DIGITALIZZAZIONE NELLA COOPERAZIONE GIUDIZIARIA IN MATERIA PENALE: IL RISPETTO DEI PRINCIPI DI NECESSITÀ E PROPORZIONALITÀ (ANCHE) NELLA PROVA ELETTRONICA*

Stefano Busillo**

SOMMARIO: 1. Considerazioni introduttive: la digitalizzazione della cooperazione giudiziaria penale tra fonti tradizionali e nuovi impulsi europei; 2. L'impiego delle prove elettroniche in materia penale: alcune questioni irrisolte; 3. Necessità e proporzionalità nella *Data Retention Saga*: l'estensione della disciplina alla prova elettronica?; 4. Le incompatibilità con la Proposta di ordine europeo di produzione e conservazione della prova; 5. Osservazioni conclusive.

1 Considerazioni introduttive: la digitalizzazione della cooperazione giudiziaria penale tra fonti tradizionali e nuovi impulsi europei

Il processo di digitalizzazione nell'ambito della cooperazione giudiziaria rappresenta quell'insieme di iniziative ed adeguamenti giuridico-normativi che la comunità internazionale si è impegnata a predisporre al fine di aggiornare gli strumenti di indagine e di persecuzione penale nella particolare fase storica di transizione tecnologica[1]. Così, sia a livello regionale che universale, si è intrapreso un processo normativo caratterizzato dalla messa a punto di meccanismi preventivi e repressivi – di natura squisitamente digitale – sempre più sofisticati e sempre più al passo con le nuove fattispecie criminali, caratterizzate anzitutto da una dimensione transnazionale, come risulta dalle disposizioni della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale (UNTOC) del 2000[2]. Tuttavia, la digitalizzazione ha inciso anche sul diritto penale sostanziale e processuale, costituendo la rete il luogo per la consumazione di vecchi reati (adeguamento fattispecie esistenti) e/o possibile elemento costitutivo (fatto tipico) per nuovi reati, nonché per i mezzi di persecuzione penale,

* Il presente contributo riprende, ampliandolo, l'intervento svolto in occasione della Conferenza internazionale dal titolo "*Nuove e vecchie tendenze della cooperazione di polizia e giudiziaria in materia penale*", tenutosi presso l'Università degli Studi di Salerno il 26 maggio 2022, nel quadro delle attività del Modulo Jean Monnet "*EU-Western Balkans Cooperation on Justice and Home Affairs*" (EUWEB).

** Dottorando di Ricerca in "Scienze Giuridiche" (*curriculum* internazionalistico-europeo-comparato); Cultore in Diritto dell'Unione europea, Diritto dell'Unione europea delle migrazioni, Diritto internazionale penale e Organizzazione internazionale; *Senior Member* del *Legal Observatory* del Modulo Jean Monnet "*EU-Western Balkans Cooperation on Justice and Home Affairs*" (EUWEB) 2019-2022, Dipartimento di Scienze Giuridiche (Scuola di Giurisprudenza) – Università degli Studi di Salerno. Cultore in Istituzioni di Diritto internazionale e *Diplomatic and Consular Law*, Dipartimento di Studi Politici e Sociali – Università degli Studi di Salerno. Cultore in *International Law and Cyber Security*, Dipartimento di Scienze Aziendali - Management and Innovation Systems, Università degli Studi di Salerno.

[1] Per avere una dimensione della portata della trasformazione del crimine in atto nel sostrato digitale, v. L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime. Diritto e procedura penale dell'informatica*, 2018; S. Aterno, *Digital Forensics (investigazioni informatiche)*, in *Digesto delle discipline penalistiche*, UTET, Torino, 2014; S. Amore, V. Stanca, S. Staro, *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, 2006; C. Sarzana di Sant'Ippolito, *Criminalità e tecnologia: il caso dei "computer crimes"*, in *Rass. penit. crim.*, 1979, n. 1, p. 53 ss.

[2] Risoluzione dell'Assemblea Generale 55/25, Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale (UNTOC, Convenzione di Palermo), 15 novembre 2000, il cui testo è disponibile al link www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf. Sulla digitalizzazione, in particolar modo si guardi all'Art. 20 che tratta di consente espressamente tecniche investigative che prevedano forme di sorveglianza digitale (par. 1), incoraggiando gli Stati a concludere accordi, bilaterali o multilaterali, finalizzati al l'utilizzo di tecniche investigative speciali nel contesto della cooperazione internazionale (par. 2) e chiarendo che, in assenza di tali accordi, le decisioni sull'utilizzo di tecniche investigative speciali a livello internazionale dovrebbero essere prese caso per caso (par. 3).

che comportano inevitabili difficoltà di bilanciamento tra esigenze di sicurezza e tutela dei diritti fondamentali[3] delle persone indagate o imputate. Ad esempio, la qualificazione astratta delle fattispecie di criminalità informatica, è riconducibile alla Convenzione di Budapest del 2001, adottata dal Consiglio d'Europa[4], comprensiva dei protocolli aggiuntivi di riferimento ed in particolare il recentissimo Protocollo aggiuntivo sulla cooperazione rafforzata e la divulgazione delle prove elettroniche, aperto alla firma il 12 maggio scorso[5]. La lotta a tali "nuove" forme di criminalità transnazionale ha richiesto, non a caso, l'individuazione dei primi *blueprints* delle fattispecie di reato (da individuarsi comunemente negli ordinamenti degli Stati), nonché la messa a punto di innovativi strumenti informatici volti, tra l'altro, all'acquisizione di informazioni e prove[6] che ne favorissero l'emersione e la perseguibilità.

Ne consegue che il processo di digitalizzazione della cooperazione giudiziaria non solo non è concluso ma, all'opposto, costituisce uno dei *leitmotiv* dell'attività normativa – in modo peculiare – dell'Unione europea e del Consiglio d'Europa su cui si intende concentrare la presente indagine. Nel caso della prima, il pacchetto di iniziative contenute nella Comunicazione della Commissione europea del 2 dicembre 2020 è diretto all'adozione di strumenti volti ad accelerare le riforme per digitalizzare la trattazione delle cause da parte delle istituzioni giudiziarie, lo scambio di informazioni e documenti tra le parti e gli avvocati e l'accesso costante e agevole alla giustizia per tutti. Alla digitalizzazione per una giustizia migliore si riferisce anche la Commissione europea per l'efficienza della giustizia del Consiglio d'Europa (CEPEJ) che ha pubblicato, il 9 dicembre 2021, il documento "*2022 – 2025 CEPEJ Action plan: Digitalisation for a better justice*"[7] volto a favorire l'ambiente digitalizzato, migliorando la qualità della giustizia che deve essere trasparente, collaborativa, umana. Infatti, ormai già da tempo i sistemi processuali penali degli Stati sono stati stravolti dall'impatto delle nuove tecnologie. Solo per fare alcuni esempi: si pensi alla possibilità di celebrazione dei processi da remoto senza trasferimento degli imputati, ovvero all'acquisizione delle prove con strumenti audiovisivi di conservazione e archiviazione dei dati su *software*, l'ordine di indagine europeo, aventi ad oggetto la richiesta di audizione in video conferenza di indagati, imputati, testimoni e parti lese, e via discorrendo[8].

[3] La mancanza di garanzie adeguate espone al rischio di violazione una serie di diritti fondamentali, quali, ad esempio, il diritto alla *privacy* (art. 8 CEDU, art. 8 CDFUE), il rispetto della vita familiare (art. CEDU, art. 7 CDFUE), ma anche alla libertà di comunicazione e corrispondenza (art. 10 CEDU, art. 11 CDFUE); ciò senza indicare i rischi di violazione del diritto ad un equo processo (art. 6 CEDU, art. 47 CDFUE) nel caso in cui non sia garantita l'indipendenza dell'autorità giudiziaria. Sul bilanciamento in questione v. R. Palladino, *La tutela dell'identità e dei dati personali nell'era digitale: il bilanciamento dei diritti tra "valori comuni" europei e specificità nazionali*, in *Beni e valori comuni nelle dimensioni internazionale e sovranazionale. XXV Convegno SIDI*, 2022, pp. 349-367.

[4] Consiglio d'Europa, *Convenzione sulla criminalità informatica*, STE no. 185, sottoscritta il 23 novembre 2001.

[5] Consiglio d'Europa, Secondo Protocollo aggiuntivo alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione delle prove elettroniche, STCE n° 224.

[6] Proprio l'ambito delle prove penali (*digital evidence* e *automated evidence*) è stata oggetto di maggior attenzione nella prassi quotidiana della giustizia penale, a seguito di "*perquisizioni e sequestri su documenti informatici, all'apprensione processuale di e-mail o sms, fino alle captazioni effettuate direttamente tramite virus informatici installati sui devices dell'intercettato*" come rilevato da C. Cesari, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal, Porto Alegre*, Vol. 5, N. 3, 2019, pp. 1167-1188.

[7] Documento CEPEJ(2021)12F.

[8] In accordo con la relazione annuale del Desk Italiano presso Eurojust dello scorso anno (2021), p. 35: "*l'utilizzo sistematico di nuove tecnologie, al fine di permettere una più agevole e veloce formazione della prova nei procedimenti transfrontalieri, non soltanto è pienamente conforme alla disciplina dello strumento di cooperazione penale azionato e*

Tanto premesso, nell'ambito di tale "processo" di digitalizzazione della cooperazione giudiziaria, il presente lavoro intende soffermarsi più da vicino sulle criticità emerse in materia di ricerca e conservazione della prova elettronica. La disciplina in questione si presta ad alcuni spunti di comparazione con la recentissima giurisprudenza afferente alla *data retention*, oggetto di pronunce tanto da parte della Corte di giustizia dell'Unione europea (CGUE) che della Corte europea dei diritti dell'uomo (Corte EDU): entrambe insistono sulla corretta applicazione dei principi di necessità e proporzionalità, quali *safeguards* della sfera individuale dell'individuo interessato dal procedimento penale[9]. Sebbene, infatti, la digitalizzazione della cooperazione giudiziaria in materia penale apporti benefici in termini di sicurezza attraverso una più efficace persecuzione del crimine, non è escluso che i soggetti destinatari di tali misure possano subire una violazione dei loro diritti fondamentali, quali, ad esempio, il diritto alla *privacy*, al rispetto della vita familiare, ma anche alla libertà di comunicazione e di corrispondenza, alla luce, come si cercherà di dimostrare, della formulazione delle proposte normative in esame – in particolare, della Proposta di ordine europeo di produzione e conservazione della prova elettronica e delle interpretazioni della CGUE in materia di conservazione dei dati personali.

2 L'impiego delle prove elettroniche in materia penale: alcune questioni irrisolte

Come è noto, le modalità che consentano di *far rientrare nella disponibilità* delle autorità inquirenti prove elettroniche da recuperarsi presso i *providers* (che, va ricordato, sono soggetti privati tenuti al rispetto della disciplina normativa dello Stato ove hanno sede), era già stato affrontato dalla Commissione europea nella Proposta di direttiva sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali[10] nonché, soprattutto, nella Proposta di

rispettoso dei principi e delle garanzie del giusto processo degli Stati, ma anche in linea con le esperienze giudiziarie europee tecnologicamente più avanzate, con il piano d'azione dell'Unione 2019-2023 in materia di giustizia elettronica e con la proposta di regolamento della Commissione europea dell'1.12.21 sulla digitalizzazione della cooperazione giudiziaria e l'accesso alla giustizia in materia civile, commerciale e penale transfrontaliera e recante modificazioni di alcuni atti nel settore della cooperazione giudiziaria", https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/RELAZIONE-ANNUALE-2021-DESK-ITALIANO-EUROJUST.pdf.

[9] Ciò è ribadito, a livello delle Nazioni Unite, dalla *Kyoto Declaration on Advancing Crime Prevention, Criminal Justice and the Rule of Law*, del 12 marzo 2021 in cui rileva che l'insieme dei diritti fondamentali dei soggetti indagati o perseguiti da tutelare, è inevitabilmente posto a rischio dall'azione congiunta degli Stati (cooperazione in materia penale), laddove non rispettosa delle norme procedurali e dei principi generali in materia. La *Kyoto Declaration*, pertanto, riafferma la piena responsabilità degli Stati a promuovere e tutelare "tutti" i diritti umani e libertà fondamentali, con riferimento peculiare alla *privacy* ed al giusto processo, nell'imparziale amministrazione della giustizia nonché per l'intera esecuzione e durata degli sforzi volti a prevenire e/o contrastare il crimine. In altre parole, la natura digitale della cooperazione non esenta gli Stati membri da tale impegno, ma deve – a fronte di chiari rischi – invitarli a maggiori cautele.

[10] Proposta di Direttiva del Parlamento europeo e del Consiglio *recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali*, COM/2018/226 final - 2018/0107 (COD). La Proposta deriva dalla necessità di regolare i rapporti con, in particolare, gli Stati Uniti. Infatti, tramite essa si mira a far sì che gli Stati membri obblighino i prestatori di servizi attivi nell'Unione, anche se non stabiliti nel territorio di questa, a individuare almeno un rappresentante legale ai fini della ricezione, dell'ottemperanza e dell'esecuzione di provvedimenti emessi dalle autorità competenti di ciascuno Stato membro a fini probatori. Il rappresentante legale deve risiedere o essere stabilito nel territorio di uno degli Stati membri in cui il prestatore svolge la propria attività ed è obbligato a cooperare con le autorità. A tal fine, egli gode dei poteri e delle risorse necessari e può essere ritenuto responsabile del mancato rispetto degli obblighi derivanti dalla disciplina in materia di ordini di produzione e di conservazione. Cf. A. Rosanò, *Il*

regolamento – ancora in fase di discussione – relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale[11]. Attraverso la Proposta di regolamento si mira ad introdurre una disciplina unitaria relativa a due nuovi strumenti di cooperazione giudiziaria in materia penale: l'ordine europeo di produzione e l'ordine europeo di conservazione, di cui nel dettaglio a breve. Lo scopo della proposta è sopperire ai problemi cagionati dal fatto che "*l'ottenimento di prove elettroniche presenta problematiche specifiche che non riguardano gli altri atti d'indagine contemplati dalla direttiva OEI*", per cui "*anziché modificare la direttiva OEI si è deciso di creare un nuovo strumento per tali prove*"[12]. Tali ordini verrebbero emessi sotto forma di "certificati"[13] disposti in presenza di procedimenti penali già avviati nei confronti di persone fisiche o giuridiche[14], sia in fase istruttoria che processuale, al fine di (ordine di produzione) acquisire – direttamente, senza l'intermediazione e controllo *ex ante* delle autorità giudiziarie locali – prove elettroniche dai fornitori di servizi di comunicazione elettronica; oppure al fine di imporre ai medesimi (ordine di conservazione) la conservazione di nomi, domini Internet, nonché di numeri IP attivi nell'Unione europea.

Non è difficile constatare che l'ordine europeo di produzione e l'ordine europeo di conservazione implicherebbero una straordinaria semplificazione delle procedure, con una riduzione tangibile dei termini per la consegna delle prove e un'evidente facilitazione nella lotta alla criminalità. Ciononostante, ci sembra che tale neo-acquisita speditezza dovrebbe rispondere, a maggior ragione, ai principi di proporzionalità e necessità[15] (cui andrebbe aggiunta l'indipendenza degli organi deputati al controllo di questi meccanismi), come interpretati dalla CGUE. Questa ha, infatti, già avuto modo di chiarire[16] che proprio le limitazioni dei diritti al rispetto della vita privata e alla protezione dei dati

nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea: le proposte della Commissione Europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence), in *Leg. Pen*., 16 ottobre 2020; G. Robinson, *The European Commission's e-Evidence Proposal*, in *European Data Protection Law Review*, n. 3, 2018, pp. 347-352.

[11] Proposta di Regolamento del Parlamento Europeo e del Consiglio *relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, COM/2018/225 final - 2018/0108 (COD). https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0108(COD)&l=en

[12] Relazione introduttiva alla proposta, sezione 1, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018PC0225. L'OEI è stato istituito dalla Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'Ordine europeo di indagine penale, creando un quadro unico e completo per l'acquisizione delle prove (ad eccezione delle SIC). Pertanto, esso consiste in una decisione giudiziaria emessa o convalidata dall'autorità giudiziaria di un Paese dell'UE al fine di disporre di misure investigative per raccogliere o utilizzare prove in materia penale svolte in un altro Paese dell'UE. Gli atti investigativi comprendono, ad esempio, l'audizione di testimoni, le intercettazioni telefoniche, le indagini segrete e le informazioni sulle operazioni bancarie. Sebbene l'OEI sia ammissibile per le prove elettroniche, l'introduzione del nuovo strumento dell'Ordine di produzione consentirà a un'autorità giudiziaria di uno Stato membro di ottenere prove elettroniche (come e-mail, SMS o messaggi nelle app, nonché informazioni per identificare un autore come primo passo) direttamente da un fornitore di servizi o dal suo rappresentante legale in un altro membro Stato, che sarà obbligato a rispondere entro 10 giorni, ed entro 6 ore in caso di emergenza e non più rispetto ai 120 giorni previsti per l'OEI.

[13] Art. 8 Proposta.

[14] Art. 3 Proposta

[15] È infatti richiesto di operare una valutazione di proporzionalità al fine di misurare l'impatto negativo sui diritti e le libertà dei cittadini, dimostrando che gli effetti negativi prodotti nei loro confronti siano giustificati da un corrispondente o superiore impatto positivo sul benessere generale. La valutazione della necessità deve essere condotta per dimostrare chiaramente che il ricorso a una particolare tecnologia o sistema di analisi dei dati è necessario per raggiungere obiettivi specifici altrimenti non raggiungibili con strumenti o tecniche meno invasive della sfera giuridica altrui.

[16] See CGUE (Grande Sezione), sentenza del 8 aprile 2014, cause riunite C-293/12 e C-594/12 *Digital Rights Ireland*; CGUE (Grande Sezione), sentenza del 21 dicembre 2016, cause riunite C-203/15 e C-698/15 *Tele2Sverige and Tom Watson*, parr. 96 e 155; dal proprio canto, per la giurisprudenza di Strasburgo, v. Corte EDU (Grande Sezione), sentenza

personali devono essere strettamente *necessarie*, ovvero disposte poiché nessun'altra misura meno invasiva potrebbe raggiungere lo scopo previsto, e *proporzionate*, per cui la restrizione di talune situazioni giuridiche soggettive positive dovrà essere giustificata dalla tutela di altri diritti (es. sicurezza) di pari o superiore entità. Abbracciando una linea apparentemente[17] sempre più garantista, i giudici di Lussemburgo hanno sottolineato che le iniziative dell'UE e degli Stati membri, perfino quando rispondono all'obiettivo di combattere il terrorismo e la criminalità organizzata, comportando il *trasferimento* di dati oltre frontiera (in particolare verso Paesi terzi), devono aderire a forme di limitazione e controllo così da giustificare l'azione dei *law enforcers*[18]. Appare poi evidente alla Corte che il dovere di verificare il rispetto dei diritti fondamentali e del principio dello Stato di diritto dipende, in primo luogo, dalle autorità preposte all'emissione o alla convalida di una decisione di applicazione della giurisdizione penale transfrontaliera, e che gli atti che provvedono, in sostanza, alla compressione dei diritti dell'individuo devono essere precisi e chiari sia nel contenuto che nella motivazione e soggetti a controllo giurisdizionale o amministrativo indipendente[19].

Alle considerazioni appena svolte, si aggiungono le preoccupazioni legate all'implementazione dei nuovi strumenti di cooperazione penale digitale relativi alle modalità di ricerca e conservazione della prova elettronica. Del resto, sempre più spesso si procede all'acquisizione di tracce elettroniche e all'analisi di dati informatici nel contesto di indagini non solo per i c.d. *cybercrimes*, ma anche per i reati comuni. Vero è che il dato elettronico è suscettibile di integrareun mezzo di prova, ma questo, per le sue caratteristiche intrinseche di volatilità e modificabilità, richiede particolari cautele all'atto della ricerca, raccolta, conservazione, presentazione e analisi processuale. Detta prova elettronica ha, infatti, natura molto spesso transnazionale[20], in quanto è svincolata dalla giurisdizione territoriale ove il reato è stato posto in essere o si svolge l'attività di indagine. Pertanto, tre aspetti definiscono in modo esaustivamente caratterizzante la natura della prova elettronica: (i) la sua peculiare localizzazione e conservazione; (ii) le fonti private (ISP - *Internet Service Provider*) da cui di frequente origina; (iii) il connotato transnazionale del reato nel cui contesto sovente rileva. L'attuale realtà tecnologica non poteva, quindi, che mettere in crisi i tradizionali concetti di giurisdizione,

del 4 dicembre 2015, ricorso n. 47143/06, *Roman Zakharov c. Russia*, par. 227 ss.; Corte EDU (Grande Sezione), sentenza del 4 maggio 2000, ricorso n. 28341/95, *Rotaru c. Romania*, par. 47 ss.

[17] L'apparenza e la non sostanzialità deriva dal fatto che, guardando alle pronunce richiamate nella successiva sezione, la centralità della sicurezza degli Stati Membri non è smarrita, quanto – al massimo – temperata dall'imposizione di controlli più stringenti verso gli organi di *law enforcement*.

[18] Progresso significativo è stato ottenuto indubbiamente nella c.d. "*Schrems saga*" che consta di CGUE (Grande Sezione), sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*; and CGUE (Grande Sezione), sentenza del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems*. Per maggiori informazioni sulla *Schrems saga*, per tutti, si guardi ai contributi di M. Nino, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, Vol. 3, n. 14, 2020, pp. 733-760; ID., *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE*, in *Il Diritto dell'Unione europea*, n. 4, 2016, pp. 755-788.

[19] In tal senso, una delle ultime decisioni è CGUE (Grande Sezione), sentenza del 2 marzo 2021, causa C-746/18, *H.K. c. Prokuratuur*. Inoltre, agli individui deve essere garantita la possibilità di far esercizio di rimedi giudiziali in caso di illegittime restrizioni alla propria sfera giuridica, sia in UE che nei paesi terzi, v. CGUE (Grande Sezione), parere del 26 luglio 2017, n. 1/15, *EU-Canada PNR Agreement*. V. anche G. González Fuster, *A Security Union in Full Respect of Fundamental Rights: But How Effectively Respectful*?, in S. Carrera, V. Mistilegas (eds.), *Constitutionalising the Security Union: Effectiveness, Rule of Law and Rights on Countering Terrorism and Crime*, *Centre for European Policy Studies (CEPS*), 2017.

[20] Per maggiori informazioni su tale aspetto, v. il contributo di R. *Geraci*, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento e-evidence*, in *Cassazione Penale*, Fasc. 3, 2019, pp. 1340-1362.

ovvero fondati su territorio e sovranità, insieme a quelle limitazioni tecnico-giuridiche del singolo ordinamento nazionale che da essa discendono. Nello specifico, l'osservazione delle dinamiche proprie al cyberspazio evidenzia chiaramente che l'applicazione delle nozioni classiche limita l'azione degli investigatori – con la conseguente impossibilità di produrre effetti positivi per i consociati, in questo caso legati al contrasto alla criminalità – e che i criteri definitori tradizionali non sempre sono idonei a individuare lo Stato competente alla gestione delle informazioni, in quanto non tengono in adeguato conto le specificità dei dati elettronici e segnatamente la loro mobilità, la loro contemporanea conservazione in più *server* ubicati in nazioni diverse e l'assenza di luoghi di custodia fisicamente delimitati. Da ciò, senza dubbio alcuno, deriva l'esigenza di una disciplina o gestione "unitaria" di stampo europeo. Vieppiù, l'ampio coinvolgimento dei privati, i c.d. *providers*, nei procedimenti penali rappresenta elemento di forte incertezza, siccome trattasi di soggetti dotati di limitata conoscenza delle tutele disposte dall'ordinamento, europeo o nazionale che sia, e che pertanto agevolano involontariamente le ipotesi di abuso nei confronti degli individui indagati, come a breve sarà esplicato.

Tali esigenze sembrano emergere anche dalle novità legislative riconducibili all'aggiornamento digitale della cooperazione giudiziaria UE che promanano dalla già richiamata Comunicazione del 2 dicembre 2020 da parte della Commissione europea (*Digital Justice*). Segnatamente, l'8 dicembre 2021 la presidenza del Consiglio ed il Parlamento europeo hanno raggiunto un accordo provvisorio sulla Proposta di regolamento relativo al sistema e-CODEX[21]. La Commissione, in somma sintesi, è dell'avviso che e-CODEX possa diventare la soluzione digitale primaria per una trasmissione sicura di *tutti* i dati elettronici nei procedimenti civili e penali transfrontalieri nell'Unione, andando ad agevolare la trasmissione di elementi probatori *già nella disponibilità delle autorità*. In modo particolare, rileva per questo contributo che e-CODEX è *parzialmente* già alla base del sistema digitale dell'Unione, essendo impiegato nello scambio di prove elettroniche e negli scambi concernenti gli ordini europei di indagine e, genericamente, l'assistenza giudiziaria reciproca nel settore della cooperazione giudiziaria in materia penale.

3 Necessità e proporzionalità nella *Data Retention Saga*: l'estensione della disciplina alla prova elettronica?

Ci sembra, quindi, che le questioni relative alla conservazione di prove elettroniche, siano collegabili con la dibattuta questione della *bulk data retention*, rispetto alla quale la CGUE aveva già dichiarato l'invalidità della Direttiva 2006/24/CE[22] per violazione dei diritti di cui agli artt. 7 e 8 della Carta dei

[21] Proposta di regolamento del Parlamento europeo e del Consiglio *relativo a un sistema informatizzato di comunicazione per i procedimenti civili e penali transfrontalieri (sistema e-CODEX) e che modifica il regolamento (UE) 2018/1726*, del 2 dicembre 2020, 2020/0345 (COD). Il sistema e-CODEX consiste in un pacchetto di componenti *software* che permette la connettività tra sistemi nazionali. Permette ai suoi utenti (autorità giudiziarie competenti, operatori della giustizia e cittadini) di inviare e ricevere, per via elettronica, documenti, formulari giuridici, prove e altre informazioni in maniera rapida e sicura. Una *governance* stabile del sistema e-CODEX consentirebbe di farne il sistema predefinito per lo scambio di messaggi elettronici nell'ambito della cooperazione giudiziaria a livello dell'UE, per mezzo della creazione di reti di comunicazione decentrate, interoperabili e sicure tra i sistemi informatici nazionali a sostegno della cooperazione transfrontaliera in materia civile e penale.

[22] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, *riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*.

diritti fondamentali dell'Unione europea. Trattasi, infatti, della pratica consistente nell'obbligo generale imposto ai fornitori di servizi di telecomunicazione di conservare i metadati[23] prodotti dai propri utenti; ciò al fine di consentire un successivo ed eventuale accesso a tali informazioni da parte di autorità di *law enforcement* o di *intelligence* nell'ambito di azioni di prevenzione, indagine e lotta alle minacce alla sicurezza pubblica nazionale[24]. Il parallelismo viene in considerazione a fronte della possibilità che i principi di necessità e proporzionalità, così come "perimetrati" dalla giurisprudenza europea per la *bulk data retention*, possano essere estesi anche ai futuri ordine di conservazione della prova elettronica. Da tale estensione, infatti, potrebbero scaturire delle incongruenze nell'attuale modello degli istituti proposti dalla Commissione.

Circa l'applicabilità e l'entità dei principi citati, con le sentenze del 6 ottobre 2020, *Privacy International*[25] e *La Quadrature*[26], la CGUE ha ribadito che la regolamentazione della *bulk data retention* rientra nell'ambito di applicazione del diritto dell'UE anche laddove essa sia volta alla garanzia della sicurezza nazionale, in quanto l'obbligo di conservazione e la possibilità di accesso implicano comunque un *trattamento dei dati* da parte di soggetti privati e non unicamente attività svolte da autorità dello Stato[27]. Viene, in altre parole, descritta la chiara e ormai incontrovertibile incompatibilità con il diritto dell'UE di una forma di conservazione generalizzata e indiscriminata - o meglio, sproporzionata e non necessaria - dei dati di traffico e di ubicazione. La CGUE tuttavia ha individuato, in maniera innovativa, una possibilità eccezionale ed unica di ricorso alla *bulk data retention*: qualora sia *necessario* garantire la sicurezza nazionale (ad esempio in caso di pericolo di terrorismo), che rappresenta un obiettivo superiore rispetto alla lotta alla criminalità organizzata, come tra l'altro stigmatizzato nella recentissima sentenza *SpaceNet e Telekom Deutchland* del 20 settembre 2022[28] e già ammesso, purché la *retention* sia predisposta per un periodo limitato (vincolato

[23] Ovvero i dati di traffico (ora, durata, destinatario, frequenza delle chiamate) o di ubicazione (localizzazione dell'apparecchio utilizzato), indirizzi IP o dati relativi all'utente – sono in grado di svelare relazioni, abitudini e luoghi frequentati, consentendo quindi di trarre conclusioni precise sulla vita degli utenti. Una descrizione e commento dell'istituto è quella offerta, *ex multis*, da F. La Chioma, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, in *Magistratura Indipendente*, 6 giugno 2019; L. Moxley, *EU Releasaes e-Evidence Proposal for Cross-Border Data Access, in www.insideprivacy.com*, 2019; O. Pollicino, M. Bassini, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, in *www.medialaws.eu*, 26 ottobre 2018, pp. 1-8;F. Ruggeri, *Novità. Il protocollo 16 alla Cedu in vigore dal 1° agosto 2018. La proposta per l'ordine europeo di conservazione o di produzione della prova digitale*, in Cass. Pen., 2018, nn. 7-8, pp. 2660- 2663; Della Torre, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in Dir. Pen. Cont., n. 5, 2018, pp. 277-294; V. Frassen, *The European Commission's e-Evidence Proposal: toward an EU-wide obligation for service providers to cooperate with law enforcement?*, in *www.europeanlawblog.eu*, 12 ottobre 2018.

[24] Pur non riguardando il contenuto della comunicazione, i metadati – ovvero i dati di traffico (ora, durata, destinatario, frequenza delle chiamate) o di ubicazione (localizzazione dell'apparecchio utilizzato), indirizzi IP o dati relativi all'utente – sono in grado di svelare relazioni, abitudini e luoghi frequentati, consentendo quindi di trarre conclusioni precise sulla vita degli utenti.

[25] CGUE (Grande Sezione), sentenza del 6 ottobre 2020, causa C-623/17, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service.*

[26] CGUE (Grande Sezione), sentenza del 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatife, Igwan.net c. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées*.

[27] Coerentemente con CGUE (Grande Sezione), sentenza del 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB c. Postoch telestyrelsen e Secretary of State for the Home Department c. Tom Watson e a.*; e a CGUE (Grande Sezione), sentenza del 2 ottobre 2018, causa C-207/16 *Secretary of State for the Home Department c. Tom Watson e a., Ministerio Fiscal*.

[28] CGUE (Grande Sezione), sentenza del 20 settembre 2022, cause riunite C-793/19 e C-794/19, *Bundesrepublik Deutschland c. SpaceNet AG* (C-793/19) *e Telekom Deutschland GmbH* (C-794/19), punti 72-74, 92-106 e (per tutti) 131.

ad un termine) ma rinnovabile[29] dalla sentenza *Commissioner of An Garda Síochán*[30]. In tali casi è da ritenersi giustificata la maggiore ingerenza nei diritti fondamentali rappresentata dalla conservazione generalizzata, purché ricorrano determinate condizioni che permettano di soddisfare il principio di *proporzionalità* – come del resto affinato nella sentenza *H.K. c. Prokuratuur*[31], la quale ha fornito chiarimenti sui requisiti (condizioni) di gravità del reato e di controllo *preventivo* di una autorità giudiziaria o amministrativa indipendente. In ciò, i giudici di Lussemburgo si distinguono da quelli di Strasburgo, che hanno favorito un'interpretazione meno estesa del requisito del controllo all'interno della sentenza *Szabo*. La Corte EDU, in sostanza, riconosce sufficiente un controllo *successivo*, se giustificato da condizioni di eccezionale urgenza e caratterizzato da un'analisi *ex post* che controbilanci l'assenza di controlli *ex ante*[32].

Altra questione è chi può avere accesso ai dati, considerato che, sempre nella sentenza *H.K c. Prokuratuur*, la CGUE ha avuto modo di precisare *la natura "indipendente" dell'autorità deputata a svolgere il controllo di legittimità preventivo all'accesso*, giungendo tra l'altro alle medesime conclusioni nella sentenza *VD e SR* dello scorso settembre[33] (sentenza gemella e coerente con i contenuti della già citata *SpaceNet e Telekom Deutchland*). In maniera non dissimile si è espressa la Corte EDU in una pluralità di pronunce[34]. Ciò escluderebbe, innanzitutto, i privati ed altri soggetti "parziali", dal poter di effettuare questo genere di controllo, mentre ammetterebbe l'impiego di autorità non giudiziali che siano "*compatible with the Convention*"[35].

A consuntivo di quanto finora chiarito, il test sulla legittimità del provvedimento/intimazione proveniente dallo Stato/autorità richiedente è assai rilevante poiché potrebbe assurgere a vera e propria regola[36] della cooperazione giudiziaria digitale in materia penale, finalizzata a garantire il

[29] In maniera non dissimile dalla disciplina delle intercettazioni in Italia, che prevede una violazione giustificata della privacy a patto che essa sia limitata ad un termine preciso, il quale tuttavia – per esigenze d'indagine – può essere posticipato se l'autorità giudiziaria competente lo consente.

[30] CGUE (Grande Sezione), sentenza del 5 aprile 2022, causa C-140/20, *Commissioner of An Garda Síochána e a.*, punto 58.

[31] CGUE (Grande Sezione), sentenza del 2 marzo 2021, causa C-746/18, *H.K. c. Prokuratuur.*

[32] Corte EDU (Quarta Sezione), sentenza del 12 gennaio 2016, ricorso n. 37138/14, *Szabó and Vissy v. Hungary*. punto 77: "*The ex-ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation*".

[33] CGUE (Grande Sezione), sentenza del 20 settembre 2022, cause riunite C-339/20 e C-397/20, VD e SR, punti 96-107.

[34] Corte Edu, *Szabo*, cit. punto 77; Corte EDU (Terza Sezione), sentenza del 26 aprile 2017, ricorso n. 71525/01, *Dumitru Popescu c. Romania*, punti 70-73; Corte EDU (Plenaria), sentenza del 6 settembre 1978, ricorso n. 5029/71, *Klass and Others c. Germania*, punti 42 e 55; Corte EDU (Terza Sezione), decisione del 29 giugno 2009, ricorso n. 54934/00, *Weber and Saravia c. Germania*, punto 115; Corte EDU (Quarta Sezione), sentenza del 18 maggio 2010, ricorso n. 26839/05, *Kennedy c. Regno Unito*, punto 31

[35] Corte Edu, *Szabo*, cit. punto 77.

[36] Tale sospetto per l'applicazione di un assioma generale è avvalorato dal contenuto della storica sentenza CGUE (Grande Sezione) sentenza del 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a* con la quale Corte di giustizia aveva dichiarato invalida la direttiva sulla conservazione dei dati perché l'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, determinata dall'obbligo generale di conservazione dei dati relativi al traffico e all'ubicazione, non era limitata allo stretto necessario. Per tale motivo, "*dal punto di vista del test di necessità in senso stretto, i criteri di accesso ai dati da parte delle autorità pubbliche (persone autorizzate, uso strettamente necessario, ecc.) devono essere oggetto di scrutinio e analisi approfondita*". Coerentemente a ciò, nella sentenza *Ministerio Fiscal* la Corte di giustizia ha affermato che la limitazione dei diritti quali la privacy e della riservatezza delle comunicazioni elettroniche non sono necessariamente giustificate, quale necessità, alla presenza di attività di crimine organizzato da prevenire o impedire ma anche in ipotesi minori se le interferenze non sono considerabili gravi.

rispetto dei diritti umani *a prescindere dall'istituto o meccanismo d'applicazione*[37]. In definitiva, ci sembra possibile che i principi di proporzionalità e necessità, così come interpretati per la *bulk data retention*, possano essere traslati anche nelle "nuove" procedure relative all'acquisizione e conservazione delle prove elettroniche. È chiaro che, in tale caso, gli ordini di conservazione non sono diretti ad una generalità di soggetti bensì a individui direttamente identificati dal certificato prodotto nei confronti dei *providers*, ma non per questo possono essere meno lesivi dei diritti fondamentali delle persone coinvolte[38].

4 Uno sguardo (critico) alla Proposta di ordine europeo di produzione e conservazione della prova

Alla luce delle considerazioni finora svolte, ci sembra che quindi, che la Proposta della Commissione risalente al 2018 relativa all'ordine europeo di produzione e conservazione della prova, andrebbe ricalibrata alla luce della giurisprudenza più recente degli anni 2020-21 in modo da garantire la corretta applicazione dei principi di necessità e proporzionalità, che pure sono ampiamente richiamati dall'atto[39]. In maniera particolarmente spinosa, emergono problematiche relative alla *garanzia* che l'ordine sia emesso in via necessaria e proporzionale, nonché alle modalità di controllo esercitate sulla legittimità dell'atto.

Come si è anticipato, in accordo con la Proposta, gli ordini in questione sono trasmessi, ovvero adeguatamente trasformati, in forma di certificati nei confronti dei *providers* che sono tenuti alla loro esecuzione. Pertanto, dal meccanismo originano due atti differenti. I certificati non corrispondono

[37] Sovvengono la statuizione della Comunicazione in parola che afferma "*Qualsiasi azione relativa alla digitalizzazione della giustizia deve essere attuata nel pieno rispetto dei diritti fondamentali, quali il diritto alla protezione dei dati personali e il diritto a un ricorso effettivo e a un giudice imparziale, e dei principi di proporzionalità e sussidiarietà*." Ed il contenuto della Risoluzione del Parlamento europeo *sulla lotta alla criminalità informatica*, del 3 ottobre 2017, 2017/2068(INI), par. 50 "*sottolinea la necessità di consentire alle autorità di contrasto di accedere legalmente alle informazioni pertinenti in circostanze limitate laddove tale accesso sia necessario e proporzionato per ragioni di sicurezza e giustizia; sottolinea la necessità che le autorità giudiziarie e di contrasto siano dotate di sufficienti capacità e finanziamenti per condurre indagini legittime*".

[38] Il riferimento è ai vincoli di necessità esistenti al momento della nascita dell'Ordine d'indagine europeo, nel 2014, antecedenti alla giurisprudenza sulla *bulk data retention* e sulla trasmissione di dati formatasi più diffusamente proprio a partire dal 2014; Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, *relativa all'ordine europeo di indagine penale*, del 3 aprile 2014, in GUUE L 130 del 1° maggio 2014, considerando 11 e 42 nonché art. 6, par. 1, lett. a): "*l'emissione dell'OEI è necessaria e proporzionata ai fini del procedimento di cui all'articolo 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata*".

[39] Si pensi alla sintesi nel documento di presentazione della proposta ove si afferma ove i principi pervadono le motivazioni della proposta in maniera evidente; al considerando 2 Proposta: "*Le misure per ottenere e conservare prove elettroniche sono sempre più importanti per consentire lo svolgimento delle indagini e dei procedimenti penali all'interno dell'Unione. Per combattere la criminalità sono essenziali meccanismi efficaci per l'ottenimento di prove elettroniche, che garantiscano nel contempo il pieno rispetto dei diritti fondamentali e dei principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea e sanciti nei trattati, in particolare i principi di necessità e proporzionalità e i diritti al giusto processo, alla protezione dei dati, alla segretezza della corrispondenza e al rispetto della vita privata*"; all'art. 5, par. 2 Proposta, sull'ordine di produzione. "*L'ordine europeo di produzione è necessario e proporzionato ai fini del procedimento di cui all'articolo 3, paragrafo 2, e può essere emesso solo se una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione*"; all'art. 6, par. 2 Proposta, sull'ordine di conservazione: "*L'ordine europeo di conservazione può essere emesso se è necessario e proporzionato per impedire la rimozione, la cancellazione o la modifica di dati in vista di una successiva richiesta di produzione dei medesimi tramite l'assistenza giudiziaria, un ordine europeo d'indagine o un ordine europeo di produzione. L'ordine europeo di conservazione per la conservazione di dati può essere emesso per qualsiasi reato*".

agli ordini in sé, configurandosi i primi come atti ontologicamente diversi da un punto di vista oggettivo, visto il contenuto più limitato e sintetico che sarà reso noto al *provider*; nonché soggettivo, in quanto saranno destinatari degli stessi i privati, e non già un'autorità giudiziaria. Al contrario, l'ordine di conservazione o produzione della prova elettronica ha un contenuto più specifico circa le motivazioni di emissione, circostanziando la richiesta sulla base della proporzionalità e necessità della stessa; inoltre, la conoscenza del contenuto dell'ordine sarà nota unicamente alle autorità giudiziarie degli Stati Membri coinvolti, se del caso. Ed infatti, laddove un certificato dovesse presentarsi come potenzialmente iniquo, in quanto sulla base delle "*sole informazioni ivi contenute risulta che esso viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o che è manifestamente arbitrario*"[40], il destinatario (privato) provvederà ad inviare richiesta di "controllo", in forma di modulo all'autorità giudiziaria di esecuzione competente dello Stato membro di appartenenza.

Naturalmente – ed è qui che emerge una prima criticità – presupposto per forza di cose fondamentale, è che il privato da sé possa individuare ("*ritenga*") quegli aspetti patologici dell'atto trasmessogli, conseguendone che il controllo dell'autorità giudiziale da questi "attivata" non sia la regola, bensì l'eccezione rimessa alle capacità tecnico-giuridiche del *provider*. Quest'ultimo, tuttavia, è un soggetto non sufficientemente indipendente, né avvezzo al diritto e alle tutele da esso preposte e che ivi rappresenta la tendenza alla cd. privatizzazione della tutela dei diritti fondamentali che si è largamente osservata a partire dalla introduzione del GDPR[41]. Se nella sentenza *Prokuratuur* viene richiesta l'indipendenza dell'autorità giudicante sulla legittimità dell'imposizione del precetto al privato, nella Proposta corrente risulta che il privato sia chiamato a giudicare da sé – costituendo *de plano* una violazione del requisito dell'indipendenza – e che un controllo dell'autorità giudiziaria indipendente è in pratica, solo eventuale, con il rischio che non sia azionato quando opportuno. Pertanto, tale meccanismo porterebbe ad una duplice (ingiustificata) limitazione nei confronti non solo dei diritti dell'indagato, per effetto diretto dell'ordine di produzione e/o conservazione, ma anche verso i mezzi di prevenzione degli abusi a disposizione, a causa della mera "possibilità" di verificare

[40] Art. 9, par. 5 Proposta.

[41] A riguardo sono espressi A. Rosanò, *La "privatizzazione" nello spazio di libertà, sicurezza e giustizia: tre esempi per una tendenza*, in *Il Diritto dell'Unione europea*, Fasc. 1, 2020, pp. 179-220; V. Mitsilegas, *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-Evidence*, in *Maastricht Journal of European and Comparative Criminal Law*, N. 25, 2018, pp. 263-265. Un ulteriore esempio di privatizzazione della tutela dei diritti promanata dal GDPR è la sentenza *Google Spain SL* ove è stato precisato come anche i motori di ricerca, a dispetto della direttiva e-commerce che prevede una serie di esenzioni per i fornitori di servizi online, siano da considerare "titolari del trattamento dati" e pertanto siano tenuti al rispetto della normativa sulla *data protection* ed al controllo dei dati indicizzati: CGUE (Grande Sezione), sentenza del 13 maggio 2014, causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, punto 38: "*Pertanto, nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti web, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46, affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti e possa essere effettivamente realizzata una tutela efficace e completa delle persone interessate, in particolare del loro diritto al rispetto della loro vita privata*". Ne hanno discusso, tra gli altri, A. Correra, *La tutela dei dati personali e la portata territoriale dell'obbligo di deindicizzazione dei contenuti online*, in *eurojus*, Fasc. 3, 2020, pp. 35-50; R. Palladino, *Sul diritto all'oblio e la tutela dei diritti fondamentali in internet: ambito di applicazione territoriale e bilanciamento a margine della sentenza Google LLC della Corte di giustizia dell'UE*, in *I Diritti dell'Uomo*. Vol. 3, 2019, pp. 543-562; G. De Gregorio, *The e-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?*, in *Robert Schuman Centre for Advanced Studies Research Paper*, n. RSCAS 2019/36.

che i principi di necessità e la proporzionalità non siano state violati[42]. A ciò si aggiunge un altro fattore determinante: mentre gli ordini stessi, quale atto dal contenuto minimo predefinito dal Regolamento *de jure condendo*, devono includere le motivazioni di necessità e proporzionalità in virtù dello scopo perseguito dal procedimento penale in atto; *a contrario*, per non mettere a repentaglio il corretto svolgimento delle indagini, l'inclusione di tali informazioni non è prevista nei certificati comunicati ai privati, ovvero i *providers*[43]. Di conseguenza, elidendo un'informativa essenziale come quella sulle esigenze di necessità e proporzionalità[44], il privato avrà ancora meno informazioni a disposizione per esprimere dubbi circa l'esecuzione dell'ordine, rendendo lo *stage* di controllo da parte dell'autorità indipendente circa suddetti principi non solo eventuale, come più volte ribadito, ma addirittura improbabile. Pertanto, i principi più volte richiamati, sembrano essere messi a rischio in quanto anche se previsti dalla Proposta, sarebbero di difficile applicazione – rendendo manifesta un'incompatibilità *ab origine* tra l'atto avanzato dalla Commissione e i principi garantisti imposti e sviluppati dalla giurisprudenza delle Corti europee.

Infine, la proposta può comportare "*practices that will have an unlawful impact*"[45] poiché tali atti distinguono in maniera inappropriata tra diversi tipi di informazioni personali, ammettendo una *concessione incondizionata* dell'ordine europeo di produzione e di quello di conservazione per livelli inferiori di *privacy*[46], sulla base del presupposto, non verificato e dato per assunto, che talune categorie di informazioni siano meno sensibili (c.d. garanzie a geometria variabile), piegando i principi di proporzionalità e di necessità oltremodo ed escludendo forme di controllo per la corretta applicazione dei medesimi.

5 Osservazioni conclusive

[42] Anche se, va riconosciuto, la proposta dispone all'art. 17 che, in ogni caso, gli imputati ed indagati possono ricorrere contro un ordine di produzione o conservazione durante il procedimento penale per il quale l'ordine è stato emesso "*dinanzi a un organo giurisdizionale dello Stato di emissione in conformità al diritto nazionale di tale Stato e include la possibilità di contestare la legittimità della misura, comprese la sua necessità e la sua proporzionalità*". Al contempo, tale diritto di ricorrere implica che una (potenziale) violazione dei diritti fondamentali dell'individuo si sia già concretizzata, sottraendosi ad una logica di controllo preventivo utile ad impedire qualsiasi effetto dannoso ingiustificato.

[43] Art. 8, parr. 3 e 4 della Proposta: "*3. L'EPOC contiene le informazioni di cui all'articolo 5, paragrafo 5, lettere da a) a h), comprese informazioni sufficienti a permettere al destinatario di identificare e contattare l'autorità di emissione. I motivi della necessità e della proporzionalità della misura o ulteriori dettagli sulle indagini non sono inclusi. 4. L'EPOC-PR contiene le informazioni di cui all'articolo 6, paragrafo 3, lettere da a) a f), comprese informazioni sufficienti a permettere al destinatario di identificare e contattare l'autorità di emissione. I motivi della necessità e della proporzionalità della misura o ulteriori dettagli sulle indagini non sono inclusi.*".

[44] Come sostenuto da A. Tinoco-Pastrana, *The Proposal on Electronic Evidence in the European Union*, in *Eucrim*, n. 1, 2020, pp. 48-49; cf. B.J. Blažič, T. Klobučar, *Removing the Barriers in Cross-Border Crime Investigation by Gathering e-Evidence in an Interconnected Society*, in *Information & Communication Technology Law*, Vol. 29, n. 1, 2020, pp. 66-81.

[45] M. Stefan, G. González Fuster, *Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and Latest Developments in the EU and the US*, in *CEPS Papers*, n. 7, 2018, p. 50.

[46] Art. 5, parr. 3 e 4 Proposta distinguono tra "*dati relativi agli abbonati o dati relativi agli accessi*" per i quali l'ordine "*può essere emesso per qualsiasi reato*" ed "*i dati relativi alle operazioni o dati relativi al contenuto*" nel cui caso invece subentrano delle condizioni di emissione che insistono sulla gravità dei reati oggetto delle indagini (applicazione di necessità e proporzionalità). La Proposta chiarisce in via precettiva che gli ordini relativi alla sottoscrizione e all'accesso ai dati sono emessi sia dall'Autorità Giudiziaria che dalle Procure per tutti i reati. Gli ordini relativi ai dati di natura transazionale e di contenuto sono emessi solo dall'Autorità Giudiziaria e sostanzialmente per reati con pena detentiva massima pari o superiore a 3 anni (o, ulteriormente, per i reati catalogati). Per maggiori informazioni, v. S. Carrera, M. Stefan, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, in *CEPS Papers*, n. 1, 2020, pp. 1-73.

La breve indagine sinora presentata ha fatto emergere come la cooperazione penale in ambito digitale sia caratterizzata da dalle necessità di garantire sicurezza, speditezza ed efficacia, non sempre facilmente conciliabili In tale quadro, la circolazione della prova elettronica ha incentivato il legislatore comunitario ad un adeguamento degli strumenti preposti alla sua ricerca e trasmissione. Tuttavia, l'analisi della Proposta ha evidenziato dubbi in ordine alle garanzie e tutele offerte ai soggetti coinvolti nel meccanismo. Verificata infatti l'inadeguatezza, per ragioni di lentezza ed inefficacia, dell'OEI (2014), i nuovi strumenti quali l'ordine di conservazione e produzione della prova elettronica (2018), elaborati nell'alveo di una più estesa strategia digitale (2020), ci sembrano presentare rischi di violazioni similari a quelli prodottosi in tema di *data retention*.

In questa direzione, proprio la giurisprudenza delle due Corti europee, saldamente ancorata al rispetto dei due principi fondamentali di necessità e proporzionalità, potrebbe coprire, non solo le ipotesi di conservazione di dati di tipo "generalizzato", ma anche il caso di atti che impongono la produzione e la conservazione in via "specifica", quando lasciano un'eccessiva responsabilità (o "discrezionalità") nelle mani dei privati, incapaci di offrire sicurezze sulla qualità del controllo *prima facie* cui sono deputati. Il controllo dell'autorità giudiziaria, compulsata su iniziativa dello stesso provider, diviene elemento accidentale, chiaramente subordinato all'eventualità che il privato abbia le competenze tecnico-giuridiche necessarie a denunciare un abuso.

Ne deriva l'auspicio di un adeguamento delle proposte avanzate rispetto alla giurisprudenza, in particolare di quella occorsa negli anni successivi al 2018 (anno della Proposta). Tanto consentirebbe di evitare una futura attività di "instradamento" e correzione da parte delle Corti europee che, per la formulazione attuale della Proposta, appare fortemente probabile.

A conclusione del presente lavoro, ci sembra opportuno ricordare che alcuni autori hanno paventato la costituzione di un unico organo giurisdizionale europeo deputato a svolgere i controlli che la Proposta vorrebbe invece affidare ai *providers*[47]. Probabilmente, nell'attuale tendenza alla c.d. *agencification* dell'Unione europea appare più verosimile la creazione di un'Agenzia, sebbene la Proposta preveda la possibilità di coinvolgere Eurojust in sede di esecuzione. Ad ogni modo, all'organo dovrebbe spettare, in particolare, la valutazione delle richieste istruttorie circa gli standard di tutela dei diritti consacrati nella CEDU e nella Carta di Nizza[48]. L'autorità in questione non potrebbe esimersi, a tal proposito, dal considerare la gravità dei reati oggetto del procedimento, le modalità e le circostanze di emissione del provvedimento, la presenza di elementi di prova a carico del sospettato già presenti in quel momento, nonché il contenuto e la finalità del provvedimento[49], rendendo sostanzialmente operativi i principi di necessità e di proporzionalità.

[47] Come teorizzato da M. Daniele, *L'acquisizione delle prove dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Revista Brasileira de Direito Processual Penal*, Vol. 5, N. 3, 2019, pp. 1292-1293.
[48] Come del resto parzialmente inteso all'art. 9, par. 5 della Proposta: "[…] *risulta che esso viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o che è manifestamente arbitrario*".
[49] Dovrebbe trattarsi di un organo in grado di operare con la massima efficienza, capace di soddisfare in tempi ragionevolmente rapidi richieste provenienti da ogni parte del globo. A questo fine potrebbe magari essere utile prevedere, nei casi di urgenza, una procedura velocizzata. Com'è evidente, la soluzione è complessa per le difficoltà di predisposizione e di mantenimento di tale organo.