessato 32477 utenti, su un totale di 66134 utenti iscritti, ripartiti in 122 Paesi, 4600 dei quali in Germania, permettendo l'esecuzione di intercettazioni.

Il 9 marzo 2020, taluni rappresentanti del *Bundeskriminalamt* (Ufficio federale della polizia criminale tedesca, in prosieguo, «BKA») e della Procura di Francoforte nonché alcuni rappresentanti, fra l'altro, delle autorità della Francia, dei Paesi Bassi e del Regno Unito, hanno partecipato a una videoconferenza organizzata dall'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust). Nel corso di tale riunione, **i rappresentanti delle autorità della Francia e dei Paesi Bassi hanno informato le autorità degli altri Stati membri dell'indagine** in corso nei confronti della società di gestione di telefoni cellulari criptati e **delle intercettazioni** poste in essere, **comprensive anche dei dati provenienti da telefoni cellulari che si trovavano all'esterno del territorio francese**.

Con una nota del 13 marzo 2020, il BKA ha annunciato l'apertura di un'indagine a carico di un gruppo di ignoti utenti del servizio EncroChat per traffico di sostanze stupefacenti e per associazione a delinquere, spiegando che **l'utilizzo del servizio EncroChat destava, in quanto tale, il sospetto della commissione di reati gravi, in particolare dell'organizzazione di un traffico di stupefacenti**.

In data 20 marzo 2020, sulla base della nota della polizia criminale federale, la Procura generale di Francoforte ha avviato un procedimento.

Tra il 3 aprile e il 28 giugno 2020, **il BKA ha consultato i dati diffusi quotidianamente sul server di Europol relativi ai telefoni cellulari utilizzati in Germania**.

Il 2 giugno 2020, la Procura generale di Francoforte ha chiesto alle autorità francesi, mediante **un primo ordine europeo di indagine (in seguito OEI)**, **l'autorizzazione ad utilizzare in procedimenti penali i dati provenienti dal servizio EncroChat**, sul presupposto che un gran numero di reati molto gravi, in particolare l'importazione e il traffico di sostanze stupefacenti, venivano commessi in Germania con l'ausilio di telefoni cellulari dotati di tale servizio; due ulteriori ordini europei di indagine sono stati inviati in data 9 settembre 2020 e 2 luglio 2021.

In forza di tali domande, il *Tribunal correctionnel de Lille* ha autorizzato la trasmissione dei dati tratti dai telefoni cellulari dotati del servizio EncroChat degli utenti tedeschi.

Successivamente, **la Procura generale di Francoforte ha separato, dall'originario unitario procedimento, distinti procedimenti, assegnati alle Procure locali competenti rispetto ai diversi indagati**.

In siffatto contesto, **il *Landgericht Berlin* ha sollevato alcune questioni pregiudiziali sulla legittimità degli ordini europei di indagine alla luce delle previsioni della direttiva 2014/41**.

La questione

Il Tribunale di Berlino, giudice del rinvio pregiudiziale, ha posto **cinque questioni pregiudiziali**.

La prima riguarda la possibilità di ricomprendere, ai sensi dell'art. 2, par. 1, lett. c), della direttiva 2014/41, anche il pubblico ministero tra le **autorità competenti ad adottare un OEI**, quando tale ordine concerne la trasmissione di esiti di intercettazione compiute in un altro Stato membro.

La seconda e la terza questione riguardano le **condizioni sostanziali**, disciplinate dall'art. 6 della direttiva 2014/41, alle quali è subordinata l'adozione di un OEI.

È stato chiesto alla Corte europea, tra l'altro, di precisare se, al fine di **soddisfare i presupposti di necessità e di proporzionalità** richiesti dall'art. 6, par. 1, lett. a, della direttiva 2014/41 per l'emissione di un OEI con cui si chiede l'accesso a dati raccolti mediante l'intercettazione di telecomunicazioni in un altro Stato membro, **devono essere stati già raccolti, a carico di ciascuna persona interessata, elementi concreti, di partecipazione a un reato grave**.

La quarta questione verte sull'interpretazione dell'art. 31 della direttiva 2014/41, essendo stato chiesto alla Corte europea se le **autorità investigative francesi avrebbero dovuto notificare all'autorità tedesca competente l'atto di infiltrazione in telefoni cellulari tedeschi**, dotati del servizio EncroChat, prima dell'attuazione di tale misura.

La quinta questione attiene alla determinazione delle conseguenze di una eventuale violazione del diritto dell'Unione alla luce dei principi di equivalenza e di effettività.

Le soluzioni giuridiche

1. Con la prima questione, dunque, il Tribunale di Berlino ha chiesto se un OEI diretto alla trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione debba necessariamente essere adottato da un giudice dello Stato di emissione quando, in forza del diritto di tale Stato, in un procedimento interno, **la raccolta originaria di tali prove avrebbe dovuto essere ordinata da un giudice**.

La Corte europea ha rilevato che, secondo l'art. 1, par. 1, della direttiva 2014/41, un OEI – che può riguardare tanto il compimento di atti specifici al fine di acquisire prove, quanto l'acquisizione di prove che sono già in possesso delle autorità competenti dello Stato di esecuzione - deve essere emesso o convalidato da un'«autorità giudiziaria». Tale disposizione non definisce la nozione di «autorità giudiziaria». L'**art. 2, lett. c), della direttiva**, tuttavia, **ricomprende espressamente il pubblico ministero tra le autorità che**, al pari del giudice, **possono emettere un OEI**.

Il pubblico ministero, peraltro, rientra nella nozione di «autorità di emissione, se, in forza del diritto dello Stato di emissione, tale autorità giudiziaria è competente, in un caso interno, ad ordinare un atto di indagine diretto alla trasmissione di prove raccolte in un diverso procedimento nazionale.

L'art. 1, par. 1, e l'art. 2, lettera c), della direttiva 2014/41, pertanto, devono essere interpretati nel senso che**:**

- **un OEI inteso a ottenere la trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione non deve essere adottato necessariamente da un giudice;**
- è necessario, però, che, in forza del diritto dello Stato di emissione, in un procedimento interno a tale Stato, seppur la raccolta iniziale di tali prove avrebbe dovuto essere ordinata da un giudice, la competenza ad ordinare la trasmissione di dette prove sia assegnata dalla legge al pubblico ministero.

2. La seconda e la terza questione posta alla Corte europea concernono **l'interpretazione dell'art. 6, par. 1, lett. a) e b), della direttiva 2014/41.** Si tratta della disposizione che fissa le condizioni necessarie per l'emissione di un OEI.

Al riguardo, la Corte europea ha precisato che:

- **il carattere necessario e proporzionato dell'emissione dell'OEI deve essere valutato unicamente alla luce del diritto dello Stato di emissione**;

- **l'emissione di un OEI diretto alla trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione non è necessariamente subordinata all'esistenza elementi concreti di un grave reato a carico di ciascuna persona interessata**, qualora un tale requisito non derivi dal diritto dello Stato di emissione;
- il presupposto della proporzionalità **non osta all'emissione di un OEI neppure nel caso in cui l'integrità dei dati ottenuti tramite l'intercettazione non possa essere verificata a causa della riservatezza delle basi tecniche che hanno permesso l'attuazione di tale misura**, purché **il diritto a un processo equo venga garantito nel corso del successivo procedimento penale**.
- **l'integrità delle prove già esistenti nello Stato di esecuzione e trasmesse in adempimento di un OEI può essere valutata solo nel momento in cui le autorità dello Stato di emissione dispongono effettivamente delle prove** e non nella fase anteriore dell'emissione dell'OEI.

3. L'art. 6, par. 1, lett. b), della direttiva 2014/41, poi, prevede una ulteriore condizione per l'emissione dell'OEI. Occorre che l'atto o gli atti di indagine richiesti avrebbero potuto essere emessi alle **stesse condizioni in un caso interno analogo**.

In ordine a tale presupposto, secondo la Corte, impiegando i termini «alle stesse condizioni» e «in un caso interno analogo», la disposizione della direttiva subordina **al solo diritto dello Stato di emissione la determinazione delle specifiche condizioni richieste per l'emissione di un OEI**.

Qualora un'autorità di emissione intenda acquisire prove già in possesso delle autorità competenti dello Stato di esecuzione, pertanto, tale autorità deve subordinare un OEI al rispetto di **tutte le condizioni previste dal diritto del proprio Stato per un caso interno analogo**.

L'art. 6, par. 1, lettera b), della direttiva 2014/41, invece, **non richiede** che **l'emissione di un OEI diretto alla trasmissione di prove già in possesso** delle autorità competenti dello Stato di esecuzione **sia soggetta alle stesse condizioni sostanziali applicabili, nello Stato di emissione, in materia di raccolta di tali prove**.

L'autorità di emissione, inoltre, in forza delle disposizioni della direttiva, **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**.

La direttiva 2014/41, infatti, garantisce il controllo giurisdizionale del rispetto dei diritti fondamentali delle persone interessate, imponendo **agli Stati membri di provvedere affinché mezzi di impugnazione equivalenti a quelli disponibili in un caso interno analogo siano applicabili agli atti di indagine richiesti nell'OEI** (art. 14, par. 1) e stabilendo di assicurare che, nel procedimento penale avviato nello Stato di emissione, siano rispettati **i diritti della difesa e sia garantito un giusto processo** nel valutare le prove acquisite tramite tale OEI (art. 14, par. 7).

Per quanto riguarda segnatamente il diritto a un processo equo, qualora un organo giurisdizionale consideri che **una parte non sia in grado di svolgere efficacemente le proprie osservazioni in merito a un elemento di prova idoneo ad influire in modo preponderante sulla valutazione dei fatti**, deve constatare una violazione del diritto ad un processo equo ed escludere tale mezzo di prova al fine di evitare una violazione di questo tipo (CGUE 2 marzo 2021, Prokuratuur).

4. La quarta questione concerne l'interpretazione dell'art. 31 della direttiva 2014/41. Secondo questa disposizione, **l'autorità competente di uno Stato membro**, che ha

autorizzato l'intercettazione di telecomunicazioni di una persona il cui indirizzo di comunicazione è utilizzato sul territorio di un altro Stato membro la cui assistenza tecnica non è necessaria per effettuare tale intercettazione, è tenuta a **notificare l'intercettazione** all'autorità competente di tale Stato,

Secondo la Corte di Giustizia, una misura connessa all'infiltrazione in apparecchi terminali, diretta a estrarre dati relativi al traffico, all'ubicazione e alle comunicazioni di un servizio di comunicazione basato su internet costituisce un'«intercettazione di telecomunicazioni». Essa, pertanto, **deve essere oggetto di notifica** all'autorità a tal fine designata dallo Stato membro sul cui territorio si trova la persona sottoposta all'intercettazione.

Nel caso in cui lo Stato membro di intercettazione non sia in grado di identificare l'autorità competente dello Stato membro notificato, **tale notifica può essere inviata a qualsiasi autorità dello Stato membro notificato che lo Stato membro di intercettazione ritenga idonea a tal fine**.

5. L'art. 31, par. 3, della direttiva 2014/41 prevede che, qualora, in un caso interno analogo, l'intercettazione non sia ammessa, l'autorità competente dello Stato membro notificato **può notificare** all'autorità competente dello Stato membro di intercettazione che tale intercettazione non può essere effettuata o che si deve porre fine alla medesima o, anche, che i dati intercettati non possono essere utilizzati o possono essere utilizzati solo alle condizioni da essa specificate.

Secondo la Corte europea, l'utilizzo del verbo «potere» in tale disposizione implica che lo Stato membro notificato disponga di una facoltà che rientra nella discrezionalità dell'autorità competente di tale Stato. La norma, però, **non mira solo a garantire il rispetto della sovranità** dello Stato membro notificato, ma anche ad assicurare che **il livello di tutela garantito in tale Stato membro in materia di intercettazione delle telecomunicazioni non sia compromesso**.

6. Sulla quinta questione, infine, **la Corte ha rilevato che, allo stato attuale del diritto dell'Unione, spetta**, in linea di principio, **unicamente al diritto nazionale determinare le norme relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale, di elementi di prova che sono stati ottenuti con modalità contrarie al diritto dell'Unione** (CGUE 6 ottobre 2020, *La Quadrature du Net e a.*, punto 222).

Secondo una costante giurisprudenza, infatti, in assenza di una normativa dell'Unione in materia, **spetta all'ordinamento giuridico interno di ciascuno Stato membro, ai sensi del principio dell'autonomia procedurale, stabilire le modalità procedurali dei ricorsi intesi a garantire la tutela dei diritti spettanti ai singoli in forza del diritto dell'Unione**, a condizione tuttavia che esse non siano meno favorevoli rispetto a quelle relative a situazioni analoghe assoggettate al diritto interno (principio di equivalenza) e che non rendano in pratica impossibile o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione (principio di effettività) (v., in tal senso, CGUE 16 dicembre 1976, *Rewe-Zentralfinanz e Rewe-Zentral*, punto 5; CGUE 6 ottobre 2020, *La Quadrature du Net e a*., punto 223).

L'art. 14, par. 7, della direttiva 2014/41, peraltro, **impone espressamente agli Stati membri di garantire** che, in un procedimento penale nello Stato di emissione, **siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove ottenute mediante l'OEI**, il che comporta che un elemento di prova sul quale una parte non sia in grado di svolgere efficacemente le proprie osservazioni debba essere escluso dal procedimento penale.

Osservazioni

1. Sono stati definiti **"criptofonini"** i telefoni cellulari che permettono lo scambio di dati crittografati con una cifratura a più livelli. Tali apparecchi sono costituiti da un *hardware* opportunamente modificato (in genere *Apple*, *Android* o *Black Berry*) e da un sistema operativo avente particolari requisiti di sicurezza, in quanto i servizi di localizzazione (GPS, *Bluetooth*, fotocamera, scheda SD e porta USB) sono disabilitati. Le chiamate rimangono attive solo in modalità *Voice over IP* (VoiP), utilizzando applicazioni che assicurano comunicazione cifrate (*Encrochat*, *Sky ECC, Anom, No1bc*, etc.) ed evitando l'uso della rete GSM.

Nel procedimento penale tedesco nel quale sono state sollevate le questioni di pregiudizialità appena illustrate **i telefoni usavano il programma *Encrochat***, una rete di comunicazione eliminata a seguito della complessa operazione di polizia congiunta tra Francia e Paesi Bassi che è stata descritta in precedenza.

Nei procedimenti penali italiani nei quali sono stati usate come prove le chat tratte da criptofonini, invece, è emerso per lo più l'utilizzo del **diverso applicativo *Sky Ecc***. Tale programma apparteneva a *Sky Global,* società fornitrice di servizi di comunicazione con sede a Vancouver, in Canada. 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.

Sembra corretto sostenere che *Encrochat, Sky Ecc* e i sistemi di comunicazione similari si rivolgano alla medesima comunità di utenti o, quanto meno, a persone che hanno esigenze di riservatezza di analoga intensità.

Dalla motivazione dell'autorizzazione di intercettazione della corrispondenza per via elettronica del giudice istruttore di Lille del 3 agosto 2020 relativa alle indagini che hanno riguardato *Sky Global*, difatti, risulta che, da metà giugno 2020 all'agosto 2020, il servizio *Sky Ecc* ha registrato "*più di 30.000 nuovi utenti*". Questo improvviso incremento di utilizzatori è stato ritenuto connesso alla migrazione di soggetti che in precedenza si avvalevano della soluzione crittografata *Encrochat*. L'esigenza di rendere anonime le conversazioni, dunque, era tanto pregnante per gli utenti da determinarne il rapido passaggio da *Encrochat* a *Sky Ecc.*

2. Il procedimento penale tedesco nel quale sono state sollevate le questioni pregiudiziali ha seguito un percorso che sembra significativamente diverso da quello che ha caratterizzato i procedimenti penali italiani - ormai numerosi - nei quali sono state usate le *chat* tratte da telefoni criptati che impiegano l'applicativo *Sky Ecc*.

Dalla sentenza illustrata, infatti, risulta che la polizia giudiziaria tedesca, ammessa a far parte di una squadra investigativa comune (strumento istituito per combattere il traffico di stupefacenti, la tratta degli esseri umani e il terrorismo e disciplinato dalla Decisione quadro del Consiglio UE del 13 giugno 2002), ha consultato per qualche tempo i dati, diffusi quotidianamente sul server di Europol, relativi ai telefoni cellulari utilizzati in Germania

La Procura generale di Francoforte, successivamente, ha chiesto alle autorità francesi, mediante un primo OIE, l'autorizzazione ad utilizzare in procedimenti penali i dati captati. **Questo ordine sembra aver riguardato tutti i dati desunti dalle intercettazioni di cittadini tedeschi**, in quel momento non identificati, **sul presupposto che, per il solo fatto di impiegare il sistema *Encrochat* per comunicare, essi fossero sospettati di pianificare e di commettere reati molto gravi in Germania.**

La Procura generale di Francoforte, poi, dopo altri due OIE per la trasmissione di dati ulteriori, ha separato il procedimento iniziale trasmettendo gli atti a carico di taluni utenti alle diverse Procure locali competenti.

Il procedimento penale nel quale è stata sollevata la questione pregiudiziale è uno di quelli che sono derivati dal descritto "stralcio".

Nei procedimenti penali italiani in cui sono state utilizzate come prova le chat tratte *da Sky Ecc*, invece, nel corso di indagini già in corso, **i pubblici ministeri italiani, con OIE, hanno chiesto all'autorità francese la trasmissione delle conversazioni intervenute in precisi ambiti temporali e relative a specifiche persone, già coinvolte in precedenti indagini**.

I due procedimenti penali trattati dalle Sezioni unite della Corte di cassazione in data 29 febbraio 2024, in particolare, hanno riguardato persone che erano già indagate, in quanto raggiunte da consistenti indizi di traffico internazionali di stupefacenti, in un contesto in cui è stato accertato l'impiego di telefoni criptati da parte di costoro.

Nel procedimento istruito dalla Procura della Repubblica di Potenza, l'utilizzatore del criptofonino, prima dell'acquisizione dell'emissione dell'OIE, aveva addirittura già preso parte ad una transazione simulata avente ad oggetto l'acquisto di droga da un agente sotto copertura.

Non risulta in detti procedimenti, i pubblici ministeri competenti o la polizia giudiziaria che ha curato le indagini abbiano avuto la disponibilità dell'intero materiale intercettato dalle autorità francesi.

3. Appare utile anche evidenziare che **la decisione europea dà per acquisito che il mezzo di ricerca della prova che è stato compiuto in Francia sia qualificabile come una intercettazione** di comunicazioni e che, con OIE, siano stati richiesti gli esiti di tali captazioni. Nella sentenza, peraltro, è precisato che l'art. 31 della direttiva 2014/41 non contiene una definizione della nozione di telecomunicazioni che sono oggetto di intercettazioni; dal contesto in cui è inserita questa norma, tuttavia, si desume che **l'infiltrazione in apparecchiature terminali volta ad estrarre dati di comunicazione,** ma anche dati relativi al traffico o all'ubicazione, a partire da un servizio di comunicazione basato su internet **costituisce un'intercettazione di telecomunicazioni**.

La soluzione accolta dalla Corte europea sembra conforme a quella accolta dalle Sezioni unite della Corte di cassazione sulla base di quanto può desumersi dalle informazioni provvisorie relative alle sentenze del 29 febbraio 2024.

4. La prima questione pregiudiziale concerne, come si è visto, la competenza del pubblico ministero ad emettere un OIE che ha per oggetto i risultati di intercettazioni già eseguite nello Stato di esecuzione.

La Corte europea ha accolto dell'espressione "*autorità di emissione*" dell'OIE di cui agli artt. 1, 2, lett. c), e 6 della direttiva 2014/41/UE **una interpretazione che ricomprende anche il pubblico ministero, pure nel caso in cui con l'OIE si chieda la trasmissione dei risultati di intercettazioni**.

È necessario, però, che, in forza del diritto dello Stato di emissione, il pubblico ministero sia competente, in un caso interno a tale Stato, ad ordinare un atto di indagine diretto alla acquisizione di prove già formate in un diverso procedimento.

La Corte, pertanto, **ha ritenuto che**, ai fini dell'acquisizione di una prova già raccolta nello Stato di esecuzione dell'OIE, **debba essere valorizzata la base giuridica che ne**

permette, nell'ordinamento dello Stato di emissione, la trasmissione da un procedimento ad un altro, piuttosto che quella che regola la sua raccolta iniziale.

L'interpretazione della Corte europea risulta in linea con le sentenze delle Sezioni unite della Corte di cassazione citate e **costituisce una conferma della legittimità degli ordini europei di indagine con i quali diversi pubblici ministeri italiani** hanno richiesto la trasmissione di chat avvenute tramite l'applicativo *Sky ECC* intercettate nel corso di un procedimento francese a seguito di provvedimenti di giudici di questo Stato.

Circa la competenza del pubblico ministero italiano ad ordinare la trasmissione di prove raccolte in diverso procedimento, deve rilevarsi che:

- ai sensi dell'art. 27, comma 1, del d.lgs. n. 108 del 2017, recante le norme di attuazione della direttiva relativa all'OIE, **può emettere**, nell'ambito delle proprie attribuzioni nella fase delle indagini preliminari, **un OIE volto all'acquisizione di una prova «già disponibile» in un altro Stato membro** e a trasmetterlo direttamente all'autorità di esecuzione;
- in tema di intercettazioni, l'art. 270 c.p.p. permette, in presenza di talune condizioni, l'importazione degli esiti del mezzo di ricerca della prova svolto in un diverso procedimento su iniziativa del pubblico ministero;
- l'art. 78 disp. att. c.p.p., infine, prevede che "*la documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera può essere acquisita a norma dell'art. 238 del codice*", anche in questo caso su iniziativa del pubblico ministero.

5. La Corte europea, in particolare, **ha escluso che l'accesso delle autorità dello Stato di emissione ai dati intercettati relativi al servizio *EncroChat* tramite gli ordini europei di indagine emesso ex art. 6 della direttiva 2014/41/UE sia soggetto a criteri analoghi a quelli che regolano l'accesso ai dati conservati in applicazione dell'art. 15, par. 1, della direttiva 2002/58** relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Sono stati così ribaditi i diversi spazi operativi delle due direttive.

Secondo **l'art. 15 della direttiva 2002/58/UE**, come è noto, l'acquisizione di dati trattati dai gestori di comunicazioni elettroniche presuppone **sempre l'autorizzazione del giudice** (cfr. CGUE, 2 marzo 2021, *H.K. c. Prokuratuur*; CGUE 16 dicembre 2021, *Spetsializirana prokuratura*).

La trasmissione dei risultati delle intercettazioni già compiute in altro Stato membro, in forza di un provvedimento del giudice di tale Stato, invece, non necessità di OIE emesso da un giudice, dovendo escludersi, pertanto, una sovrapposizione delle due discipline.

Se ne trae una indiretta conferma che **la Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002 non concerne la disciplina delle intercettazioni.**

Essa, infatti, «lascia … inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della … direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale» e «… non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, come interpretata dalle sentenze della Corte europea dei diritti dell'uomo» (così il considerando n. 11 della direttiva).

La Direttiva 2002/58/CE riguarda il trattamento dei dati personali da parte dei fornitori dei servizi e, di conseguenza, la tutela della vita privata nel settore delle comunicazioni elettroniche, concetto che ricomprende anche la conservazione – c.d. *data retention* – e l'accesso ai metadati derivanti da telecomunicazioni elettroniche.

I metadati, anche denominati "dati di traffico" o "dati esterni alle telecomunicazioni", rappresentano "l'involucro delle comunicazioni elettroniche". Si tratta di informazioni raccolte dai fornitori di servizi di telecomunicazione per finalità di erogazione, di gestione e di fatturazione dei servizi e che non attengono al contenuto della comunicazione bensì al luogo (cioè, la cella di aggancio e la possibile – per quanto talvolta vaga e ampia – ubicazione del dispositivo telefonico), all'ora, alla data, alla durata e al destinatario di una comunicazione, unitamente all'identità dell'utilizzatore.

La Direttiva 2002/58/CE è stata adottata sul presupposto che la disponibilità di una enorme mole di dati conservati dai fornitori di servizi di comunicazione elettronica consente alle autorità pubbliche di "andare indietro nel tempo" e di reperire informazioni utili a scopi di prevenzione, indagine e repressione di minacce alla sicurezza pubblica e nazionale, svolgendo indagini "retrospettive". Per tale ragione, la disciplina europea ha accolto un approccio fortemente attento al rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati, anche a discapito della efficacia degli strumenti posti a garanzia della sicurezza.

Essa, più in particolare, si è resa necessaria per garantire i diritti fondamentali individuali e per evitare la realizzazione di forme di sorveglianza di massa; in altri termini, la disciplina in esame mira a circoscrivere le informazioni che i privati fornitori di servizi possono conservare ed il loro uso successivo a scopo di prevenzione, di indagine e di repressione di minacce alla sicurezza pubblica e nazionale. Si tratta di informazioni riguardanti soggetti previamente sconosciuti e non sospettati dalle forze dell'ordine e, dunque, non sottoposti a controlli specifici o intercettazioni dirette da parte dell'Autorità giudiziaria.

È netta allora la differenza tra le informazioni desumibili dai dati oggetto del trattamento da parte dei fornitori dei servizi e le intercettazioni che sono disposte per l'acquisizione di elementi probatori che emergeranno soltanto dopo l'autorizzazione del giudice, contestualmente all'esecuzione del mezzo di ricerca della prova e alla captazione di un flusso di dati elettronici in atto.

Su questo tema, appare opportuno segnalare che, la Corte europea, con una sentenza depositata nello stesso giorno di quella in commento, ha ulteriormente delimitato l'area operativa della direttiva 2002/58/CE affermando che «il diritto dell'Unione non osta a una normativa nazionale che autorizza l'autorità pubblica competente, al solo scopo di identificare la persona sospettata di aver commesso un reato, ad accedere ai dati relativi all'identità civile corrispondenti a un indirizzo IP, conservati separatamente e in maniera effettivamente stagna dai fornitori di accesso a Internet» (CGUE 30 aprile 2024, causa C-470/21, La Quadrature du Net e a.).

Quest'ultima decisione, considerata congiuntamente rispetto a quella in esame che, come si è visto, ha riconosciuto la competenza del pubblico ministero all'emanazione dell'OEI per acquisire le chat tratte dall'intercettazione criptofonini, pare segnare **una significativa evoluzione della giurisprudenza della Corte di Giustizia** sul tema della tutela dei dati personali rispetto alle affermazioni precedenti (il riferimento, in particolare, è a CGUE, 2 marzo 2021, *H.K. c. Prokuratuur*; CGUE 16 dicembre 2021, *Spetsializirana prokuratura*).

6. Nel caso delle intercettazioni, d'altra parte, il bilanciamento tra i diritti confliggenti è realizzato in concreto dal provvedimento autorizzativo del giudice.

A tal proposito, per quanto attiene al nostro ordinamento è stato affermato che «l'atto dell'autorità giudiziaria con il quale vengono autorizzate le intercettazioni telefoniche deve essere puntualmente motivato», ossia «deve avere una adeguata e specifica motivazione» (C. cost. n. 366/1991). Con la motivazione del decreto autorizzativo, il giudice deve chiarire le ragioni del provvedimento in ordine alla indispensabilità del mezzo probatorio ai fini della prosecuzione delle indagini ed alla sussistenza dei gravi indizi di reato, dando conto dei motivi che impongono l'intercettazione di una determinata persona ed indicando il collegamento tra questa e l'indagine in corso.

Questa prospettiva non sembra sia stata trascurata dalla Corte europea.

L'interpretazione delle norme della direttiva 2014/41/UE accolta nella sentenza in esame, infatti, distinguendo la base giuridica che disciplina l'autorizzazione del mezzo di ricerca della prova da quella che permette il trasferimento della prova, sottende anche **il rilievo centrale che presenta il principio del riconoscimento reciproco** nell'ambito della cooperazione giudiziaria europea.

Quando l'OIE è rivolto all'acquisizione di una prova già raccolta nello Stato di esecuzione, in detto Stato è necessariamente intervenuto un vaglio giurisdizionale. La Corte di giustizia, pertanto, non ha ritenuto necessario che anche l'OIE diretto alla sua acquisizione della prova già raccolta debba essere parimenti emesso da un giudice.

7. Il principio del riconoscimento reciproco delle sentenze e delle decisioni giudiziarie, invero, costituisce la chiave di lettura della sentenza illustrata.

Come è noto, esso costituisce la «pietra angolare» della cooperazione giudiziaria in materia penale, ed 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 (CGUE 8 dicembre 2020, Staatsanwaltschaft Wien, punto 40).

La Corte europea, infatti, ha significativamente sottolineato che le norme della direttiva 2014/41/UE vanno interpretate alla luce del fine perseguito dalle stesse consistente nella istituzione di **un sistema semplificato e più efficace** basato su un unico strumento denominato OEI, per facilitare e per accelerare la cooperazione giudiziaria al fine di contribuire a realizzare l'obiettivo assegnato all'Unione di diventare uno spazio di libertà, di sicurezza e di giustizia, fondandosi sull'elevato livello di fiducia che deve esistere tra gli Stati membri.

8. Passando ad affrontare le questioni che concernono le condizioni per l'emissione dell'OEI, infatti, la Corte ha affermato, con nettezza, che **la necessità e la proporzionalità dell'emissione dell'OEI**, richieste dall'art. 6, par. 1, della direttiva 2014/41/UE per l'acquisizione di una prova già raccolta nello Stato di esecuzione, **devono essere valutate unicamente alla luce del diritto dello Stato di emissione**.

Una diversa interpretazione, del resto, oltre a non corrispondere alla lettera della disposizione della direttiva, che circoscrivere la valutazione della sussistenza di tali presupposti al procedimento in cui è stato emesso l'OEI, contrasterebbe con il principio del mutuo riconoscimento, comportando un sindacato, nello Stato di emissione dell'attività di raccolta della prova intervenuta nello Stato di esecuzione.

9. L'art. 6, par. 1, della direttiva stabilisce che la necessità e la proporzionalità dell'emissione debba essere valutata «tenendo conto dei diritti della persona sottoposta a indagini o imputata».

Questa disposizione, secondo la sentenza in esame, non implica che l'emissione di un OEI diretto alla trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione debba essere necessariamente subordinata all'esistenza di **una presunzione**

di reato grave fondata su fatti concreti, a carico di ciascuna persona interessata, "*qualora un tale requisito non derivi dal diritto dello Stato di emissione*".

Il rispetto del principio di proporzionalità, inoltre, **non osta all'emissione di un OEI neppure nel caso in cui l'integrità dei dati ottenuti tramite l'intercettazione non possa essere verificata** a causa della riservatezza delle basi tecniche che hanno permesso l'attuazione di tale misura, purché **il diritto a un processo equo venga garantito nel corso del successivo procedimento penale**.

Si tratta di affermazioni nette che delineano l'area delle questioni sull'utilizzabilità della prova ottenuta con OEI che possono essere poste nello Stato di emissione.

10. In ordine al secondo presupposto dell'emissione, cioè al rispetto del principio di equivalenza, secondo la Corte, impiegando i termini «alle stesse condizioni» e «in un caso interno analogo», l'art. 6, par. 1, lettera b), della direttiva 2014/41 subordina **al solo diritto dello Stato di emissione la determinazione delle specifiche condizioni richieste per l'emissione di un OEI**.

Qualora un'autorità di emissione intenda acquisire prove già in possesso delle autorità competenti dello Stato di esecuzione, pertanto, tale autorità deve subordinare un OEI al rispetto di **tutte le condizioni previste dal diritto del proprio Stato per un caso interno analogo**.

La legittimità di un OEI diretto alla trasmissione di dati concernenti le comunicazioni già in possesso delle autorità competenti dello Stato di esecuzione, pertanto, è soggetta alle stesse condizioni applicabili, se del caso, alla **trasmissione di tali dati** in una situazione interna allo Stato di emissione.

Se il diritto dello Stato di emissione subordina tale trasmissione all'esistenza di indizi concreti di commissione di reati gravi da parte dell'imputato, l'adozione di un OEI è soggetta a queste condizioni.

Nell'ordinamento italiano, nel caso in cui il trasferimento delle conversazioni intercettate in un diverso procedimento trova applicazione l'art. 270 c.p.p. sicché, dopo la riforma di tale norma ad opera della legge 9 ottobre 2023, n. 137, che ha convertito il d.l. 10 agosto 2023, n. 105, occorre che i risultati delle intercettazioni eseguite *aliunde* siano **rilevanti e indispensabili** per l'accertamento di **delitti per i quali è obbligatorio l'arresto in fragranza di reato**.

Si tratta di presupposti, ai quali sembra abbiano fatto riferimento anche le Sezioni unite secondo quanto pare desumersi dalle informazioni provvisorie relative alle sentenze dapprima citate, che assicurano adeguatamente il bilanciamento tra i diritti individuali e l'interesse all'accertamento dei reati secondo una logica di proporzionalità fondata sulla necessità probatoria e sulla previsione di un catalogo di reati che, per la loro assoluta gravità, giustificano addirittura l'applicazione di una misura cd. "precautelare" come l'arresto in flagranza.

L'art. 6, par. 1, lettera b), della direttiva 2014/41, comunque, **non richiede** che **l'emissione di un OEI diretto alla trasmissione di prove già in possesso** delle autorità competenti dello Stato di esecuzione **sia soggetta alle stesse condizioni sostanziali applicabili, nello Stato di emissione, in materia di raccolta di tali prove**.

11. Secondo la sentenza in esame, l'autorità di emissione, in forza dell'art. 6 della direttiva, **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**.

La prova deve essere raccolta nello Stato di esecuzione la prova sulla base della *lex loci* ed i vizi eventualmente intervenuti non sono rilevabili nello Stato di emissione.

Se si ammettesse la possibilità di contestare la legittimità dell'attività svolta dalle autorità dello Stato di esecuzione, d'altra parte, **verrebbe irrimediabilmente incrinato il principio del mutuo riconoscimento delle decisioni e la fiducia** che ispira i rapporti tra gli Stati membri in tema di cooperazione penale, ammettendo che, tramite i principi di necessità, proporzionalità e equivalenza che governano le modalità di funzionamento dell'OEI, si possa valutare, in forza di regole interne, l'attività di raccolta della prova svolta in un altro Stato membro, ritenuta lesiva di prerogative fondamentali.

Ne consegue che, nel caso specifico dell'indagine sugli utilizzatori della rete di comunicazione *EncroChat*, sembra preclusa, tra l'altro, la possibilità di dedurre nei giudizi che si svolgono nello Stato di emissione le questioni sulla regolarità del procedimento di acquisizione della prova, tra le quali l'effettiva consistenza della base indiziaria in forza della quale le stesse sono state autorizzate (il sospetto che, per il solo uso di telefoni criptati, gli utenti fossero dediti a gravi reati), la legittimità dell'intercettazione tramite *trojan* (inoculato non in un dispositivo mobile, ma in un server) e anche la dimensione "massiva" delle intercettazioni (che hanno riguardato migliaia di utenti). Tali questioni sono state poste (o avrebbero dovuto essere poste) nei procedimenti dinanzi alle autorità francesi.

Possono invece essere poste le questioni con le quali si desume che l'OEI è stato emesso in modo illegittimo, violando il diritto dell'Unione, in particolare l'art. 6 della direttiva citata (cioè quelle relative al rispetto dei principi di necessità, proporzionalità ed equivalenza, anche sotto il profilo dell'equità del procedimento e dell'effettività del diritto di difesa).

Sembra emergere una significativa deviazione rispetto alla disciplina nazionale dell'acquisizione dei risultati delle intercettazioni eseguite in un diverso procedimento contenuta nell'art. 270 c.p.p.

Secondo l'orientamento giurisprudenziale consolidato, infatti, il giudice del procedimento diverso da quello nel quale sono state autorizzate le intercettazioni può rilevare i vizi di inutilizzabilità dei risultati delle stesse quando risultino dagli atti, gravando sulla parte interessata a farla valere l'onere di allegare e provare il fatto dal quale dipende l'eccepita inutilizzabilità, sulla base di copia degli atti rilevanti del procedimento originario che la parte stessa ha diritto di ottenere (Cass. pen., Sez. Un., n. 45189/2004, PM in proc. Esposito).

Quando il pubblico ministero ha ottenuto con OEI la trasmissione dei risultati di intercettazioni svolte in un altro Stato membro, invece, l'autorità giudiziaria dello Stato di emissione davanti alla quale sono utilizzate tali prove non è autorizzata a controllare la regolarità del procedimento con il quale esse sono state raccolte.

12. L'esclusione di un sindacato nello Stato di emissione sulla legittimità della raccolta della prova nello Stato di esecuzione, però, non incide sulla efficacia del controllo giurisdizionale del rispetto dei diritti fondamentali delle persone interessate.

Nello Stato membro di esecuzione, infatti, ai sensi dell'art. 14, par. 1, della direttiva 2014/41, **vanno assicurati mezzi di impugnazione** nei confronti degli atti richiesti nell'OEI **equivalenti a quelli disponibili in un caso interno analogo**.

L'art. 14, par. 2, della direttiva, infatti, stabilisce che «le ragioni di merito dell'emissione dell'OEI possono essere impugnate soltanto mediante un'azione introdotta nello Stato di emissione».

Sul punto, la Corte di Giustizia aveva già affermato che i presupposti di ammissibilità della prova oggetto di OEI possono essere posti in discussione contestando, nello Stato di emissione, il provvedimento di ammissione tramite una impugnazione (CGUE, 11/11/2021, Gavanozov, C-852/19). Trattandosi di OEI volto alla trasmissione di prove già raccolte, la questione della sua legittimità, però, non può essere posta nel momento dell'emissione dell'atto, ma va sollevata davanti al giudice competente dello Stato di emissione, il quale è tenuto a controllare il rispetto delle condizioni previste dalla direttiva nel momento in cui procede all'utilizzo della prova raccolta in un diverso Stato membro.

13. Nel procedimento penale avviato nello Stato di emissione, in particolare, ai sensi dell'art. 14, par. 7, della direttiva 2014/41, devono essere rispettati **i diritti della difesa** e **deve essere garantito un giusto processo** nel valutare le prove acquisite tramite tale OEI.

Su questi profili la Corte europea rinvia alle Corti nazionali, non senza precisare, in linea di principio, che «un organo giurisdizionale, qualora consideri che una parte non sia in grado di svolgere efficacemente le proprie osservazioni in merito a un elemento di prova idoneo ad influire in modo preponderante sulla valutazione dei fatti, deve constatare una violazione del diritto ad un processo equo ed escludere tale mezzo di prova al fine di evitare una violazione di questo tipo» (CGUE 2 marzo 2021, Prokuratuur, punto 44).

Spetta all'autorità giurisdizionale dello Stato membro di esecuzione, dinanzi al quale il dato raccolto in altro Stato membro è utilizzato come prova, **accertare eventuali violazioni del diritto ad un processo equo**, escludendo il mezzo di prova viziato.

L'utilizzo di espressioni come «svolgere efficacemente le proprie osservazioni» o «in modo preponderante», tuttavia, rende alquanto aperto il giudizio che deve essere compiuto dai giudici nazionali.

Calando questi principi nel nostro ordinamento, comunque, non pare che possa essere ritenuto leso il diritto di difesa per effetto della sola mancata conoscenza (e, dunque, dell'indisponibilità per la difesa) dell'algoritmo utilizzato per la decriptazione della messaggistica acquisita.

Il difensore dell'indagato, nell'ordinamento italiano, può, infatti, avere conoscenza solo del verbale delle operazioni di cui all'art. 268 c.p.p. e delle registrazioni, ma non anche dei mezzi tecnici, hardware e software, utilizzati per l'intrusione nelle conversazioni intercettate o per decodificare il contenuto.

Costituisce principio consolidato quello per cui, in tema di intercettazioni di flussi comunicativi, l'indisponibilità dell'algoritmo utilizzabile per la decriptazione dei dati informatici non determina alcuna lesione del diritto di difesa, perché l'interessato può avvalersi della procedura prevista dall'art. 268, commi 6 e 7, c.p.p. per verificare il contenuto delle captazioni, ma non può anche pretendere un controllo diretto mediante l'utilizzo esclusivo e non mediato del programma di decriptazione (Cass. pen., sez. VI, n. 14395/2018 dep. 2019, Testa, Rv. 275534).

L'art. 89 disp. att. c.p.p., come modificato con riferimento all'introduzione dei captatori informatici, d'altra parte, prevede che debba essere indicato nel verbale delle operazioni solo il tipo di programma di intrusione utilizzato, dovendo adoperarsi solo quelli conformi ai requisiti tecnici stabiliti al Ministero della giustizia; non è, invece, previsto che sia reso disponibile il contenuto del programma utilizzato, di norma di proprietà di soggetti privati.

Nell'ordinamento interno la conoscibilità delle eventuali tecniche di hackeraggio, del resto, sarebbe preclusa dal "segreto industriale" del proprietario del software utilizzato per l'operazione di intrusione.

In ogni caso, la violazione dell'art. 268, commi 6 e 7, c.p.p. non rientra tra le cause di inutilizzabilità dell'intercettazione contemplate dall'art. 271 c.p.p.

Resta ferma la possibilità per la difesa di **dedurre**, sulla base di ragioni specifiche, **anomalie tecniche in grado di fare dubitare della correttezza delle acquisizioni** e dell'inquinamento del risultato probatorio e, in tal caso, il correlativo obbligo, per l'autorità giudiziaria, di promuovere accertamenti sul punto.

Su questo punto, deve rilevarsi che i singoli utilizzatori dei criptofonini posseggono i messaggi "in chiaro", potendo, pertanto, per esempio depositando le schermate, produrre almeno un principio di prova che possa lasciare diffidare della correttezza delle decodificazioni.