https://doi.org/10.6092/issn.1825-1927/17201 ISSN 1825-1927

La Natura Transnazionale della *Digital Evidence* tra Richieste di Cooperazione e Pretese di Sovranità

Un Equilibirio Necessario per il Contrasto alle Nuove Forme di Criminalita'

Gaspare Dalia*

Abstract: L'evoluzione tecnologica porta con sé due conseguenze negative: l'emersione di nuovi crimini informatici e l'aumento esponenziale di crimini comuni commessi attraverso l'uso degli strumenti informatici. L'obiettivo della ricerca è stato quello di comprendere come anche il tema della cooperazione giudiziaria in materia penale possa trarre beneficio dalla recente apertura alla firma del Secondo Protocollo aggiuntivo alla Convenzione di Budapest: se gli Stati non sono capaci di accordarsi sulla previsione di norme processuali comuni ai fini dell'accertamento dei reati a carattere sovranazionale, secondo una logica federale che andrebbe perseguita, se non altro, a livello europeo, emerge però un difetto di fondo dell'assetto vigente. L'entrata in vigore della legge 18 marzo 2008, n. 48 ha rappresentato un fondamentale passo per l'adeguamento del sistema processual-penalistico italiano a *standard* condivisi, così come significativa è la circostanza che il Secondo Protocollo sia stato aperto alla firma sotto la presidenza italiana del Comitato dei Ministri del Consiglio d'Europa. Ad una prima lettura, appare evidente l'arricchimento dello strumentario messo a disposizione delle autorità giudiziarie nazionali – basti pensare alle nuove previsioni in materia di videoconferenza e squadre investigative comuni, di cui agli artt. 11 e 12 – che mira a fissare la cornice normativa in mancanza di altre e specifiche disposizioni tra le autorità chiamate ad operare. La vera sfida sarà capire se la Convenzione *Cybercrime* per la tempestività e lungimiranza con cui è stata redatta – abbracciando a tutto campo le esigenze di tutela penale sostanziale, di innovazione ed armonizzazione della disciplina processuale e degli strumenti di indagine, nonché di cooperazione internazionale – rappresenterà effettivamente un efficiente baluardo contro le più moderne forme di criminalità, da contrastare a livello sovranazionale, proprio alla luce del Secondo Protocollo addizionale.

Parole chiave: cooperazione, sovranità, tutele, transnazionale, prova, utilizzabilità.

1 La cooperazione giudiziaria in materia penale e i limiti derivanti dalla circolazione della prova elettronica

L'evoluzione tecnologica, tra i tanti aspetti positivi, porta con sé almeno due conseguenze negative: l'emersione di nuovi crimini informatici e l'aumento esponenziale di crimini comuni commessi attraverso l'uso degli strumenti informatici[1].

*Dipartimento di Scienze Giuridiche – Scuola di Giurisprudenza, Università degli Studi di Salerno; ✉ gadalia@unisa.it

1. Come precisato in dottrina, per evitare vuoti di tutela è preferibile assumere la nozione più ampia possibile di *computer*, per ricomprendere i sistemi a programma variabile, gli elaboratori cosiddetti dedicati, nonché i calcolatori nei quali l'inserimento del *software* è precostituito mediante *firmware* o circuitazione integralmente prestabilita e non mutabile. Sul punto, R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti, 1994, *Profili penali dell'informatica*, Giuffrè, Milano; S. Aterno, *Aspetti problematici dell'art. 615-quater c.p.,* 2000, in *Cass Pen*., Milano. «Essenziale è l'elaborazione dei segnali in formato digitale (bit) e non analogico, mediante una pluralità di istruzioni, che fa assumere rilevanza alla diversa programmabilità e alla variabilità dei risultati: ritenendo diversamente si rischierebbe di confondere un sistema informatico con un semplice apparecchio elettronico», in questi termini F. Corona, 2021, *Il cybercrime: soggetto, oggetto e condotta*, in *Reati informatici e investigazioni digitali*, F. Corona (a cura di), Pacini Giuridica, Pisa, p. 19. Sul tema sia consentito, altresì, il rinvio a G. Dalia, 2016, *I reati informatici*, in AA.VV. *Manuale di diritto dell'informatica*, Edizioni Scientifiche Italiane, p. 657-689.

A tal proposito, occorre comprendere come anche il tema della cooperazione giudiziaria in materia penale, chiamato inevitabilmente a misurarsi con la dirompente digitalizzazione – quale causa dell'emersione, sempre più diffusa, di fattispecie criminose che si estendono oltre i confini nazionali –, possa trarre beneficio dalla recente apertura alla firma del Secondo Protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001[2], interamente dedicato alla cooperazione rafforzata ed alla divulgazione delle prove elettroniche.

È pacifico che il principio di sovranità nazionale e le prerogative riconosciute ai singoli Paesi subiscano un'ulteriore attenuazione quando le autorità giudiziarie siano chiamate a fronteggiare, appunto, la circolazione ed utilizzazione della prova elettronica formatasi altrove rispetto al luogo di utilizzazione e/o spendibilità della stessa nell'ambito di un procedimento penale incardinatosi dinnanzi all'autorità giudiziaria di altro Paese.

Nonostante la resistenza, registrata in molti Paesi, ad accettare la natura quasi completamente transnazionale della prova elettronica[3], gli stessi si sono dovuti necessariamente misurare con diversi fattori[4].

In primo luogo, la localizzazione e conservazione della prova elettronica, dovendo fare i conti con le svariate sedi degli *Internet service provider*[5] (privati) dislocati ovunque nel mondo, che ben potrebbe essere considerato personalmente responsabile per illeciti commessi con la propria condotta: si pensi, ad esempio, alla diffusione illecita di dati personali degli utenti registrati.

Tuttavia, il profilo di maggiore interesse rimane quello legato ad una sua eventuale responsabilità per illeciti commessi da terzi, ovvero gli utenti che sfruttano la struttura tecnica dell'*Isp*.

Tale aspetto ha condotto, con ogni probabilità, ad un atteggiamento di chiusura da parte di questi quando chiamati a fornire determinate informazioni, al fine di scongiurare il rischio di essere esposti ad azioni risarcitorie da parte di chi si possa ritenere danneggiato dal contenuto delle informazioni oggetto dei servizi telematici[6].

A ciò si aggiunga un ulteriore livello di dilatazione dello spazio in presenza di indagini informatiche rappresentato dalla captazione delle prove digitali reperibili nel *cloud*, ossia direttamente in rete.

Si tratta di dati che perlopiù non sono localizzabili in uno specifico Stato, ma che, per ragioni economiche od organizzative, vengono fatti circolare dai loro gestori fra *server* situati in diversi Stati.

In casi del genere, le prove digitali si trovano "diluite" in una zona neutrale, in cui la dissoluzione del parametro della *lex loci,* a beneficio di una raccolta interamente disciplinata dalla *lex fori* dello Stato che la effettua, magari in forza di regole non dotate di un sufficiente tasso di garanzia, rischia di mettere in crisi la legalità processuale[7].

In secondo luogo, la natura transnazionale del presunto crimine richiede necessariamente una disciplina rinvenibile in accordi fra gli Stati coinvolti per il relativo accertamento.

2. La Convenzione entra in vigore il 1° luglio 2004, tra dubbi e incertezze, tanto da essere ratificata in Italia solo nel 2008. Ad oggi, è recepita da 67 Stati di cui due, seppur firmatari, non l'hanno mai ratificata (Irlanda e Sud Africa).

3. Sugli aspetti che determinano la natura transazionale della prova elettronica, si rinvia a F. Spiezia, 2022, *Cooperazione internazionale e tutela delle vittime nel cyberspazio*, in *Diritto penale e processo. Speciale cybercrime*, 9, p. 1137-1142.

4. Per un'accurata panoramica del tema v. J. P. M. Bonnici, M. Tudorica, J. A. Cannataci, 2015, *La regolamentazione delle prove elettroniche nei processi penali*, in *Informatica e diritto*, XLI annata, Vol. XXIV, n. 1-2, pp. 201-215.

5. Il riferimento è al soggetto che gestisce la rete informatica su cui transitano le informazioni telematiche fornendo a terzi l'accesso alla stessa, sia gratuitamente che a pagamento. Tale accesso è garantito esclusivamente attraverso una procedura di registrazione che genera username e password previo rilascio di una serie di dati che consentono al provider di registrare i file di log, relativi alla connessione effettuata da ciascun utente, i quali consentiranno in futuro di individuare da quale utenza sia stata effettuata una determinata connessione, la sua durata ed i siti visitati. In dottrina, v. A. Ghirardini, G. Faggioli, 2013, *Computer Forensics*, Apogeo, Milano; D. D'Agostini, 2007, *Diritto penale dell'informatica, dai computer crimes alla digital forensic*, Experta edizioni.

6. L. Cuomo, R. Razzante, 2009, *La nuova disciplina dei reati informatici*, Giappichelli, Torino; S. Amore, V. Stanca, S. Staro, 2006, *I crimini informatici, Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Halley editrice, Milano.

7. «L'informatica ha creato mezzi di ricerca della prova capaci di coprire spazi fisici e virtuali sempre più estesi. Eppure la legge si è finora dimostrata incapace di regolarne l'utilizzo, a livello tanto nazionale quanto sovranazionale. Sul primo fronte emergono asimmetrie nel dosaggio delle garanzie, velleitari tentativi di limitare il raggio operativo di taluni strumenti (si pensi alle intercettazioni ambientali tramite i c.d. captatori), e preoccupanti vuoti normativi tali da lasciare eccessiva libertà alla giurisprudenza (è il caso delle perquisizioni online). Sul fronte sovranazionale, poi, è evidente come la disciplina della cooperazione giudiziaria non è in grado di evitare che le acquisizioni delle prove digitali effettuate dall'estero eludano le tutele previste dagli ordinamenti nazionali in cui le medesime sono reperibili. Si sconta, qui, l'incapacità degli Stati di accordarsi in merito alla previsione di regole probatorie comuni, l'unica soluzione in grado di portare il dovuto ordine nell'attuale far west informatico», in questi termini M. Daniele, 2018, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Processo Penale e Giustizia*, 5, p. 831-839.

Riguardo al primo aspetto, chiaramente problematica è la scelta del regime giuridico da applicare alla raccolta, alla conservazione e all'utilizzazione degli elementi probatori: tradizionalmente, le regole in vigore nel luogo in cui vengono esperiti i mezzi di ricerca della prova.

Il fatto che gli Stati non siano capaci di accordarsi sulla previsione di norme processuali comuni ai fini dell'accertamento dei reati a carattere sovranazionale, secondo una logica federale che andrebbe perseguita – se non altro, a livello europeo – denota il difetto di fondo dell'assetto vigente: lacune ed incoerenze riscontrabili tanto a livello nazionale quanto a livello sovranazionale, che si evidenziando quando i singoli Stati dimostrano di non riuscire a liberarsi da schemi burocratici ormai obsoleti rispetto all'irrefrenabile sviluppo dell'informatica.

Negli addetti ai lavori vi è ampia consapevolezza rispetto alla delicatezza dei negoziati UE sul pacchetto *E-evidence*, atteso che, pur nel disciplinare strumenti fondamentali per una cooperazione giudiziaria rapida e agevole in materia penale, occorre garantire il rispetto dei diritti fondamentali sanciti dalla Carta e dalla Convenzione come riconosciuti dall'art. 6 del Trattato sull'Unione Europea[8].

2 Le proposte sovranazionali

L'attuale quadro normativo dell'Unione Europea contempla già strumenti di cooperazione giudiziaria internazionale diretti a disciplinare l'acquisizione transfrontaliera delle prove elettroniche nei procedimenti penali, basati su meccanismi di riconoscimento reciproco nei rapporti tra Stati membri e sull'assistenza giudiziaria nei rapporti con i Paesi terzi[9].

Nonostante l'articolato ed ampio strumentario normativo, uno dei maggiori ostacoli all'ottenimento della prova elettronica risiede nel fatto che, allo stato, i fornitori di servizi telematici non hanno alcun obbligo generale di essere fisicamente presenti nel territorio dell'Unione, potendo offrire i propri servizi in linea di massima da qualsiasi luogo del mondo.

Spesso accade, infatti, che rifiutino la produzione della prova digitale deducendo la carenza di giurisdizione dell'autorità procedente in ragione ora del luogo di stabilimento della propria sede principale, ora del luogo di ubicazione dei dati, ora della cittadinanza della persona in relazione alla quale questi ultimi sono stati richiesti. La situazione si complica quando risultano coinvolti Paesi terzi, ipotesi piuttosto prevedibile dal momento che molti dei maggiori fornitori di servizi telematici hanno sede legale negli Stati Uniti.

Al fine di superare questi problemi e di rendere più efficienti le procedure di acquisizione e di conservazione delle prove nell'ambito dei procedimenti penali, soprattutto con riferimento a quelle digitali, il 17 aprile 2018 la Commissione europea ha presentato due proposte normative tra loro complementari[10]:

– una proposta di Direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali da parte dei prestatori di servizi ai fini dell'acquisizione di prove nei procedimenti penali (COM (2018)226 *final*);

8. N. Russo, 2022, *20° anniversario della Convenzione di Budapest*, in *Diritto penale e processo, Speciale cybercrime*, 8, p. 1021; D. Curtotti, 2022, *Speciale sul Secondo Protocollo addizionale alla Convenzione di Budapest. Premessa*, in *Diritto penale e processo, Speciale cybercrime*, 8, p. 1017-1019.

9. Tra i principali vanno ricordati: la Direttiva 2014/41/UE sull'ordine europeo di indagine penale (EIO); la Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea del 29 maggio 2000; il Regolamento (UE) 2018/1727 del 14 novembre 2018 che istituisce Eurojust (e abroga la precedente Decisione 2002/187/GAI del Consiglio); il Regolamento (UE) 2016/794 che istituisce Europol; la Decisione quadro 2002/465/GAI del Consiglio relativa alle squadre investigative comuni; gli accordi bilaterali sulla mutua assistenza giudiziaria tra l'Unione e gli Stati terzi, come quello con gli Stati Uniti d'America e con il Giappone. In dottrina R. Belfiore, 2015, *Riflessioni a margine della direttiva sull'ordine europeo di indagine penale*, in *Cass. Pen.*, p. 3288C, fasc. 9; L. Camaldo – F. Cerqua, 2014, *La direttiva sull'ordine europeo di indagine penale. Le nuove prospettive per la libera circolazione delle prove*, in *Cass. Pen.,* 10, p. 3511B; S. Monici, 2017, *Emanate le norme di attuazione della Convenzione di assistenza giudiziaria in materia penale del 29 maggio 2000: quali margini operativi in vista dell'(imminente) trasposizione della direttiva sull'ordine europeo di indagine penale*, in *Eurojus*; E. Selvaggi, 2017, *Un ammodernamento diventato necessario per tutti gli Stati UE*, in *Guida dir*., n. 25, p. 45 ss.; E. Gonzato, 2016, *Squadre investigative comuni: l'Italia finalmente recepisce la decisione quadro 2002/465/GAI*, in *Eurojus*; G. Colaiacovo, 2017, *Nuove prospettive in tema di coordinamento delle indagini e cooperazione giudiziaria alla luce della disciplina delle squadre investigative comuni*, in *Dir. pen. cont*. – Riv. trim., 1, p. 169 ss.

10. Al fine di segnalare l'influenza "esterna" del diritto UE in materia digitale si ricorda che, con riguardo ai c.d. intermediari (e alla loro responsabilità, anche se non penale) la Commissione europea aveva già da tempo avviato due procedimenti legislativi presentando, il 15 dicembre 2020, un pacchetto di misure per aggiornare la disciplina UE del settore digitale ossia il regolamento Digital Services Act (DSA) che mira a regolare la sicurezza, la trasparenza e le condizioni di accesso ai servizi online, modificando la Dir. 2000/31/CE e il regolamento Digital Markets Act (DMA) che si occupa invece degli aspetti commerciali e di concorrenza. Entrambi gli atti sono stati approvati dal Parlamento Europeo il 5 luglio 2018 ed il Consiglio ha chiuso la relativa procedura il 18 luglio dello stesso anno.

– una 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*)[11].

Con il primo strumento si mira ad armonizzare le regole sulla rappresentanza legale di alcuni prestatori di servizi all'interno dell'Unione, al fine di identificare chiaramente a chi le autorità competenti degli Stati membri possano indirizzare i propri provvedimenti di acquisizione della prova emessi nei procedimenti penali e secondo quali procedure, così prevedendo una soluzione comune atta a superare l'attuale frammentazione delle discipline nazionali e a facilitare l'ottemperanza da parte dei *service providers*.

Con il secondo, invece, si persegue l'obiettivo di notificare direttamente gli ordini europei di produzione e di conservazione di prove elettroniche al prestatore di servizi nei casi in cui le autorità nazionali competenti rivolgano tali ordini a *providers* che non siano stabiliti sul proprio territorio. Esso mira a semplificare e rendere più rapido il processo di "messa in sicurezza" e acquisizione di prove digitali detenute da prestatori di servizi stabiliti o rappresentati nella giurisdizione di un altro Stato membro, prevedendo la trasmissione del provvedimento penale di conservazione o acquisizione della *E-evidence* direttamente dall'autorità nazionale richiedente al rappresentante legale designato dal *service provider* sul territorio europeo, con obbligo per quest'ultimo di ottemperare consegnandole direttamente i dati, salva la sussistenza di specifici e tassativi motivi che lo impediscano e senza poter opporre ragioni legate al luogo di conservazione dei dati.

È bene sottolineare fin da ora che tali strumenti possono essere utilizzati dalle autorità nazionali competenti solo in situazioni transfrontaliere, ossia nei casi in cui il prestatore di servizi sia stabilito o rappresentato in un altro Stato membro. Ove, invece, sia stabilito o rappresentato sul proprio territorio nazionale, le autorità requirenti dovranno continuare ad avvalersi delle misure normative messe a disposizione dal diritto interno[12].

Inoltre, occorre evidenziare che gli ordini europei di produzione e di conservazione di prove elettroniche sono stati concepiti per affiancare e non per sostituire gli strumenti di cooperazione giudiziaria già attualmente esistenti, che potranno dunque continuare ad essere utilizzati dalle autorità nazionali competenti quando li ritengano pertinenti ed appropriati. Si pensi, in particolare, all'ordine europeo di indagine penale, che ha in gran parte sostituito gli strumenti di cooperazione giudiziaria previsti dalla Convenzione del 2000 relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'UE[13] e che può avere ad oggetto qualsiasi atto di indagine, ivi compresa l'acquisizione della prova elettronica. Esso, tuttavia, prevede la trasmissione della richiesta dall'autorità giudiziaria di emissione a quella di esecuzione, la quale non ha l'obbligo di eseguirla subito; deve anzi sottoporla ad una serie di controlli che potrebbero condurre a rinviarne o, addirittura, a rifiutarne l'esecuzione.

Pertanto, ove l'acquisizione della prova elettronica sia l'unico atto di indagine transnazionale che l'autorità nazionale competente deve porre in essere, sarà tendenzialmente più rapido ed efficace emanare un ordine di acquisizione della prova elettronica piuttosto che un ordine europeo di indagine penale, atteso che il primo consente la trasmissione diretta della richiesta al *service provider* e non richiede il coinvolgimento dell'autorità giudiziaria del paese di esecuzione, se non con precisi limiti.

Invece, quando l'autorità nazionale deve compiere diversi atti di indagine nello Stato membro di esecuzione (e non solo l'acquisizione di prove elettroniche), potrebbe preferire ricorrere all'ordine europeo di indagine penale, al fine di formulare un'unica richiesta all'autorità giudiziaria dello Stato di esecuzione.

Ad ogni modo, al fine di salvaguardare i diritti fondamentali, l'articolo 4 dell'orientamento generale[14] ha previsto che gli ordini di produzione riguardanti dati relativi alle operazioni o al contenuto, atteso il loro carattere maggiormente invasivo della libertà

11. Vedasi la Dichiarazione comune dei Ministri della Giustizia e degli Interni dell'UE e dei rappresentanti delle Istituzioni UE sugli attentati terroristici di Bruxelles del 22 marzo 2016 e le Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel cyberspazio del 9 giugno 2016 (ST9579/16). Cfr. sul tema G. Suffia, 2018, *Geografia delle cyberwars. Uomini e Stati alla prova dello spazio digitale*, Milano.

12. In Italia, per esempio, il mezzo investigativo utilizzato dal pubblico ministero per ottenere la prova digitale dal *service provider* che abbia una sede di stabilimento o un rappresentante legale sul territorio italiano, è l'ordine di esibizione ai sensi dell'art. 256 c.p.p. Per quanto attiene, invece, alla conservazione della prova digitale, il sequestro probatorio di dati informatici presso fornitori di servizi previsto dall'art. 254 bis c.p.p. sembra essere lo strumento nazionale che più si avvicina concettualmente all'ordine europeo di conservazione, anche attesa la possibilità per l'autorità inquirente italiana di ordinare al fornitore di servizi la conservazione e adeguata protezione dei dati originali. Si rimanda, sul punto, alla nota a sentenza delle Sezioni Unite della Suprema Corte n. 40963/2017 di G. Todaro, 2017, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite*, in *Diritto penale contemporaneo*, 11, p. 157 ss.

13. Vedasi al riguardo M. Daniele, 2017, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d.lgs. n. 108 del 2017*, in *Diritto penale contemporaneo*, 7-8, p. 208.

14. Orientamento generale del Consiglio UE sulla proposta di Regolamento in parola, adottato dai Ministri della Giustizia degli Stati membri il 7 dicembre 2018.

personale, debbano essere emessi o autorizzati da un giudice o da un organo giurisdizionale o da un giudice addetto alle investigazioni, mentre quelli riguardanti i dati relativi agli abbonati o agli accessi possono essere emessi o autorizzati anche da un pubblico ministero. Quanto, invece, agli ordini di conservazione, considerata la loro mera finalità di "congelamento" del dato informatico, possono essere emessi o autorizzati da un'autorità giudicante ma anche da un pubblico ministero.

Appare rilevante precisare che in casi di emergenza e con riferimento ai soli ordini di produzione e di conservazione di dati relativi agli abbonati o agli accessi, la convalida dell'autorità giudiziaria o del pubblico ministero può essere richiesta successivamente all'emissione dei provvedimenti in parola e comunque non oltre le quarantotto ore (cosiddetta "*ex-post validation*"), a condizione che l'autorità emittente detenga tale potere di agire senza previa autorizzazione, in circostanze simili, da parte dell'ordinamento nazionale di appartenenza.

Ove la convalida non venga disposta, l'autorità emittente deve immediatamente revocare l'ordine in questione e procedere, secondo le norme del diritto nazionale, a cancellare ogni dato nel frattempo acquisito oppure ad assicurare che lo stesso non venga utilizzato come prova nel procedimento penale.

Un aspetto fondamentale da evidenziare è che tutti i dati che rientrano nella definizione di prova elettronica devono essere conservati in formato elettronico dal prestatore di servizi, o per suo conto, al momento della ricezione del certificato di ordine europeo di produzione o di conservazione.

Ciò significa che non può essere disposta dall'autorità nazionale la produzione o la conservazione di dati che vengano registrati dal *service provider* in un tempo futuro rispetto al momento di ricezione del relativo ordine, atteso che tale misura si tradurrebbe di fatto in un'intercettazione e che tale mezzo di ricerca della prova è stato, invece, volontariamente escluso dall'ambito di applicazione della proposta di Regolamento[15].

Tuttavia, il quadro normativo che emerge appare, per molti versi, più un punto di partenza che un punto di arrivo.

Particolarmente controversa appare la decisione sulla valenza da attribuire alla notifica dell'ordine di produzione allo Stato di esecuzione ed in particolare sul se mantenerne una natura meramente informativa oppure, come vorrebbero taluni Stati membri (finora in minoranza) farla divenire un mezzo di sindacato effettivo e di eventuale opposizione da parte dello Stato di esecuzione.

La risposta dipenderà dal grado di reale volontà di dare piena applicazione al principio del mutuo riconoscimento delle decisioni giudiziarie nazionali, strettamente collegato alla disponibilità a rinunciare alla propria sovranità nazionale ai fini della concreta realizzazione di uno spazio unico di libertà, giustizia e sicurezza. Un contributo importante potrebbe essere dato dal Parlamento europeo, che nell'esercizio della sua funzione di co-legislatore ha dato spesso prova di saper promuovere il raggiungimento di traguardi più ambiziosi rispetto a quelli proposti dagli Stati membri, guardando alla realizzazione di una effettiva integrazione giuridica europea[16].

3 Uno sguardo d'insieme al Secondo Protocollo addizionale alla Convenzione di Budapest sulla cooperazione rafforzata e la divulgazione delle prove elettroniche

Lo strumento principale d'azione del Consiglio d'Europa consiste nel predisporre e favorire la stipulazione di accordi o convenzioni internazionali anche con Paesi terzi, che costituiscono la base per l'armonizzazione delle rispettive legislazioni.

15. Vedasi il considerando 19 dell'orientamento generale. Si segnala, peraltro, che nel corso del negoziato intercorso in sede COPEN presso il Consiglio UE, taluni Stati membri, tra cui l'Italia, avevano proposto di allargare l'ambito di applicazione del Regolamento sia alle intercettazioni delle comunicazioni on-line ("real-time interception") che al cosiddetto "accesso diretto" da remoto dell'autorità giudiziaria ai dati disponibili nel server del provider senza bisogno del coinvolgimento di quest'ultimo ("direct access to e-evidence") a seguito della perquisizione e sequestro del dispositivo oppure attraverso l'uso delle credenziali di accesso dell'utente legittimamente acquisite. Questa proposta è stata portata dalla Presidenza bulgara all'attenzione dei Ministri della giustizia nella riunione del Consiglio UE – Giustizia e Affari interni del 4-5 giugno 2018 per riceverne linee politiche di indirizzo, ma molte delegazioni hanno espresso perplessità al riguardo e la Commissione europea ha manifestato forte contrarietà, ritenendo che ne sarebbe risultato stravolto l'impianto originario dell'iniziativa normativa, allungando notevolmente i tempi del negoziato e conseguentemente ritardando l'adozione dello strumento. L'opzione in parola è stata, pertanto, abbandonata sotto Presidenza austriaca.

16. R. Pezzuto, 2019, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della commissione europea al vaglio del Consiglio dell'Unione*, in *Diritto penale contemporaneo*, 1, p. 57.

Proprio tale necessità ha determinato l'adozione da parte del Consiglio d'Europa, nel 2001, della Convenzione di Budapest in materia di criminalità informatica[17] richiedendo ai singoli Stati di tipizzare una serie di offese legate all'utilizzo di strumenti informatici.

Particolare importanza all'interno della Convenzione riveste la disciplina dettata dall'articolo 22 in materia di giurisdizione: «per limitare l'area delle fattispecie non punibili a causa dell'ontologica delocalizzazione del crimine informatico» il citato articolo prevede infatti che, per i reati indicati dalla Convenzione, ogni ordinamento debba perseguire penalmente le condotte comprese nel territorio di ciascuno Stato aderente alla Convenzione medesima, anche quando siano state poste in essere da un cittadino straniero, se l'infrazione è penalmente punibile laddove è stata commessa o se l'infrazione non rientra nella competenza territoriale dello Stato è inoltre creato uno spazio giudiziario comune in base al quale, quando più Stati rivendicano la propria competenza, le diverse autorità statuali provvederanno ad una consultazione al fine di stabilire il modo più appropriato per esercitare l'azione penale.

Quindi, per ciò che attiene alla collaborazione fra gli Stati, è previsto che le autorità statuali cooperino fra loro nella misura più ampia possibile nello svolgimento delle relative investigazioni[18].

L'obiettivo del legislatore era, ed è, quello di preservare l'integrità e l'immodificabilità del dato digitale originario, sia all'atto della sua acquisizione, sia con riferimento a tutta la catena di conservazione del reperto[19]; ciò nella convinzione che, qualora la fase dell'acquisizione e quella della conservazione siano improntate a regole uniformi e rigorose, nella successiva fase di valutazione da parte del giudice, gli elementi di prova raccolti potranno essere considerati idonei a provare i fatti della causa.

In tal senso, la Convenzione di Budapest prescrive agli Stati membri di provvedere, una volta acquisita la prova della commissione degli illeciti[20], ad assumere misure idonee a garantire la conservazione dei dati informatici facilmente modificabili ed al mantenimento dell'integrità delle informazioni per il tempo necessario all'individuazione dei colpevoli ed all'accertamento processuale della loro responsabilità.

Il materiale da selezionare potrebbe essere molto vasto, ed è proprio per questo che risulta indispensabile l'utilizzazione di *software* di ricerca e di selezione delle informazioni ai fini dell'individuazione[21].

Il criterio metrico-selettivo adottato dal consulente tecnico o dal perito nominato dal Tribunale è molto importante, perché è l'unico capace di delimitare il campo della ricerca selezionando questo o quel materiale. E questo è il primo punto di difficoltà per un consulente tecnico, in quanto, non avendo un punto di riferimento per giustificare la legittimità del proprio operato, deve procedere sulla base di quella che è considerata la metodologia migliore.

Questa prima selezione dei dati è il punto di partenza per giungere alla seconda fase: l'acquisizione. Fase facilmente esposta a rischi di alterazione o dispersione, rispetto alle tradizionali prove acquisite in quanto anche la semplice accensione del *computer* determina una automatica alterazione dei file di registro del sistema, con conseguente perdita di informazioni che potrebbero essere rilevanti ai fini della causa; al contrario, lo spegnimento di un *computer* acceso determinerebbe la perdita, dalla memoria "*ram*", di informazioni anche importanti sull'attività svolta al momento della perquisizione.

Si intuisce come l'attività di acquisizione da un *computer* acceso debba essere considerato un atto di natura "irripetibile", da compiere nel contraddittorio tra le parti proprio per evitare contestazioni processualmente valide e quindi potenzialmente invali-

17. «L'obiettivo primario della Convenzione sulla criminalità informatica risiede nell'esigenza di introdurre... un minimum target di tutela dei beni giuridici offesi dai cybercrimes ed un livello minimo essenziale comune di strategie di contrasto a tali illeciti, soprattutto in ragione della loro natura tendenzialmente transnazionale, che comporta chiaramente la necessità dell'armonizzazione della relativa normativa di contrasto nell'ambito dei vari ordinamenti», in questi termini F. Resta, 2008, *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura*, in *Corriere del Merito*, Torino.

18. In dottrina, L. Cuomo, R. Razzante, *La nuova disciplina dei reati informatici*, cit.; D. D'Agostini, *Diritto penale dell'informatica,* cit. Nell'ordinamento italiano, l'entrata in vigore della legge 18 marzo 2008, n. 48, di ratifica della Convenzione di Budapest, ha rappresentato un fondamentale passo per l'adeguamento del sistema processual-penalistico italiano agli standard europei, così come significativa è la circostanza che il Secondo Protocollo addizionale sia stato aperto alla firma sotto la presidenza italiana del Comitato dei Ministri del Consiglio d'Europa.

19. A livello internazionale esistono documenti redatti per istruire i tecnici nella condotta delle attività di acquisizione quali "The good practices guide for Computer based electronic evidence" pubblicato dalla NHCTU inglese nel 2003 e la "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition" pubblicato dal Dipartimento di Giustizia degli Stati Uniti d'America; più importante ancora il documento RFC3227 "Guidelines for Evidence Collection and Archiving" pubblicata nel febbraio 2002.

20. Prova informatica può essere definita come «la rappresentazione di un insieme di dati ed informazioni digitalizzate, facenti capo ad un determinato fatto o evento, informazioni che sono espresse in linguaggio informatico che, per sua stessa natura, non è immediatamente intellegibile dall'uomo attraverso i suoi sensi». Così L. Luparia, G. Ziccardi, 2007, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano.

21. L. Marafioti, 2011, *Digital evidence e processo penale*, in *Cass. pen.*, p. 4509-4523.

danti in sede processuale[22]. In sintesi, «più il processo di acquisizione e conservazione sarà improntato a criteri di scientificità e rigore, maggiori saranno le probabilità che il giudice consideri gli elementi raccolti idonei a provare i fatti oggetto della causa»[23].

Tuttavia, una delle originarie debolezze[24] della Convenzione di Budapest si rinveniva nel silenzio della normativa rispetto alla regolamentazione della raccolta in tempo reale e/o l'intercettazione dei dati sul traffico e dei dati relativi ai contenuti quando tali presunte informazioni si trovino al di fuori della giurisdizione dello Stato in cui si sta svolgendo l'indagine.

Secondo la Convenzione, le autorità competenti sono autorizzate a raccogliere o a registrare i dati sul traffico trasmessi da un sistema informatico in tempo reale. Se i dati a cui si vuole accedere sono pubblici, l'autorità che investiga può accedere a tali dati ovunque sia la loro locazione geografica, senza l'autorizzazione delle autorità dello Stato che ha giurisdizione sul territorio in cui si trovano tali dati.

Inoltre, la Convenzione stabilisce che quando l'autorità giurisdizionale dello Stato in cui si svolge l'investigazione ha fatto accesso o ha ricevuto i dati memorizzati fuori dal proprio territorio attraverso un sistema informatico presente nel proprio territorio e ha ottenuto il consenso legale e volontario della persona legalmente autorizzata a divulgare i dati all' autorità giurisdizionale dello Stato investigante, allora quest'ultima può procedere senza l'autorizzazione delle autorità competenti dell'altro Stato.

In quest'ultimo caso, chi sia la persona legittimamente autorizzata a divulgare questi dati dipende dalle circostanze del caso, dalla natura della persona e dalla specifica legge da applicare.

Perciò, in tutti gli altri casi, la parte investigante deve attivare una procedura di mutua assistenza giudiziaria che è molto dispendiosa in termini di tempo.

Durante la fase di preparazione della Convenzione è stato molto discusso il problema di quando dovesse essere permesso alla parte investigante di accedere unilateralmente ai dati memorizzati su dispositivi localizzati in altre giurisdizioni, senza chiedere la mutua assistenza.

Probabilmente, la mancata esperienza ed il momento storico in cui è maturato l'accordo portarono alla conclusione che non fosse ancora possibile approntare una regolamentazione completa e giuridicamente vincolante della materia.

Per tali ragioni, il 12 maggio 2022 si è resa necessaria l'apertura alla firma del Secondo Protocollo aggiuntivo alla Convenzione di Budapest sulla cooperazione rafforzata e la divulgazione delle prove elettroniche.

Inoltre, con Decisione (UE) 2023/436 del Consiglio del 14 febbraio 2023 gli Stati membri sono stati autorizzati a ratificare il suddetto protocollo il cui obiettivo è stabilire norme comuni a livello internazionale per rafforzare la cooperazione in materia di criminalità informatica e la raccolta di prove in formato elettronico a fini di indagini o procedimenti penali.

Come si legge nel Preambolo, il Protocollo «fornisce una base giuridica per la divulgazione di informazioni relative alla registrazione dei nomi di dominio e per la cooperazione diretta con i fornitori di servizi per le informazioni sugli abbonati e dati relativi al traffico, la cooperazione immediata in casi di emergenza, strumenti di assistenza reciproca, come anche garanzie in materia di protezione dei dati personali».

22. Un'evidenza informatica per poter essere impiegata a livello probatorio deve rispettare i seguenti principi: a) Ammissibilità; b) Autenticità; c) Completezza; d) Attendibilità; e) Credibilità. In dottrina A. Macrillò, 2008, *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. Internet*, Milano; G. Ziccardi, 2006, *Informatica giuridica*, Giuffrè, Milano. In pratica, l'evidenza informatica potrà essere considerata attendibile solamente se non sussistono dubbi su come sia stata acquisita e successivamente manipolata, evitando che si possano sollevare dubbi in merito alla veridicità. Al fine di comprendere la complessità del problema in esame, immancabile deve essere il riferimento agli ondivaghi orientamenti della giurisprudenza interna che, solo da ultimo, si è assestata sul riconoscere a tale attività il carattere della irripetibilità. V'è da aggiungere che, comunque, è sempre più diffuso l'atteggiamento prudenziale dei pubblici ministeri italiani che adottano la procedura *ex* art. 360 c.p.p. nel delegare il compimento di simili operazioni, ovvero attraverso un accertamento tecnico irripetibile e, perciò, almeno partecipato da indagato e persona offesa.

23. Da Valle, 2008, *Legge 18 marzo 2008 (criminalità informatica), art. 9,* in *Legisl. pen*., p. 298; cfr. F. Cajani, 2013, *Il vaglio dibattimentale della digital evidence*, in *Archivio Penale* settembre-dicembre, fascicolo 3 anno LXV; pp. 837–852.

24. Sotto il profilo pratico-operativo, l'obiettivo per il futuro è quello di delineare una procedura più agile e snella rispetto a quella già sperimentata dalla Convenzione del 2001, superando cioè la distinzione previgente sull'*iter* da seguire per acquisire dati allocati su *server* situati nel territorio dello Stato Parte, ovvero su *server* fuori giurisdizione; ciò anche nell'ottica di preservare l'integrità dei dati informatici per la cui tutela il "fattore tempo" risulta dirimente. In dottrina, cfr. F. Graziani, 2019, *L'acquisizione della prova digitale all'estero: verso un secondo protocollo addizionale alla Convenzione di Budapest sul cybercrime,* in A.a. V.v., *Lo spazio* cyber *e cosmico Risorse dual use per il sistema Italia in Europa*, (a cura di) S. Marchisio – U. Montuoro, Torino, p. 56 ss.

Per quanto concerne la tutela dei diritti fondamentali, l'art. 13 impone agli Stati aderenti al Protocollo, di fare in modo che le procedure interessate alla sua applicazione garantiscano una tutela adeguata dei diritti fondamentali, anche se "curiosamente[25]" alle «alle condizioni e alle garanzie previste dal proprio diritto interno», e il rispetto del principio di proporzionalità, ai sensi dell'art. 15 della Convenzione.

L'auspicio è che tali condizioni e garanzie non vengano strumentalizzate dai singoli Stati, come già accaduto in passato, per sacrificare la cooperazione sull'altare della sovranità statuale.

Nel descritto contesto, si ribadisce la circostanza che spesso le prove informatiche oggetto del protocollo siano nella disponibilità di fornitori di servizi online i quali giocano un ruolo fondamentale per il corretto bilanciamento di opposte posizioni giuridiche al punto che ne è stata riconosciuta una funzione quasi "*governmental*"[26].

In merito, è stato osservato che la regolamentazione predisposta sembri realizzata non più mediante l'imposizione di obblighi materiali, cioè di contenuto sostanziale, ma attraverso norme di rito, e quindi intervenendo sui procedimenti i quali poi si riflettono, seppur indirettamente, sulle questioni sostanziali[27]. Tale approccio pare caratterizzare anche la logica del Secondo Protocollo addizionale proprio al fine di agevolare e rafforzare la cooperazione senza restare impigliati nelle maglie di questioni sostanzialistiche che da più parti potrebbero essere sollevate.

Sul piano pratico, si pensi al contesto operativo in cui è chiamato ad intervenire l'art. 6 del Secondo protocollo – che rientra nelle misure di cooperazione rafforzata[28] – relativo all'accesso da parte delle forze dell'ordine ed autorità giudiziarie alle informazioni di identificazione del titolare di un nome di dominio *Internet*.

La disposizione prevede che la richiesta sia inviata direttamente dalle autorità competenti al fornitore di servizi, senza pertanto passare attraverso l'autorizzazione o l'intermediazione delle autorità giudiziarie della giurisdizione di destinazione. Specularmente, è previsto che ciascuna Parte adotti le misure necessarie per consentire ai fornitori di servizi di registrazione dei nomi di dominio presenti sul suo territorio di rispondere alle richieste avanzate.

Tale misura, tuttavia, non è da intendersi come impositiva di un obbligo a fornire una risposta, che altresì può essere prodotta alle «condizioni ragionevoli previste dal diritto nazionale» necessarie a bilanciare l'esigenza di condurre investigazioni efficaci – dal momento che nello scenario attuale trattasi di informazioni non più disponibili su fonti aperte – e preservare diritti e libertà fondamentali dell'individuo. La norma, dunque, preserva l'elemento di volontarietà della cooperazione[29] tra autorità competenti e fornitori di servizi in un'altra giurisdizione, riaffermando un principio cardine applicato in questi venti anni di vigenza della Convenzione.

Inoltre, governata da un rapporto esclusivo tra autorità competente a raccogliere il dato e società fornitrici di servizi è anche l'acquisizione dei *subscriber data*, il cui *status* giuridico è stato finalmente cristallizzato[30] all'art. 7 del Secondo Protocollo.

Anche in tal caso occorre sperare che riserve generali o clausole di salvaguardia procedimentali non pregiudichino l'efficienza di tale sistema di accesso transfrontaliero data anche la rilevanza di tali dati quali elementi informativi primari e basilari nell'attività investigativa.

---

25. In questi termini, G.M. Ruotolo, 2022, *Il Secondo Protocollo alla Convenzione cybercrime sulle prove elettroniche tra diritto internazionale e relazioni esterne dell'Unione europea*, in *Diritto penale e processo, Speciale cybercrime*, 8, p. 1022-1027.

26. F. Wettstein, 2009, *Multinational Corporations and Global Justice: Human Rights Obligations of a Quasi-Governmental Institution,* Stanford; G.M. Ruotolo, 2021, *Scritti di diritto internazionale ed europeo dei dati*, Bari, p. 229 ss.

27. G.M. Ruotolo, *Il Secondo Protocollo alla Convenzione cybercrime sulle prove elettroniche tra diritto internazionale e relazioni esterne dell'Unione europea*, cit., p. 1026.

28. Si intende che tali procedure si applicano indipendentemente dall'esistenza o meno di un Trattato di assistenza giudiziaria o di un accordo fondato su normative uniformi e reciproche tra le parti interessate.

29. Per una prima analisi della disposizione citata, si rinvia a M. Lucchetti, 2022, *L'acquisizione di informazioni sulla registrazione di nomi di dominio nelle investigazioni in materia di cybercrime (art. 6)*, in *Diritto penale e processo. Speciale Cybercrime*, 8, p. 1041-1044

30. Così, C. Pirozzoli, 2022, *Acquisizione del subscriber data: dalla Convenzione di Budapest al Protocollo addizionale (art. 7)* in *Diritto penale e processo. Speciale Cybercrime*, 8, p. 1045-1049 secondo cui, con riferimento all'art. 18 della Convenzione di Budapest "la limitata operatività, solo"domestica", della previsione ha rappresentato un limite rispetto alla reale esigenza di acquisire i predetti dati in modo generalizzato, transnazionale e soprattutto efficiente e ciò proprio in virtù della moltitudine di operatori esistenti ed operanti a livello globale […] si è ritenuto cruciale istituire e formalizzare un meccanismo complementare prescindendo dalle ipotesi di *voluntary disclosure* da parte degli *ISP*". Sul tema, cfr., altresì, W. Nocerino, 2022, *La cooperazione internazionale rinforzata per lo scambio di dati degli abbonati e di traffico (art. 8)*, in *Diritto penale e processo. Speciale Cybercrime*, 8, p. 1050-1054.

Al di là dei tecnicismi che caratterizzano un istituto piuttosto che un altro, come accuratamente osservato in dottrina[31], "l'impatto concreto di tali previsioni dipenderà, in primo luogo, dalla scelta degli Stati membri di aderire o meno al Protocollo".

Inoltre, fatta salva l'adesione, saranno decisive le dichiarazioni di cui all'art. 9 par. 5 all'art. 10, par. 9 che delineeranno nel concreto una sorta di "limite di velocità" dell'intero meccanismo di cooperazione rafforzata in presenza di situazioni di emergenza.

Ad una prima lettura, però, appare evidente l'arricchimento dello strumentario messo a disposizione delle autorità giudiziarie nazionali.

Basti pensare, altresì, alle nuove previsioni in materia di videoconferenza e squadre investigative comuni, i cui artt. 11 e 12 mirano a fissare la cornice normativa in mancanza di altre e specifiche disposizioni tra le autorità chiamate ad operare.

Nonostante verso le prime siano state già sollevate non poche perplessità con riferimento al rispetto delle garanzie individuali e dei principi del rito penale[32], le seconde sono state recepite come strumenti di condivisione di percorsi investigativi in grado di determinare l'attenuazione delle differenze e dei rallentamenti causati dalle frontiere nazionali superando il modello cooperativo basato sul vetusto meccanismo rogatoriale[33]; sempre che la forte vocazione repressiva sottesa allo strumento non determini un conflitto con l'insieme delle garanzie e tutele a presidio dei diritti fondamentali.

È per questo che una delle principali critiche sollevate in questo ambito – sia dai teorici della materia, sia dai soggetti che operano in maniera pratica – riguarda il concetto di giurisdizione territoriale, in particolare applicato alla regolamentazione dei poteri di investigazione, che risulta piuttosto restrittivo e non adatto all'attuale realtà tecnologica dove l'informazione elettronica viene elaborata, scambiata, e conservata nell'ambito di giurisdizioni diverse e in relazione ad aree geografiche diverse.

Dunque, è evidente come da questa breve panoramica emerga la *ratio* delle singole disposizioni: energico rafforzamento degli strumenti di cooperazione.

Ora, non resta che attendere la loro entrata in funzione per testarne l'effettiva capacità operativa.

4 Conclusioni

Sia a livello internazionale che europeo, è costante la tendenza ad incoraggiare la volontarietà della cooperazione tra autorità competenti e fornitori di servizi ricadenti in un'altra giurisdizione.

La vera sfida sarà capire se, anche per la tempestività e lungimiranza con cui è stata redatta, la Convenzione *Cybercrime* – soprattutto alla luce del Secondo Protocollo addizionale – resterà un punto di riferimento, quale efficiente baluardo contro le più moderne forme di *cyber*-criminalità.

È anche vero, però, che per risolvere i limiti evidenziati non basta soltanto introdurre nuovi accordi internazionali o armonizzare meglio le regole sulle prove elettroniche.

La situazione appare più complessa, ed è necessaria l'elaborazione di nuovi concetti giuridici e la collaborazione di una ampia varietà di soggetti[34].

Svantesson[35] ed altri sostengono che sia arrivato il momento di distinguere tra giurisdizione delle autorità che giudicano e applicano le leggi (*enforcement jurisdiction*) e giurisdizione delle autorità che conducono le investigazioni (*investigative jurisdiction*): mentre la competenza limitata al territorio di uno specifico Stato è pienamente comprensibile e ragionevole rispetto alle autorità

31. F. Cajani, 2022, *Le procedure di emergenza (artt. 9-10)*, in *Diritto penale e processo. Speciale Cybercrime*, 8, p. 1055-1060; ID, 2017, *"The song remains the same" riflessione sul tempo che passa e sulla necessità di "macchine utili" per un'effettiva tutela delle vittime di reati*, in F. Cajani - G. Cernuto – G. Costabile - F. D'Arcangelo, *Le nuove frontiere dell'acquisizione degli elementi di prova nel cyberspace*.

32. Sul punto, accuratamente D. Curtotti, 1999, *L'uso dei collegamenti audiovisivi nel processo penale tra necessità di efficienza del processo e rispetto dei principi garantistici*, in *Riv. It. Dir. proc. pen*., p. 492; O. Murro, 2022, *La disciplina della videoconferenza per le dichiarazioni del testimone e dell'esperto*, in *Diritto penale e processo, Speciale cybercrime*, 9, p. 1143-1146.

33. G. Colaiacovo, 2022, *Squadre investigative comuni e investigazioni congiunte: una prima lettura*, in *Diritto penale e processo. Speciale cybercrime,* 9, p. 1147-1150; G. Barrocu, 2019, *Le squadre investigative comuni*, in M. R. Marchetti – E. Selvaggi, *La nuova cooperazione giudiziaria penale*, Padova, p. 393.

34. J. P. M. Bonnici, M. Tudorica J. A. Cannataci, *Informatica e diritto*, cit. pp. 201-215

35. D. Svantesson, *Preliminary Report: Law Enforcement Cross-Border Access to Data*, 2016, in ssrn.com/abstract=2874238

che giudicano e applicano le leggi nazionali, l'attività investigativa non dovrebbe trovare limiti di accesso transnazionali ai dati e alle prove elettroniche.

Va da sé che un altro aspetto che dovrebbe essere ripensato nell'ambito delle prove elettroniche (transnazionali) è il concetto dell'ammissibilità delle prove che non dovrebbe rappresentare un problema a patto che siano state acquisite legalmente: l'ammissibilità viene valutata dal giudice caso per caso.

Allo stato, la valutazione di "acquisizione legale" non è basata su principi/regole omogenee e questa difformità di approcci può rappresentare un ostacolo all'utilizzo di prove elettroniche ottenute in un'altra giurisdizione. È dunque importante stabilire delle regole comuni in questo ambito.

Il valore probatorio della prova non si riduce a causa della sua natura elettronica[36]; inoltre, la raccolta, la conservazione, l'uso e lo scambio non è generalmente limitato o proibito dalla legge. Tuttavia, la natura stessa della prova elettronica la rende volatile e facile da manipolare; sono quindi necessari protocolli e *standard* comuni per mantenerne l'integrità e per garantirne contestualmente, in maniera più agevole, l'ammissibilità di fronte a un tribunale di uno Stato membro, anche se ottenuta in un altro Stato.

Questi protocolli dovranno avere una base giuridica, essere concordati a livello internazionale ed essere integrati da un protocollo tecnologico per il trasferimento rapido dell'informazione da scambiare. Dato che gli stessi dovranno funzionare non solo tra gli Stati ma anche tra le forze di polizia e diversi soggetti privati, la loro stesura dovrà coinvolgere differenti soggetti/attori, compresi gli esperti in *digital forensics*[37].

Pensando alle prospettive future, dal momento che i lavori preparatori di una Convenzione promossa a livello globale dalle Nazioni Unite contro il crimine informatico sono ancora in una fase embrionale si può ritenere che la Convenzione *Cybercrime* continuerà a detenere un ruolo primario a livello internazionale[38]. Tuttavia, la stessa dovrà fare anche i conti con le novità in arrivo dai c.d. "*AI-crimes*", ossia i delitti riferibili a sistemi di intelligenza artificiale.

Non è consentito ignorare la continua evoluzione dei rapporti tra diritto e tecnologia all'interno di un contesto sempre più "tecnico", in costante movimento, capace di acuire una percezione di disagio tipica di ogni "mutamento di paradigma". Il rischio da evitare e lo scollamento tra il contesto tecnologico-sociale, le scelte del legislatore e l'interpretazione delle disposizioni[39].

In primo luogo, riconoscere centralità al diritto interpretato equivale a dare pieno compimento all'assetto istituzionale/costituzionale ed implementare le garanzie a tutela della persona[40]; in secondo luogo, il processo ermeneutico deve necessariamente inserirsi nel più ampio sistema multilivello di tutela dei diritti fondamentali e di interazione tra ordinamento interno e fonti sovranazionali; infine, occorre accettare la nascita di beni giuridici di nuovissima generazione che possono risultare espressione di innovative manifestazioni di diritti fondamentali, la cui compromissione sarà legittima se quelle stesse attività di indagine rispondono ai requisiti previsti dalla legge.

Tutto dipenderà, anche stavolta, dalla volontà di cooperare dei singoli Paesi e dal grado di fiducia che si vorrà, reciprocamente, garantire.

---

36. Questi dati testimoniano inequivocabilmente come la quotidianità di ogni individuo sia costantemente scandita dalla continua interazione con molteplici dispositivi mobili i quali, anche a prescindere dal più o meno specifico carattere informatico di un fenomeno criminale, possono rappresentare preziosi depositari di informazioni di interesse investigativo. In questi termini, K. La Regina,2022, *Le indagini su dispositivi digitali*, in *Investigazioni digitali* (a cura di Michele Iaselli), p. 28 - 72

37. S. Luparia, G. Ziccardi, 2011, *Le "migliori pratiche" nelle investigazioni informatiche: brevi considerazioni sull'esperienza italiana*, in F. Cajani – G. Costabile (a cura di), *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*, Forlì, p. 211 e ss.

38. Invero, in questi anni si è registrato un susseguirsi di nuovi strumenti di cooperazione, grazie al ruolo svolto parallelamente dall'Unione Europea che da un lato ha raccomandato a tutti di gli Stati membri di sottoscrivere e attuale la Convenzione *Cybercrime*, dall'altro ha fondato i suoi principali interventi sul principio del "riconoscimento reciproco" delle decisioni e dei provvedimenti giudiziari degli Stati membri. Sul tema, sia consentito il rinvio a G. Dalia, 2020, *Riconoscimento, valore ed esecuzione delle sentenze penali straniere*, Edizioni Scientifiche Italiane, Napoli.

39. R. Flor, 2022, *Le indagini ad alto contenuto tecnologico fra esigenze di accertamento e repressione dei reati e tutela penale di tradizionali e nuovi beni giuridici nell'era digitale*, in Dalla data retention alle indagini ad alto contenuto tecnologico, (a cura di) R. Flor – S. Marcolini, Giappichelli, Torino, p. 143-145.

40. R. Bartoli, 2020, *Le garanzie della "nuova" legalità,* in *Sistema pen*., 3, p. 143 ss.; F. Viganò, 2021, *Il diritto giurisprudenziale nella prospettiva della Corte Costituzionale*, in *Sistema pen*.

Bibliografia

Amore S., Stanca V., Staro S., I crimini informatici, dottrina, giurisprudenza ed aspetti tecnici delle investigazioni, 2006.

Aterno S., Aspetti problematici dell'art. 615-quater c.p., in cass pen., 2000.

Barrocu G., Le squadre investigative comuni, in Marchetti M.R., Selvaggi E., La nuova cooperazione giudiziaria penale, 2019, 393.

Bartoli R., Le garanzie della "nuova" legalità, in Sistema penale, 3, 2020,143 ss.

Belfiore R., Riflessioni a margine della direttiva sull'ordine europeo di indagine penale, in Cass. pen. 2015, 3288, 9.

Bonnici J.P.M., Tudorica M., Cannataci J.A., La regolamentazione delle prove elettroniche nei processi penali, in Informatica e diritto, 2015,1-2, 201-215.

Borruso R., Buonomo G., Corasaniti G., D'Aietti G., Profili penali dell' informatica, 1994.

Cajani F., Il vaglio dibattimentale della digital evidence, in Archivio penale settembre–dicembre 2013, 3, 837–852.

Cajani F., Le procedure di emergenza (artt. 9-10), in Diritto penale e processo. Speciale cybercrime, 8/2022,1055-1060.

Camaldo L., Cerqua F., La direttiva sull'ordine europeo di indagine penale. le nuove prospettive per la libera circolazione delle prove, in Cass. pen., 10/2014, 3511b.

Colaiacovo G., Nuove prospettive in tema di coordinamento delle indagini e cooperazione giudiziaria alla luce della disciplina delle squadre investigative comuni, in Diritto penale contemporaneo, 1/2017,169 ss.

Colaiacovo G., Squadre investigative comuni e investigazioni congiunte: una prima lettura, in Diritto penale e processo. Speciale cybercrime, 9/2022, 1147-1150.

Corona F., Il cybercrime: soggetto, oggetto e condotta, in Reati informatici e investigazioni digitali, Corona F. (a cura di), 2021, 19.

Cuomo L., Razzante L., la nuova disciplina dei reati informatici, 2009.

Curtotti D., L'uso dei collegamenti audiovisivi nel processo penale tra necessità di efficienza del processo e rispetto dei principi garantistici, in Rivista Italiana Diritto e Procedura penale, 1999, 492.

Curtotti D., Speciale sul secondo protocollo addizionale alla convenzione di budapest. premessa, in Diritto penale e processo. Speciale cybercrime, 8/2022,1017-1019.

D'Agostini D., Diritto penale dell'informatica, dai computer crimes alla digital forensic, 2007.

Da Valle, Legge 18 marzo 2008 (criminalità informatica), art. 9, in legislazione penale, 2008, 298;

Dalia G., I reati informatici, in aa.vv. Manuale di diritto dell'informatica, 2016, 657-689.

Dalia G., Riconoscimento, valore ed esecuzione delle sentenze penali straniere, 2020.

Daniele M., L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul D.lgs. n. 108 del 2017, in Diritto Penale Contemporaneo, 7-8/2017, 208.

Daniele M., La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge, in Processo penale e giustizia, 5/2018, 831-839.

F. Cajani, "The song remains the same" riflessione sul tempo che passa e sulla necessità di "macchine utili" per un'effettiva tutela delle vittime di reati, in Cajani F., Cernuto G., Costabile G., D'Arcangelo F., Le nuove frontiere dell'acquisizione degli elementi di prova nel cyberspace, 2017.

Flor R., Le indagini ad alto contenuto tecnologico fra esigenze di accertamento e repressione dei reati e tutela penale di tradizionali e nuovi beni giuridici nell'era digitale, in dalla data retention alle indagini ad alto contenuto tecnologico, (a cura di) Flor R., Marcolini S., 2022, 143-145.

Ghirardini A., Faggioli G., Computer forensics, 2013.

Gonzato E., Squadre investigative comuni: l'Italia finalmente recepisce la Decisione Quadro 2002/465/gai, in eurojus, 2016.

Graziani, F., L'acquisizione della prova digitale all'estero: verso un secondo protocollo addizionale alla Convenzione di Budapest sul cybercrime, in A.a. V.v., Lo spazio cyber e cosmico Risorse dual use per il sistema Italia in Europa, (a cura di) S. Marchisio – U. Montuoro, Torino, 2019.

La Regina K., Le indagini su dispositivi digitali, in Investigazioni digitali, Iaselli M., 2020, 28.72.

Lucchetti M., L'acquisizione di informazioni sulla registrazione di nomi di dominio nelle investigazioni in materia di cybercrime (art. 6), in diritto penale e processo. speciale cybercrime, 8/2022, 1041-1044.

Luparia L., Ziccardi G., Investigazione penale e tecnologia informatica, 2007.

Luparia S., Ziccardi G., Le "migliori pratiche" nelle investigazioni informatiche: brevi considerazioni sull'esperienza italiana, in Cajani F., Costabile G. (a cura di), Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea, forlì, 2011, 211 e ss.

Macrillò A., Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici, in Dir. internet, 2008.

Marafioti L., Digital evidence e processo penale, in Cass. pen., 2011, 4509-4523.

Monici S., Emanate le norme di attuazione della convenzione di assistenza giudiziaria in materia penale del 29 maggio 2000: quali margini operativi in vista dell'(imminente) trasposizione della direttiva sull'ordine europeo di indagine penale, in eurojus, 2017.

Murro O., La disciplina della videoconferenza per le dichiarazioni del testimone e dell'esperto, in Diritto penale e processo. Speciale cybercrime, 9/2022,1143-1146.

Nocerino W., La cooperazione internazionale rinforzata per lo scambio di dati degli abbonati e di traffico (art. 8), in Diritto penale e processo. Speciale cybercrime, 8/2022,1050-1054.

Pezzuto R., Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della commissione europea al vaglio del consiglio dell'unione, in Diritto Penale Contemporaneo, 1/19, 57.

Pirozzoli C., Acquisizione del subscriber data: dalla Convenzione di Budapest al Protocollo Addizionale (art. 7) in Diritto penale e processo. Speciale cybercrime, 8/2022,1045-1049.

Resta F., Cybercrime e cooperazione internazionale nell'ultima legge della legislatura, in Corriere del merito, 2008.

Ruotolo G.M., Il secondo protocollo alla Convenzione cybercrime sulle prove elettroniche tra diritto internazionale e relazioni esterne dell'unione europea, in Diritto penale e processo. Speciale cybercrime, 8/2022,1022-1027.

Ruotolo G.M., Scritti di diritto internazionale ed europeo dei dati, 2021, 229 ss.

Russo N., 20° Anniversario della Convenzione di Budapest, in Diritto penale e processo. Speciale cybercrime, 8/2022,1021.

Selvaggi E., Un ammodernamento diventato necessario per tutti gli stati Ue, in Guida dir., 2017, 25, 45 ss.

Spiezia F., Cooperazione internazionale e tutela delle vittime nel cyberspazio, in Diritto penale e processo. Speciale cybercrime, 9/2022, 1137-1142.

Suffia G., Geografia delle cyberwars. Uomini e Stati alla prova dello spazio digitale, 2018.

Svantesson D., Preliminary report: law enforcement cross-border access to data, 2016, in ssrn.com/abstract=2874238

Todaro G., Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite, in Diritto penale contemporaneo, 11/2017, 157 ss.

Viganò F., Il diritto giurisprudenziale nella prospettiva della corte costituzionale, in Sistema penale, 2021.

Wettstein F., Multinational corporations and global justice: human rights obligations of a quasi-governmental institution, 2009.

Ziccardi G., Informatica giuridica, 2006.