PENALE
Diritto e Procedura

LA CIRCOLAZIONE TRANSFRONTALIERA DELLE PROVE ELETTRONICHE

Gabriella Di Paolo

Sommario: 1. Premesse definitorie. – 2. Archetipi tradizionali. – 3. … e il superamento della cooperazione giudiziaria orizzontale. – 4. Sfide future.

1. Premesse definitorie

Com'è noto, per effetto dei mutamenti sociali indotti dall'avvento delle nuove tecnologie, le indagini digitali hanno ormai assunto un ruolo primario nella repressione di qualunque tipo di reato. La maggior parte delle indagini penali comporta, infatti, il sequestro e la successiva analisi di *device* digitali (smartphone e computer portatili) e dei dati in essi contenuti[1]. Inoltre, l'immaterialità dei dati e la diffusione globale delle reti informatiche e degli strumenti digitali implica sempre più spesso la necessità di operazioni investigative di carattere transnazionale, alla ricerca di dati ubicati al di fuori del territorio nazionale (ad esempio, in quanto conservati in *server* stranieri)[2].

Proprio in considerazione della vocazione transnazionale delle indagini digitali, il presente contributo si propone di tratteggiare i modelli di circolazione transfrontaliera di prove elettroniche che si sono sviluppati nel contesto dell'Unione europea, anche alla luce delle più recenti novità istituzionali e normative.

Premessa concettuale del quadro che si intende tracciare è una nozione ampia di "prova elettronica", da intendersi come '*ogni informazione generata, trasmessa, conservata o processata in forma elettronica – e quindi e che può essere utilizzata per provare un fatto nel processo penale*': in altre parole, ogni dato generato, trasmesso, trattato o

conservato da *computer* o altri dispositivi informatici/elettronici e codificato in codice binario. All'evidenza, una simile accezione è in grado di ricomprendere un'ampia gamma di dati, di natura assai composita. Vi restano inclusi, infatti, i *file* che conserviamo nei nostri *device* personali (ad esempio, *e-mail*, messaggistica, fotografie, *file* audio e video, etc.), ma anche i dati conservati dai fornitori di servizi (*service providers*) (ad esempio, i dati relativi ai titolari di certi abbonamenti, i c.d. "dati di traffico" e anche i dati relativi al contenuto delle comunicazioni) nonché, infine, i dati "dinamici", ossia i flussi informativi in transito nella rete o dei dispositivi, oggetto di captazione in tempo reale. E ciò indipendentemente dal fatto che essi siano protetti da crittografia e, quindi, non intellegibili[3].

2. Archetipi 'tradizionali'

Sulla scorta della modellistica astratta elaborata dalla dottrina in materia di circolazione transnazionale di prove penali[4], è possibile distinguere quattro diverse forme di acquisizione transfrontalieradi *e-evidence.*

Le prime due emergono nel caso EncroChat[5], una *data-driven investigation*[6] divenuta oggetto di un intenso dibattito in molti Paesi europei[7], Italia compresa, come confermano le recenti pronunce della Corte di cassazione in materia di criptodati[8].

Com'è noto, EnchroChat era una piattaforma di comunicazioni criptate operante a livello globale. Essa prometteva ai suoi utenti lo scambio sicuro di messaggistica offrendo i c.d. "cripotofonini", ovvero smartphone appositamente modificati nel *software* per garantirne l'inviolabilità grazie ad un sistema di criptazione *end to end*. Proprio perchè garantiva un altro livello di sicurezza e anonimato agli utenti[9], tale piattaforma era divenuta molto popolare tra le organizzazioni criminali.

In questo caso la prova elettronica oggetto di scambio transfrontaliero consisteva nella messaggistica (parliamo di oltre 120 milioni di messaggi, quindi, una mole immensa di dati) scambiata dagli esponenti di alcune organizzazioni criminali grazie al possesso dei suddetti "criptofonini". L'apprensione della messaggistica era avvenuta all'esito di un'operazione investigativa svolta da una squadra investigativa comune (SIC) costituita dalle autorità giudiziarie francesi, olandesi e belghe. Quanto alle modalità acquisitive, pare che le autorità francesi siano entrate in possesso di alcuni "criptofonini" tramite agenti *undercover*. Ciò avrebbe consentito – verosimilmente anche grazie all'impiego di un captatore informatico o altre tecniche di *hacking*,non del tutto chiarite – la captazione di milioni di messaggi già scambiati sulla piattaforma criptata e memorizzati nel *server* francese (dati c.d. "freddi"). Una volta acquisiti tali dati, espressi in forma di «stringhe informatiche redatte secondo il sistema binario»[10], era stato poi necessario procedere alla loro decriptazione, al fine di renderli intelligibili[11].

A indagine conclusa, in molti Paesi europei – Italia compresa – è emersa la necessità di acquisire la messaggistica così ottenuta ai fini di procedimenti interni, per lo più per reati di traffico di stupefacenti. In diverse occasioni è stato quindi emesso un ordine di indagine europeo avente ad oggetto la trasmissione dei dati **autonomamente** acquisiti dalle autorità francesi. In relazione al dato probatorio così ottenuto, posto alla base di numerosi provvedimenti cautelari, è insorto un vivace dibattito: si discute anzitutto su quale sia la natura giuridica delle attività acquisitive (intercettazioni, prova documentale *ex* art. 234 c.p.p. oppure acquisizione di documenti e dati informatici *ex* art. 234-bis c.p.p.) e il corredo di garanzie procedimentali che avrebbe dovuto assisterle; non è chiaro nemmeno se sia possibile, per il giudice italiano, sindacare la legittimità dell'operato dell'autorità giudiziaria straniera[12].

Non è questa la sede per addentrarsi in tali complesse questioni, su cui sono state chiamate a pronunciarsi, nell'analogo caso Sky ECC, le sezioni unite della Cassazione[13]. Per ciò che qui interessa, sullo sfondo di questa vicenda giudiziaria possono intravedersi due modelli, per così dire, "tradizionali" di circolazione probatoria.

Il primo è costituito dal semplice "trasferimento probatorio"[14]. Secondo tale archetipo uno Stato chiede a un altro Stato la trasmissione di elementi probatori di cui l'autorità giudiziaria straniera è già venuta autonomamente in possesso ai fini di un procedimento interno e, quindi, "precostituiti". Si tratta di un fenomeno già noto a livello

interno, in quanto disciplinato nell'art. 238 c.p.p. e, relativamente all'acquisizione di atti di un procedimento straniero, dall'art. 78 disp. att. c.p.p.[15].

Il secondo modello, più complesso, è costituito dalla "raccolta transnazionale della prova". In virtù di tale schema, uno Stato commissiona ad un altro Stato (mediante rogatoria, ordine europeo di indagine, oppure, ancora, richiedendo la costituzione di una squadra investigativa comune) il compimento di una specifica attività probatoria[16] in relazione ad un procedimento penale in corso. In questo caso, l'eterno problema – dovuto al fatto che manca a tutt'oggi un'armonizzazione, seppur minima, delle discipline probatorie nazionali – è quello della utilizzabilità della prova allogena e, a monte, quello della disciplina applicabile per la sua raccolta (*lex loci* o *lex fori*). Si tratta di una criticità in parte affievolita dall'ibridismo[17] che connota il sistema dell'ordine europeo di indagine penale (O.E.I.), nell'ambito del quale, per assicurare la spendita del 'risultato' probatorio raccolto *ultra fines,* si prevede espressamente la possibilità che la prova sia confezionata dall'autorità di esecuzione secondo le "indicazioni" formali e procedurali richieste dall'autorità emittente, con sostanziale prevalenza della *lex fori.* Altro aspetto degno di nota è l'espresso riferimento, nella direttiva relativa all'O.E.I., al principio di proporzionalità, elevato a parametro di controllo sulla legittimità dell'attività probatoria richiesta, sia per l'autorità di emissione che per l'autorità di esecuzione[18].

3. …e il superamento della cooperazione giudiziaria orizzontale.

In tempi più recenti, per effetto dei nuovi assetti che ha assunto lo spazio europeo di libertà, sicurezza e giustizia dopo il Trattato di Lisbona, si stanno delineando anche ulteriori moduli di circolazione transnazionale della *e-evidence.*

Il primo fenomeno è legato all'istituzione della Procura europea (*European Public Prosecutor's Office,* EPPO)[19] e alla conseguente possibilità che vengano compiute "indagini transfrontaliere". Rispetto a tale evenienza, che si verifica quando la misura investigativa deve essere intrapresa in uno Stato diverso da quello del Procuratore europeo delegato (PED) incaricato del caso, l'art. 31 del Regolamento 2017/1939 prevede che quest'ultimo decida in merito all'adozione della misura e poi la assegni a un Procuratore europeo delegato avente sede nello Stato membro dove essa dovrà essere eseguita (il c.d. PED incaricato di prestare assistenza), conformemente al regolamento e al diritto interno dello Stato di esecuzione[20].

Siamo al cospetto di uno schema concettuale radicalmente diverso da quelli precedentemente esaminati. In questa eventualità, la raccolta probatoria *ultra fines* rispetto al foro di avvio dell'indagine[21] è infatti affidata a una differente articolazione territoriale del medesimo organismo requirente sovranazionale. Inoltre, per come è stata concepita la Procura europea, gli esiti dell'indagine transfrontaliera sono destinati a rifluire in un procedimento penale assomigliante a quello puramente interno, in seguito all'esercizio dell'azione penale eurounitaria dinanzi agli organi giurisdizionali competenti degli Stati membri (art. 86 § 4 Trattato funz. UE). Anche in questo caso potrebbe porsi il problema dell'utilizzabilità della prova elettronica confezionata all'estero, poiché il *favor auxilii**[22]*** desumibile dagli artt. 31 e 37 del Regolamento 2017/1939 non giunge sino al punto di imporre in ogni caso l'ammissione della prova raccolta al di fuori del territorio nazionale[23] (consentendo, invero, la sua esclusione per ragioni differenti dalla mera difformità rispetto al regime probatorio interno)[24]. In tale prospettiva potrebbe assumere valenza dirimente quanto sancito recentemente dalla Corte di giustizia dell'Unione europea nella prima sentenza concernente il Regolamento 2017/1939[25], a seguito di un rinvio pregiudiziale da parte del *Oberlandesgericht* di Vienna[26] con riferimento agli artt. 31 e 32 del Regolamento, in materia di controllo giurisdizionale sulle indagini transfrontaliere. Infatti, dopo aver stabilito – con riguardo alle misure investigative per le quali è necessaria un'autorizzazione giudiziaria ai sensi del diritto del PED incaricato di prestare assistenza – un netto riparto di competenze sulla falsariga di quanto previsto per l'O.I.E.[27], la Corte ha aggiunto un interessante elemento: la necessità, per certe misure investigative (ossia quelle particolarmente intrusive, come le perquisizioni in abitazioni private, le misure cautelari relative a beni personali e il "congelamento" dei beni), di un'autorizzazione giudiziaria

preventiva nello Stato del PED incaricato del caso[28]. Si tratta di un requisito di cui non c'è traccia nel Regolamento e che potrebbe comportare problemi in quegli Stati membri, Italia compresa, che legittimano l'esecuzione di perquisizioni e sequestri probatori soltanto sulla base di un decreto motivato del pubblico ministero.

Il secondo modulo – ed ecco l'ultima, nuova frontiera in tema di circolazione transnazionale della *e-evidence* – è invece legato all'approvazione, nel luglio 2023, dopo anni di negoziati, del Regolamento 2023/1543, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive nei procedimenti penali[29]. Il regolamento in discorso – che entrerà in vigore nel luglio 2026 [30] – sembra davvero inaugurare una nuova era, in quanto configura moduli di circolazione delle "prove elettroniche" [31] che prescindono dai tradizionali meccanismi cooperazione orizzontale e, quindi, da un dialogo fra autorità giudiziarie. Infatti, al fine di acquisire i dati conservati all'estero da un prestatore di servizi nell'Unione, le autorità competenti (non necessariamente un giudice)[32] non dovranno più chiedere l'intervento delle autorità giudiziarie dello Stato di esecuzione[33], ma potranno – sulla base del principio del mutuo riconoscimento, a certe condizioni e se previsto o consentito per casi interni analoghi[34] – rivolgersi direttamente al prestatore di servizi straniero, per ingiungergli di produrre (o conservare)[35], nei termini specificati, dati di varia natura e precisamente dati relativi agli abbonati[36], dati sul traffico[37] oppure dati di qualsiasi natura, anche relativi al contenuto[38]. Pure in questo caso il modulo procedimentale non è completamente inedito, poiché ricalca il fenomeno disciplinato dal c.d. "codice privacy" per l'acquisizione dei c.d. "tabulati telefonici", con l'importante differenza la normativa interna si riferisce esclusivamente ai gestori presenti sul territorio nazionale e ai dati esterni delle comunicazioni, mentre il Regolamento 2023/1543 si riferisce anche ai dati relativi al contenuto.

4. Sfide future

I moduli di circolazione della prova elettronica poc'anzi rapidamente delineati dimostrano come l'Unione europea sia intervenuta - a più riprese e a diversi livelli, conformemente al principio di sussidiarietà – essenzialmente per assicurare un sistema efficiente e globale di acquisizione transfrontaliera della prova, al fine di agevolare la circolazione probatoria nello spazio giudiziario europeo. Ciò nonostante, il "tema dei temi" – ossia il regime concernente l'ammissibilità della prova e la sua utilizzabilità – resta una sorta di giardino proibito per il legislatore sovranazionale, non essendo stata intrapresa, a tutt'oggi, alcuna forma di armonizzazione, anche minima, delle discipline probatorie nazionali[39].

Eppure, è noto che, a dispetto della c.d. "europeizzazione" della procedura penale, continuano a sussistere profonde differenze tra i sistemi processuali degli Stati membri, e che tali divergenze rischiano non solo di compromettere l'efficacia delle "nuove forme" di cooperazione giudiziaria, ma anche di ostacolare la protezione dei diritti fondamentali delle persone che, direttamente o indirettamente, diventano bersaglio di indagini digitali.

Nella prospettiva – evocata dal titolo di questo convegno – di costruire un nuovo statuto dei mezzi investigativi nella società digitale, va quindi guardato con grande attenzione un recente studio dello *European Law Institute,* che ha elaborato una bozza di proposta di direttiva UE[40] sulla reciproca ammissibilità delle prove, comprese quelle elettroniche, nei procedimenti penali, con l'obiettivo di fissare norme comuni per l'ammissione delle prove transfrontaliere, affinché gli elementi probatori raccolti in uno Stato membro non siano esclusi soltanto perché non conformi alle regole e alle formalità previste dallo Stato membro in cui si svolge il processo.

Certo, si tratta soltanto di una proposta elaborata da un gruppo di studiosi[41] ed è verosimile pensare che difficilmente essa coagulerà il consenso politico della Commissione e delle altre istituzioni europee, non essendo forse ancora maturi i tempi per un'azione sovranazionale di armonizzazione delle procedure penali degli Stati membri in materia probatoria[42]. Tuttavia, per l'attenzione prestata alle specificità della *e-evidence* (connotata da immaterialità, volatilità, alterabilità e riproducibilità illimitata)[43] e per la conseguente previsione di regole minime volte ad assicurare, tra l'altro, a) la piena attuazione degli *standard* comuni di informatica forense (*digital forensics*)

nella sua acquisizione [44], b) il diritto a verificare la c.d. catena di custodia[45] e c) l'applicazione del principio di proporzionalità[46], non v'è dubbio che tale studio possa offrire preziosi spunti di riflessione. Questi ultimi, difatti, si rivelano estremamente utili anche nella prospettiva domestica, per elaborare uno statuto speciale degli strumenti investigativi a caratura tecnologica[47] capace di bilanciare le necessità dell'accertamento penale con l'esigenza di evitare un sacrificio sproporzionato del diritto fondamentale alla tutela dei dati personali: in altre parole, per costruire di una disciplina in grado di assicurare l'*habeas data**[48]*, inteso quale base fondativa dei diritti di libertà della persona nella dimensione immateriale dell'infosfera.

**** Contributo tratto dalla relazione svolta nell'ambito del Convegno "Per uno statuto dei nuovi mezzi di ricerca della prova di fronte alla società digitale" tenutosi a Roma, il data 22 settembre 2023, aggiornato al marzo 2024.***

---

[1] G. Di Paolo, voce *Prova informatica (diritto processuale penale*), in *Enciclopedia del Diritto, Annali,* vol. VI, Giuffrè, Milano, 2013, p. 736 ss.

[2] Per un'accurata disamina delle trasformazioni morfologiche delle indagini penali a fronte delle nuove tecnologie, cfr. S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* Giappichelli, 2918, p. 3 ss.

[3] Sul punto, cfr., volendo, G. Di Paolo, *Admissibility of E-Evidence, Transnational E-Evidence and Fair-Trial rights in Italy*, in L. Bachmaier Winter – F. Salimi (a cura di) *Admissibility of Evidence in EU Cross-Border Criminal Proceedings Electronic Evidence, Efficiency and Fair Trial Rights,* in corso di pubblicazione per la Oxford University Press (OUP).

[4] Cfr. S. Allegrezza, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo,* in T. Rafaraci (a cura di), *L'area di liberà, sicurezza e giustizia: alla ricerca di un equilibrio tra priorità repressive ed esigenze di garanzia,* Giuffrè, Milano, 2007, p. 708 ss.

[5] L'operazione EncroChat, così come l'operazione Sky ECC di poco successiva, non sono state le prime indagini avente ad oggetti i c.d. "criptofonini" ma rappresentano senz'altro le più note in ambito europeo, se non altro perché in entrambi i casi server erano collocati in Francia e l'acquisizione massiva di dati ha toccato migliaia di cittadini europei. Il fenomeno dell'impiego dei "criptofonini" era infatti già emerso nelle operazioni concernenti i casi Ennetcom (del 2016, con server situati in Canada), PGP Safe (del 2017, con server situati in Costa Rica), IronChat (del 2018, con server situati in Olanda; cfr. https://www.wired.it/internet/web/2018/11/12/olanda-polizia-messaggi-criptati/) e ANoM (del 2018, che si distingueva dai casi precedenti in quanto l'app di comunicazione protetta da criptazione era stata fornita ai criminali dagli stessi agenti sotto copertura; cfr https://www.ilriformista.it/che-cose-anom-lapp-utilizzata-dallfbi-nelloperazione-ironside-per-infiltrare-la-criminalita-organizzata-225036/).

[6] Per questa espressione, cfr. Jan-Jaap Oerlemans, Sofie Royer*, The future of data-driven investigations in light of the Sky ECC operation,* in *New Journal of European Criminal Law* 2023, Vol. 14(4) pp. 434–458.

[7] Le operazioni EncroChat e Sky ECC hanno suscitato dubbi di legittimità, ad esempio, in Olanda, Norvegia e Germania. Per un quadro di sintesi degli approdi giurisprudenziali in tali Paesi, cfr. Georgios Sagittae, *On the lawfulness of the EncroChat and Sky ECC-operations, in New Journal of European Criminal Law*, 2023, Vol. 14(3), p. 273–293, spec. 279; v. anche J.J. Oerlemans - S. Royer, *The future of data-driven investigations in light of the Sky ECC operation, New Journal of European Criminal Law 2023, Vol. 14(4)* pp. 434–458.
In Germania, la corte regionale di Berlino (*Staatsanwaltschaft Berlin*) ha anche sollevato un rinvio pregiudiziale

davanti alla Corte di Giustizia (*Staatsanwaltschaft Berlin (EncroChat) v M.N,* Causa C-670/22), ponendo varie questioni interpretative della direttiva 2014/41/EU con riferimento a un ordine di indagine penale emesso dalla Procura Generale di Francoforte (*Generalstaatsanwaltschaft Frankfurt am Main)* per chiedere alle autorità francesi l'autorizzazione a utilizzare senza restrizioni i dati di EncroChat in procedimenti penali. Alla base della richiesta della Procura tedesca sussisteva il sospetto che un gran numero di reati molto gravi (in particolare, l'importazione e il traffico di sostanze stupefacenti in grandi quantità) venisse commesso in Germania, da persone non ancora identificate, utilizzando i telefoni EncroChat. Il Tribunale penale di Lille autorizzava il trasferimento e l'utilizzo in sede giudiziaria dei dati EncroChat degli utenti tedeschi. Durante il processo, l'imputato (accusato appunto di traffico e detenzione illeciti di sostanze stupefacenti) sosteneva l'inutilizzabilità dei dati acquisiti, perché ottenuti illegittimamente in Francia. Per una sintesi del rinvio pregiudiziale, cfr. T. Whal, *EncroChat Turns into a Case for the CJEU,* in Eucrim, 18 November 2022.Per la posizione dell'Avvocato Generale Tamara Ćapeta, presentate il 26 ottobre 2023, cfr. T. Whal, *AG: EncroChat Data Can, in Principle, Be Used in Criminal Proceedings,* in Eucrim, 8 February 2024. La decisione della Corte di Giustizia è attesa per il 30 aprile 2024.

[8] Ad esempio, cfr. Cass., sez. VI, sent. 26 ottobre 2023 n.44154, Iaria, in *CED Cass*. m. 285284-01, secondo la quale, in tema di ordine europeo di indagine, l'oggetto dell'acquisizione all'estero della messaggistica criptata sulla piattaforma SKY-ECC non costituisce dato informatico utilizzabile ai sensi dell'art.234-*bis* c.p.p., sicché, in tale ipotesi, l'attività acquisitiva, se riguardante comunicazioni avvenute nella fase "statica", deve essere inquadrata nelle disposizioni in materia di perquisizione e sequestro e, in particolare, in quella di cui all'art. 254-*bis* c.p.p., mentre se avente ad oggetto comunicazioni avvenute nella fase "dinamica", deve essere inquadrata nella disciplina degli artt. 266 e ss. c.p.p. in materia di intercettazioni telefoniche; *contra*, cfr. Cass. sez. III, 3 sent. 19 ottobre 2023, n. 47201, Bruzzaniti, in *CED Cass*. m. 285350 – 01 e Cass., sez. I, sent. 13 ottobre 2022 n. 6364/2023, Calderon Raul Esteban, in *CED Cass*. m. 283998 – 01, secondo le quali la messaggistica relativa a "chat" di gruppo sulla piattaforma SKYECC, acquisita mediante ordine europeo di indagine da autorità giudiziaria straniera che ne abbia eseguito la decriptazione, costituisce dato informativo documentale conservato all'estero, utilizzabile ai sensi dell'art. 234-*bis* c.p.p. e non flusso comunicativo, sicché non trova applicazione la disciplina delle intercettazioni di cui agli artt. 266 e 266-*bis* c.p.p. Dato il contrasto insorto in merito all'utilizzabilità delle chat ottenute dal pubblico ministero nella forma già decriptata mediante ordine europeo di indagine rivolto all'autorità giudiziaria francese, la questione è stata rimessa alle sezioni unite (cfr. Cass., sez. III, ord. 3 novembre 2023 n. 47798, (dep. 30 novembre 2023); v. anche Cass., sez. VI, ord. 15 gennaio 2024 n. 2329, (dep. 18 gennaio 2024), incidente sui medesimi temi oggetto della prima pronuncia, con la quale sono state poste alle sezioni unite ulteriori questioni. Le due ordinanze, insieme alle memorie della Procura Generale, sono reperibili in *Sistema Penale,* 1° marzo 2024, https://www.sistemapenale.it/it/notizie/criptofonini-le-decisioni-delle-sezioni-unite-e-la-memoria-della-procura-generale). Per un quadro approfondito dei vari orientamenti giurisprudenziali, cfr. la memoria per l'udienza delle sezioni unite penali del 29 febbraio 2024 della Procura generale della Corte di cassazione, in *Sistema penale,* 1° marzo 2024, in https://www.sistemapenale.it/it/notizie/criptofonini-le-decisioni-delle-sezioni-unite-e-la-memoria-della-procura-generale.

[9] Di solito, i sistemi smantellati dalle forze dell'ordine si basavano sull'impiego di un'apposita APP per la comunicazione criptata, la quale veniva installata su dispositivi modificati e privi di altre funzionalità, acquistabili solo sul mercato nero. Tali telefoni potevano comunicare solo con dispositivi analoghi attraverso messaggi crittografati e registrare video. Niente telefonate, messaggi o mail.

[10] Così si esprime, Cass., sez. I, sent. 13 ottobre 2022 n. 2851, Calderon Raul Esteban, cit.

[11] Nel caso EnchoChat il *tool* di decriptazione è stato sviluppato e impiegato, a valle dell'acquisizione dei messaggi, dalle sole autorità francesi. Diversamente, nell'analoga operazione Sky ECC, lo strumento di decriptazione è stato predisposto prima di iniziare le attività di captazione e grazie alla collaborazione di tutti i Paesi

coinvolti nella costituzione della SIC, cioè Olanda, Francia e Belgio. Cfr. Georgios Sagittae, *On the lawfulness of the EncroChat and Sky ECC-operations, in New Journal of European Criminal Law*, 2023, Vol. 14(3) 273–293.

[12] Per una efficace sintesi, v. M. 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).

[13] Come anticipato, con ord. 3 novembre 2023 n. 47798, la sezione III della Corte di cassazione ha rimesso alle sezioni unite le seguenti questioni:

i) se "l'acquisizione di messaggi su *chat* di gruppo scambiati con sistema cifrato, mediante OEI, presso autorità giudiziaria straniera che ne ha eseguito la decrittazione costituisca acquisizione di 'documenti e di dati informatici' ai sensi dell'art. 234 *bis* c.p.p. o di documenti *ex* art. 234 c.p.p. o sia riconducibile in altra disciplina relativa all'acquisizione di prove";

ii) "se inoltre, tale acquisizione debba essere oggetto, ai fini della utilizzabilità dei dati in tal modo versati in atti, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte dell'autorità giurisdizionale nazionale".

In base all'informazione provvisoria delle S.U. sulla decisione assunta il 29 febbraio 2024 (Cass., sez. un., c.c. 29 febbraio 2024, Gjuzi), sembra che il Supremo consesso abbia riconosciuto l'utilizzabilità in Italia degli atti trasmessi dalla Francia (in esecuzione di un ordine europeo di indagine penale) relativi al contenuto di comunicazioni effettuate attraverso criptofonini, già acquisite e decriptate dall'autorità giudiziaria estera in un proprio procedimento penale. Si è in attesa del deposito della motivazione. Per un primo commento dell'informazione provvisoria, cfr. L. Filippi, *Le S.U. ammettono le prove francesi sui criptofonini acquisite con l'ordine europeo di indagine*, in *Pen. Dir. Proc*, 1° marzo 2024, in https://www.penaledp.it/.

[14] Per analoghe osservazioni, cfr. S. Allegrezza, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo,* in T. Rafaraci (a cura di), *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio tra priorità repressive ed esigenze di garanzia,* Milano, 2007, p. 708 ss.

[15] Allo schema del trasferimento probatorio può forse ricondursi anche lo scambio transnazionale di informazioni assicurato dal collegamento in rete di banche dati nazionali, come accade con ECRIS, con le banche dati nazionali del DNA e con i registri nazionali contenenti dati dattiloscopici o dati di immatricolazione dei veicoli. Anche in tale evenienza si tratta, infatti, di acquisire informazioni in formato elettronico già autonomamente elaborate e conservate, anche a prescindere da un procedimento penale, in altro Paese dell'Unione europea, con la peculiarità che il trasferimento non avviene tramite i consueti meccanismi di cooperazione giudiziaria, ma grazie alla possibilità di consultazione *on-line* dell'archivio straniero (la c.d. "consultazione automatizzata di dati"). Cfr., volendo, G. Di Paolo, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in *Cass. pen.,* 2010, pp. 1969-1989; Ead., *La circolazione dei dati personali e del casellario giudiziario*, in *Cass. pen.,* 2011, pp. 4034-4048. Il quadro normativo di riferimento in materia di consultazione e lo scambio automatizzati di dati è radicalmente cambiato dopo il Trattato di Lisbona. Cfr., da ultimo, il Regolamento (UE) 2024/982 del Parlamento europeo e del Consiglio del 13 marzo 2024 sulla consultazione e lo scambio automatizzati di dati per la cooperazione di polizia e che modifica le decisioni 2008/615/GAI e 2008/616/GAI del consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio (regolamento «Prüm II»).

[16] Può trattarsi, ad esempio, di perquisizioni, sequestri, intercettazioni, oppure della raccolta di prove dichiarative, oppure, ancora, dell'acquisizione di informazioni o documenti presso istituzioni bancarie etc.

[17] Parla di "sincretismo", M. Caianiello, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Proc. Pen. Giust.,* 3/2015, p. 3.

[18] Cfr. M. Caianiello, *La nuova direttiva UE sull'ordine europeo di indagine penale*, cit.,p. 6 e ss.; volendo, cfr. anche G. Di Paolo, sub *Art. 9 d. lgs. n. 108/2012 (Ordine di indagine europeo, Particolari modalità di esecuzione)* in

A. Giarda- G. Spangher (a cura di), *Codice di procedura penale commentato,* Milano, 2023, IV, p. 2749-2759.

[19] In tema, v. R.E. Kostoris *Gli organismi centralizzati della cooperazione giudiziaria*, in R. E. Kostoris (a cura di), *Procedura penale europea*, 5° ed., Milano, 2022, pp. 287-305; L. Bachmaier Winter (ed.), *The European Public Prosecutor's Office*, Cham, 2018; cfr., volendo, anche G. Di Paolo – L. Pressacco – T. Rafaraci – R. Belfiore (a cura di), *L'attuazione della Procura europea. I nuovi assetti dello spazio europeo di libertà, sicurezza e giustizia,* Napoli, 2022.

[20] Hans-Holger Herrnfeld, *Article 31*, in H-H. Herrnfeld, D. Brodowski, C. Burchard (eds.), *European Public Prosecutor's Office: EPPO Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office. Article-by-Article Commentary*, München, 2021, p. 282 ss.

[21] Foro individuato in applicazione delle disposizioni sul riparto delle competenze all'interno dell'EPPO, ai sensi dell'art. 26 del Regolamento 2017/1939.

[22] Poiché l'azione transfrontaliera si risolve in un dialogo tra colleghi dell'ufficio di procura, essa prescinde da procedure di cooperazione e, in particolare, dall'impiego di strumenti basati sul mutuo riconoscimento (salvo l'uso del MAE e il caso previsto dall'art. 31 § 6 Reg. *EPPO*). Pertanto, l'art. 31 del Regolamento 2017/1939 non prevede vere e proprie forme di rifiuto di compiere l'atto da parte del PED chiamato a fornire assistenza. Inoltre, nel *considerando* n. 80, a chiarimento dell'art. 37 del Regolamento 2017/1939, si dice che è «*necessario* che le prove presentate dall'EPPO all'organo giurisdizionale non siano considerate inammissibili per il solo motivo che sono state raccolte in un altro Stato membro o conformemente al diritto di un altro Stato membro», ferma restando la tutela dei diritti fondamentali. Nell'insieme, il sistema EPPO sembra dunque basato sulla propensione a favorire l'assistenza reciproca e l'utilizzabilità degli elementi di prova raccolti all'estero.

[23] Ai sensi dell'art. 37, §1 del Regolamento 2017/1939, «le prove presentate a un organo giurisdizionale dai procuratori dell'EPPO o dall'imputato non sono escluse per il solo motivo che sono state raccolte in un altro Stato membro o conformemente al diritto di un altro Stato membro».

[24] Ad esempio, perché raccolta in violazione della *lex loci,* oppure in quanto in contrasto con il sistema di valori che permea lo Stato dove si celebra il processo. Cfr. A. Mangiaracina, *Dalle indagini all'ammissione della prova in giudizio,* in G. Di Paolo – L. Pressacco – R. Belfiore – T. Rafaraci (a cura di), *L'attuazione della Procura europea: i nuovi assetti dello spazio europeo di libertà, sicurezza e giustizia", Atti del convegno del 26 novembre 2021,* Napoli, 2022, p. 221 ss., la quale osserva che una possibile soluzione rispetto a tali problematiche potrebbe essere l'applicazione della *lex fori*, sulla falsariga di quanto previsto per l'O.E.I.

[25] Si allude alla decisione della Corte di Giustizia dell'Unione Europea, Grande Camera, sentenza 21 dicembre 2023, C-281/22, *G.K. e altri* (*Parquet européen*)*,* ECLI:EU:C:2023:1018), intervenuta nelle more della pubblicazione del presente contributo.

[26] Nel caso da cui è scaturito il rinvio pregiudiziale, il *PED* Monaco di Baviera aveva disposto una perquisizione nei locali di una società austriaca. L'ordine di perquisizione e sequestro era stato convalidato dal Gip di Monaco, come previsto dalla normativa processuale tedesca. Il *PED* austriaco chiamato a prestare assistenza aveva disposto la perquisizione e ne aveva chiesto la convalida al proprio Gip, come previsto dal codice di rito austriaco, ma gli imputati hanno contestato la decisione di convalida davanti alla Corte di Appello di Vienna lamentando la mancanza di sufficienti indizi a proprio carico. La Corte di Appello di Vienna ha posto dunque alla Corte di giustizia le seguenti questioni:

1. Se il diritto dell'Unione, in particolare l'articolo 31, paragrafo 3, primo comma, e l'articolo 32 del regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO»), debba essere interpretato nel senso che, nel caso di

indagini transfrontaliere, qualora occorra l'autorizzazione giudiziaria di una misura da eseguire nello Stato membro del procuratore europeo delegato incaricato di prestare assistenza, è necessario un esame di tutti gli elementi giuridici sostanziali, quali la responsabilità penale, gli indizi di reato, la necessità e la proporzionalità.

2. Se l'esame debba tener conto del fatto che l'ammissibilità della misura è già stata oggetto di un controllo giurisdizionale nello Stato membro del procuratore europeo delegato incaricato del caso in base al diritto di tale Stato membro.

3. In caso di risposta negativa alla prima questione o di risposta positiva alla seconda questione, in che misura debba avvenire il controllo giurisdizionale nello Stato membro del procuratore europeo delegato incaricato di prestare assistenza.

[27] Riservando alle autorità dello Stato del PED incaricato del caso un controllo preventivo relativo alle condizioni di giustificazione e adozione della misura e alle autorità dello Stato del PED chiamato a prestare assistenza un mero controllo relativo all'esecuzione della misura. Cfr. la nota che segue.

[28] Cfr. Corte di giustizia dell'Unione Europea, grande camera, sent. 21 dicembre 2023, C-281/22, *G.K. e altri* (*Parquet européen*), cit.,la quale ha sostanzialmente sancito che gli articoli 31 e 32 del Regolamento 2017/1939, nell'ottica di consentire una efficace ed efficiente attività investigativa transfrontaliera, devono essere interpretati nel senso che: «il controllo effettuato in seno allo Stato membro del PED incaricato di prestare assistenza, qualora una misura investigativa assegnata richieda un'autorizzazione giudiziaria conformemente al diritto di tale Stato membro, può vertere solo sugli elementi relativi all'esecuzione di tale misura, e non sugli elementi relativi alla giustificazione e all'adozione della misura stessa, i quali devono essere sottoposti ad un previo controllo giurisdizionale effettuato nello Stato membro del PED incaricato del caso in situazioni di grave ingerenza nei diritti della persona interessata garantiti dalla Carta dei diritti fondamentali dell'Unione europea». Per un primo commento, cfr. N. Gibelli, *Sui controlli giurisdizionali nelle indagini transfrontaliere dell'EPPO: una prima lettura della sentenza c-281/22 della corte di giustizia dell'Unione europea*, in *Sist. pen.,* 2024, n. 3, p. 31; A. Castaldo, *La Corte di Giustizia dell'Unione Europea si pronuncia, per la prima volta, sul regolamento istitutivo della Procura Europea, chiarendo limiti e integrazioni all'attività di indagini transfrontaliere tra Procuratori Europei delegati e Corti nazionali,* in *Giurisprudenza Penale Web*, 2024, 3.

[29] Regolamento (UE) 2023/1543 del Parlamento Europeo e del Consiglio del 12 luglio 2023, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali, in *G.U.U.E.* 28.7.2023, L 191/118. Per un primo commento cfr. T. Christakis*, From Mutual Trust to the Gordian Knot of Notifications: The EU E-Evidence Regulation and Directive (June 30, 2023)* in V. Franssen, S. Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Matters, Cambridge University Press,* 2023, liberamente accessibile in SSRN: https://ssrn.com/abstract=4306874; S. Tosza, *The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?* in *European Data Protection Law Review*, Vol 9 (2023), Issue 2, pp.163-172.

[30] Ai sensi dell'art. 34, §2, del Regolamento 2023/1543, esso troverà applicazione a decorrere dal 18 agosto 2026.

[31] Va rimarcato come il Regolamento adotti una nozione autonoma e restrittiva della locuzione "prova elettronica", in quanto essa è definita (art. 3, n. 8) come «i dati relativi agli abbonati, i dati sul traffico o i dati relativi al contenuto conservati in formato elettronico da o per conto di un prestatore di servizi al momento della ricezione, di un certificato di ordine europeo di produzione (EPOC) o di un certificato di ordine europeo di conservazione (EPOC-PR)».

[32] L'art. 4 del Regolamento si riferisce «un giudice, un organo giurisdizionale, un magistrato inquirente, un pubblico ministero oppure qualunque oppure qualsiasi altra autorità, definita dallo Stato di emissione».

[33] Da intendersi, ai sensi dell'art. 3, n. 16 Regolamento 2023/1543, come «lo Stato membro nel quale lo stabilimento designato è stabilito o il rappresentante legale risiede e a cui l'ordine europeo di produzione e un EPOC o l'ordine europeo di conservazione e un EPOC-PR sono trasmessi dall'autorità di emissione, ai fini della notifica o ai fini dell'esecuzione in conformità del presente regolamento».

[34] L'autorità di emissione e le condizioni per l'emissione dell'ordine europeo di produzione (EPOC) e di conservazione (EPOC-CR) sono disciplinate rispettivamente dagli art. 4 e 5 del Regolamento 2023/1543.

[35] Data la volatilità della *e-evidence,* il Regolamento prevede altresì che l'autorità giudiziaria possa - quando sussiste il rischio di rimozione, cancellazione o modifica dei dati - ordinare il c.d. "congelamento" (*freezing*) dei dati, emettendo un ordine europeo di conservazione (EPO-CR) in vista della presentazione di una successiva richiesta di produzione dei medesimi, tramite l'assistenza giudiziaria, un ordine europeo di indagine (OEI) o un ordine europeo di produzione (EPOC). L'autorità di emissione e le condizioni per l'emissione dell'ordine europeo di di conservazione (EPOC-CR) sono disciplinate rispettivamente dagli art. 4 e 6 del Regolamento 2023/1543.

[36] Definiti dall'art. 3, n. 9 del Regolamento 2023/1543 come «i dati detenuti da un prestatore di servizi relativi all'abbonamento ai suoi servizi, riguardanti: a) l'identità di un abbonato o di un cliente, come il nome, la data di nascita, l'indirizzo postale o geografico, i dati di fatturazione e pagamento, il numero di telefono o l'indirizzo e-mail forniti; b) il tipo di servizio e la sua durata, compresi i dati tecnici e i dati che identificano le misure tecniche correlate o le interfacce usate dall'abbonato o dal cliente o a questo fornite al momento della registrazione o dell'attivazione iniziale e i dati connessi alla convalida dell'uso del servizio, ad esclusione di password o altri mezzi di autenticazione usati al posto di una password, forniti dall'utente o creati a sua richiesta»

[37] Definiti dall'art. 3, n. 11 del Regolamento 2023/1543 come «i dati riguardanti la fornitura di un servizio offerto da un prestatore di servizi, che servono per fornire informazioni di contesto o supplementari sul servizio e che sono generati o trattati da un sistema di informazione del prestatore di servizi, come la fonte e il destinatario di un messaggio o altro tipo di interazione, sull'ubicazione del dispositivo, la data, l'ora, la durata, le dimensioni, il percorso, il formato, il protocollo usato e il tipo di compressione, e altre comunicazioni elettroniche e i dati, diversi dai dati relativi agli abbonati, relativi all'inizio e alla fine di una sessione di accesso utente a un servizio, come la data e l'ora d'uso, la connessione al servizio (log-in) e la disconnessione (log-off) dal medesimo».

[38]I dati relativi al contenuto sono definiti dall'art. 3, n. 12 Regolamento 2023/1543 come «qualsiasi dato in formato digitale, come testo, voce, video, immagini o suono, diverso dai dati relativi agli abbonati o dai dati sul traffico».

[39] Cfr. D. Brodokwki, *Admissibility of Evidence in the EPPO Proceedings,* in *New Journal of European Criminal Law,* 2023, Vol.14(1), p. 42.

[40] La proposta di direttiva (*ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings. Draft Legislative Proposal of the European Law Institute*), redatta in lingua inglese, è consultabile all'indirizzo web: *https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-publishes-a-legislative-proposal-on-mutual-admissibility-of-evidence-and-electronic-evidence-in/*.
Per un commento cfr.R. Belfiore, *Quali prospettive per l'ammissibilità reciproca delle prove fra gli Stati membri dell'Unione europea?* in *Cass. Pen.*, 2023, p. 3870*;* L. Bachmaier Winter, *Mutual Admissibility of Evidence and Electronic Evidence in the EU. A New Try for European Minimum Rules in Criminal Proceedings*? in *Eucrim* 2023/2, p. 223.

[41] Come del resto lo fu, a suo tempo, la proposta di istituire la Procura europea (EPPO), risalente al *Corpus Juris* del 1997.

[42] Di questo avviso D. Brodokwki, *Admissibility of Evidence in the EPPO Proceedings,* cit., p. 42, secondo il quale non sembrano sussistere, allo stato attuale del processo di integrazione europea, le condizioni per l'armonizzazione delle procedure penali in materia di ammissione della prova.

[43] Cfr. il Considerando n. 25 della proposta.

[44] Cfr. l'art. 8 della proposta e l'*Explanatory Memorandum*, p. 23.

[45] Cfr. l'art. 8, n. 4 della proposta e l'*Explanatory Memorandum*, p. 22.

[46] Cfr. l'art. 8, n. 6 della proposta e l'*Explanatory Memorandum*, p. 24. La proposta prevede altresì la cancellazione dei dati acquisiti all'esito del processo (cfr. l'art. 8, n. 8 e l'*Explanatory Memorandum*, p. 24).

[47] Che le specificità della *e-evidence* rendano necessario concepire una disciplina speciale è sostenuto anche nello studio dell'*European Law Institute*: cfr. il Considerando n. 23 della proposta («*the increasing relevance of electronic evidence in all kinds of criminal proceedings, and the particular features of electronic evidence, warrant the adoption of specific rules on electronic evidence and its admissibility*») e l'*Explanatory Memorandum*, p. 22.

[48] Uno dei primi ad invocare l'«*habeas data*» fu S. Rodotà, nella sua veste di Garante per la protezione dei dati personali. Cfr. La Relazione al Parlamento di S. Rodotà quale Garante dell'Autorità per la protezione dei dati del 2001 è reperibile *online*: *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3541955.*