LNG La Nuova Giuridica

FIRENZE UNIVERSITY PRESS

# IL FATTORE TEMPORALE NELL'ACQUISIZIONE TRANSFRONTALIERA DELLE *E-EVIDENCE*: IL BILANCIAMENTO OPERATO NEL SECONDO PROTOCOLLO ADDIZIONALE ALLA CONVENZIONE DI BUDAPEST

Martina Conversano*

*Il contributo esamina il ruolo cruciale del fattore temporale nella cooperazione internazionale per l'acquisizione transfrontaliera delle e-evidence, focalizzandosi sull'evoluzione dei meccanismi di voluntary disclosure tra autorità pubbliche e service providers. Questo nuovo paradigma, sviluppatosi per superare la lentezza dei tradizionali meccanismi di mutua assistenza giudiziaria, ha trovato un precedente riconoscimento nella Convenzione di Budapest ed è stato recentemente implementato nel Secondo Protocollo Addizionale. L'analisi verte sugli articoli 6, 7 e 8 del nuovo Protocollo aperto alla firma nel maggio 2022, esaminando come questi meccanismi bilancino efficienza temporale e tutela dei diritti, limitando l'acquisizione diretta a e-evidence non particolarmente invasive della sfera privata, come nomi di dominio e informazioni sugli abbonati. Lo studio affronta questa evoluzione come avanzamento significativo nella cooperazione internazionale, delineandone limiti e prospettive.*

*This paper examines the crucial role of time in international cooperation for the cross-border acquisition of e-evidence, focusing on the development of voluntary disclosure mechanisms between authorities and service providers. This new paradigm was developed to overcome the slowness of traditional Mutual Legal Assistance mechanisms. First, It was recognized in the Budapest Convention and has recently been implemented in the Second Additional Protocol. The analysis focuses on Articles 6, 7 and 8 of the new Protocol, which was opened for signature in May 2022, and examines how these mechanisms balance temporal efficiency and the protection of rights by limiting direct acquisition to e-evidence, that is not particularly invasive of privacy, such as domain names and subscriber information. This study addresses the said development as a significant advancement in international cooperation and outlines its limitations and perspectives.*



* Dottoranda in Diritto e Innovazione presso l'Università di Macerata.

1. *Introduzione: il contesto giuridico e il fattore temporale nella cooperazione internazionale per l'acquisizione transfrontaliera delle e-evidence.* — L'era digitale ha introdotto una nuova dimensione temporale nelle dinamiche giuridiche, rendendo il tempo un elemento ancor più cruciale nelle indagini e nei procedimenti penali. Caratterizzata dalla rapidità delle connessioni e delle comunicazioni, questa nuova era ha profondamente trasformato non solo le dinamiche criminali, ma anche le attività statali collegate alla repressione penale. Pensare al Cyberspazio o alla diffusione delle c.d. *Information and Communication Technologies* (ICT) evoca l'idea di un'eliminazione delle barriere territoriali in campo tecnologico, in quanto è possibile oggi connettersi in tempo reale con persone in ogni parte del mondo, archiviare da remoto *file* tramite dispositivi fisici e lasciare "ovunque" tracce delle proprie attività *online*[1]. Tuttavia, l'a-territorialità del mondo digitale si scontra inevitabilmente con la realtà giuridica e territoriale degli Stati. L'utilizzo quotidiano di dispositivi collegati a Internet con accesso a servizi di diversa natura come *cloud*, messaggistica e molto altro, forniti da società con sedi e infrastrutture (*server*) per la memorizzazione di dati informatici dislocate in varie giurisdizioni, comporta, infatti, la necessità per le autorità di rapportarsi sempre più frequentemente con altri territori statali[2]. Da questi scenari interconnessi discende la possibilità di rinvenire all'estero tracce relative a qualsiasi tipologia di reato, attesa la sempre più frequente delocalizzazione delle prove elettroniche (c.d. *e-evidence*); da intendersi con quest'ultimo concetto «qualsiasi dato memorizzato o trasmesso usando un dispositivo o la rete Internet che supporta o respinge una teoria su come è avvenuto un fatto offensivo o individua elementi critici dell'offesa»[3]. Quello delineato rappresenta un contesto che importa la conseguenza per gli Stati di dover esercitare la propria giurisdizione oltre frontiera, e in particolare la giurisdizione investigativa (la c.d. *investigative jurisdiction*), quale

[1] Tali tracce includono, ad esempio, dati personali, registrazioni di indirizzi IP associate alle connessioni effettuate, *log* di accesso a siti *web* e servizi *online*, informazioni di geolocalizzazione e molto altro.

[2] Per approfondimenti F. Spiezia, *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: il ruolo di Eurojust*, in *Sistema Penale*, 2023, pp. 1-41.

[3] P. Palmieri, *L'acquisizione delle prove elettroniche, la voluntary disclosure dei providers, e l'ordine europeo di produzione e conservazione dell'e-evidence in materia penale*, in *Filodiritto*, 2021, II, n. 2, pp. 129-145.

possibile sottocategoria dell'*enforcement jurisdiction*[4]. Tuttavia, l'esercizio della giurisdizione esecutiva storicamente rappresenta un potere strettamente territoriale dello Stato e un esercizio oltre i confini geografici in assenza di una regola permissiva di natura consuetudinaria o pattizia configura una violazione del principio di sovranità territoriale[5]. Per comprendere le sfide giurisdizionali nell'ambito digitale è possibile considerare tre diversi scenari: è chiaro figurarsi la violazione del principio di territorialità nel caso in cui le autorità di uno Stato si rechino fisicamente in un altro Paese per l'acquisizione di elementi utili alle indagini; ma qualcosa di diverso sembrerebbe essere l'accesso da remoto ai dati digitali, e ancor più complessa sembra la valutazione di una possibile violazione nel caso in cui vi sia la condivisione di informazioni digitali da parte di entità private nei confronti di autorità estere. Si tratta di sfide significative per le autorità, che prima della digitalizzazione si trovavano nella maggior parte dei casi a ricercare le fonti di prova nella stessa giurisdizione in cui il reato era commesso[6]. Questi scenari importano, pertanto, la necessità di dover bilanciare l'urgenza di acquisire prove elettroniche - ontologicamente fragili e volatili in relazione alla loro capacità di transitare repentinamente da un luogo all'altro[7] - con l'obbligo di rispettare i confini giurisdizionali e le norme generali di diritto internazionale. Di conseguenza, i meccanismi di cooperazione internazionale hanno assunto un ruolo cruciale nei procedimenti penali e, parimenti, ha assunto notevole rilevanza anche il fattore temporale. Eppure, come rilevato già nel 2014 dal *Cybercrime Convention Committee* (T-CY)[8], i meccanismi di mutua assistenza giudiziaria sono considerati inefficienti, soprattutto con riferimento all'ottenimento delle *e-evidence*, considerando che richieste di cooperazione giudiziaria possono richiedere tempistiche dai sei a ventiquattro mesi. «Un problema che influisce

[4] Non vi è, all'attualità, condivisione in dottrina rispetto a questa ripartizione. In favore di questa distinzione, abbracciata in questo contributo, si vedano R.J. Currie, *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier?"*, in *Canadian Yearbook of International Law*, 2017, pp. 10-11; D. Svantesson, *Preliminary Report: Law Enforcement Cross-Border Access to Data*, SSRN, 2016, pp 1-17, reperibile in *https://ssrn.com/abstract=2874238*, ultima consultazione 9.10.2024; D. Svantesson, F. Gerry, *Access to extraterritorial evidence: The Microsoft cloud case and beyond*, in *Computer Law & Security Review*, 2015, XXXI, pp. 478-489. Uno degli argomenti a favore dell'autonomia della *jurisdiction to investigate* vede il riferimento alla circostanza per cui uno Stato potrebbe voler indagare su una determinata questione senza poi necessariamente esercitare la *jurisdiction to enforce*.

[5] Corte Permanente di Giustizia Internazionale, *S.S. Lotus* (Francia c. Turchia), 7 settembre 1927.

[6] A.K. Woods, *Mutual Legal Assistance in the Digital Age*, in *The Cambridge Handbook of Surveillance Law*, a cura di D. Gray, S. E. Henderson, Cambridge, 2017, pp. 660 ss.

[7] G. Soana, *L'accesso transfrontaliero alla prova informatica. Oltre il principio di territorialità*, in *Rivista semestrale di diritto*, 2020, II, pp. 254-271.

[8] Il *Cybercrime Convention Committee* (T-CY) rappresenta gli Stati Parte della Convenzione di Budapest sulla criminalità informatica e, con riferimento a quanto previsto dall'articolo 46 della Convenzione, le consultazioni di questo organismo mirano a facilitare l'uso efficace e l'attuazione della Convenzione, mediante lo scambio di informazioni e la valutazione di eventuali futuri emendamenti.

negativamente sull'obbligo dei governi di proteggere la società e gli individui contro la criminalità informatica e altri reati che coinvolgono le *e-evidence*»[9].

2. *L'evoluzione dei meccanismi di cooperazione: dalla mutua assistenza giudiziaria alla voluntary disclosure.* – Per soddisfare l'esigenza di acquisire all'estero elementi probatori utili alle indagini e ai processi penali, nel rispetto dei principi e delle regole di diritto internazionale, gli Stati sovente stipulano accordi bilaterali e multilaterali: i Trattati di mutua assistenza giudiziaria (*Mutual Legal Assistance Treaties* – MLAT). A livello multilaterale, benché su scala regionale, il Consiglio d'Europa si è da sempre adoperato nella negoziazione di specifiche clausole di cooperazione in convenzioni destinate alla repressione di determinate condotte criminose (c.d. *Suppression Convention*[10]), oltre che ad elaborare specifici accordi internazionali destinati a favorire la cooperazione internazionale in queste materie. Uno storico esempio è rappresentato dalla Convenzione europea sulla Mutua Assistenza Giudiziaria in materia penale del 1959[11]. Si tratta di un accordo multilaterale che ha delineato anche l'istituto della rogatoria internazionale, ancora oggi utilizzato in situazioni in cui tra Paesi non esistono accordi più specifici o moderni. Nonostante la sua diffusa applicazione a livello globale, la rogatoria ha mostrato negli anni punti di debolezza, specialmente in seguito all'avvento delle tecnologie digitali e, al pari degli altri meccanismi di cooperazione giudiziaria più tradizionali, si è rivelato un sistema troppo lento e complesso per l'acquisizione delle *e-evidence*[12]. Posto che in sistemi più integrati come l'Unione Europea sono stati sviluppati nel tempo strumenti più rapidi e flessibili come, ad esempio, l'Ordine Europeo di Indagine (OEI)[13], deve comunque essere considerato che quando si tratta di fornitori di servizi ci si rapporta molto spesso con territori *extra*-europei, sicché si è iniziata ad avvertire la necessità di nuovi istituti internazionali in materia. In risposta a queste limitazioni si è resa necessaria l'elaborazione di una nuova Convenzione e nel 1996, sempre a livello del Consiglio d'Europa, sono iniziati i lavori per concludere un nuovo accordo multilaterale: una Convenzione sulla criminalità informatica. Questo strumento, conosciuto come Convenzione di Budapest del 2001, è entrato in vigore nel 2004 per far fronte a una duplice necessità: istituire una nuova *Suppression Convention* riguardante il fenomeno transnazionale della criminalità informatica; e

[9] Cybercrime Convention Committee, *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, adottato alla 12a Plenaria (2-3 dicembre 2014), p. 123. Si veda in particolare la conclusione 1.

[10] C. Ponti, *Crimini transnazionali e diritto internazionale*, Milano, 2010, pp. 14-22.

[11] Council Of Europe, European Convention on Mutual Assistance in Criminal Matters, ETS No.030,20/04/1959, reperibile in *https://www.coe.int/en/web/conventions/-/council-of-europe-european-convention-on-mutual-assistance-in-criminal-matters-ets-no-030-translations*, data ultima consultazione 1.10.2024.

[12] N. Allahrakha *Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations*, in *International Journal of Law and Policy*, 2024, II, n. 6, pp. 1-9.

[13] C. Ponti, *Riforma dell'assistenza giudiziaria penale e tutela dei diritti fondamentali nell'ordinamento italiano. Dalla legge n.149 del 2016 al recepimento della direttiva 2014/41/UE*, in *La legislazione penale*, 2017, pp. 1-36.

regolamentare nuovi istituti di cooperazione internazionale per la raccolta di *e-evidence* relative a qualsiasi tipo di reato. Nel corso degli anni, oltre a questo strumento, ed anche sulla scia di alcune disposizioni in esso contenute e che verranno trattate nel prossimo paragrafo, si è, inoltre, iniziata a diffondere e rafforzare un'inedita prassi che vede la cooperazione diretta transfrontaliera tra le autorità statali e alcuni soggetti terzi: i fornitori di servizi[14]. Una pratica che assicura un maggiore celerità in fase investigativa, soprattutto in considerazione del ruolo in prima linea nel settore tecnologico assunto da questi nuovi soggetti. I fornitori di servizi sono, infatti, identificati come «qualsiasi entità pubblica o privata che fornisce agli utenti del suo servizio la capacità di comunicare per mezzo di un sistema informatico e qualsiasi altra entità che elabora o memorizza dati informatici per conto di tale servizio di comunicazione o degli utenti di tale servizio»[15]. Si tratta, dunque, di entità stabilite in diversi Stati che, in ragione dei servizi che offrono, si trovano inevitabilmente nella disponibilità di grandi quantità di dati digitali associati agli utenti. La cooperazione diretta si è iniziata a diffondere in via informale, sulla base di politiche interne delle stesse società (c.d. *voluntary disclosure*). Pertanto, è rimessa ai fornitori di servizi la valutazione dell'opportunità di collaborare o meno con le autorità estere che presentino loro delle richieste di divulgazione di *e-evidence*[16]. Quello illustrato è divenuto, tuttavia, uno scenario che ha dato origine inevitabilmente a una situazione di incertezza e confusione giuridica[17], aprendo anche la strada a possibili conflitti tra giurisdizioni, oltre che a situazioni di particolare vulnerabilità per la tutela dei diritti degli individui coinvolti.

3. *I meccanismi di cooperazione previsti nella Convenzione di Budapest sulla criminalità informatica del 2001.* – La Convenzione di Budapest già menzionata rappresenta dunque il primo e il più rilevante strumento internazionale multilaterale ad aver regolamentato nuovi istituti *ad hoc* per questi ambiti. Aperto anche all'adesione di Stati non Membri del Consiglio d'Europa, questo accordo internazionale ha ottenuto un ampio consenso, con ratifica anche da parte del Canada, Giappone, e alcuni Paesi del sud-America, oltre che degli USA; con partecipazione attiva di questi Paesi agli sviluppi del sistema ivi delineato[18].

---

[14] M. Daniele, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Revista Brasileira de Direito Processual Penal*, 2019, V, n. 3, pp. 1277-1296, *https://www.redalyc.org/articulo.oa?id=673971417005*, data ultima consultazione 1.10.2024.

[15] Definizione offerta dall'art. 1, par. 1, lett. c) della Convenzione di Budapest sulla criminalità informatica, Consiglio d'Europa, 23 novembre 2001, reperibile in *https://rm.coe.int/168008156*1, data ultima consultazione 2.10.2024.

[16] S. Signorato, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 160, nota 84.

[17] Soana, *L'accesso transfrontaliero*, cit., p. 255.

[18] Si veda in merito all'impatto globale della Convenzione di Budapest, Cybercrime Convention Committee (T-CY), *The Budapest Convention on Cybercrime: benefits and impact in practice*, 2020, reperibile in *https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/1680*9ef6ac, data ultima consultazione 6.10.2024.

Focalizzandosi ora sui meccanismi previsti, occorre preliminarmente rilevare che, per quanto concerne le misure di cooperazione internazionale per le *e-evidence*, la Convenzione di Budapest ha introdotto principalmente meccanismi di mutua assistenza giudiziaria da attuare nel rapporto tra pubbliche autorità di diversi Stati: dalla conservazione rapida di dati informatici archiviati, all'assistenza reciproca riguardante l'accesso ai dati informatici archiviati per assicurare la rapida acquisizione etc. Tuttavia, delle vere e proprie eccezioni al paradigma classico della cooperazione internazionale sono rinvenibili nell'art. 32 della Convenzione, rubricato «*Trans-border access to stored computer data with consent or where publicly available*», all'interno del quale è possibile rilevare due differenti contenuti. Da un lato la lettera a), in cui viene riconosciuto il libero accesso ai dati informatici pubblicamente disponibili in rete, senza dover presentare alcuna richiesta ad autorità estere[19]; atteso che, trattandosi di una fonte aperta e accessibile a tutti, il regime giuridico applicato a questi dati risulta differente rispetto alle tradizionali regole di giurisdizione e prescinde alla loro conservazione o effettiva ubicazione geografica nel sistema delle ICT. Dall'altro, la lettera b), in cui viene prevista la possibilità di non richiedere alcuna autorizzazione statale per l'acquisizione transfrontaliera di *e-evidence* nel caso in cui vi sia il «consenso legittimo e volontario della persona che ha l'autorità legale di divulgare i dati a quella Parte», potendo intendere con questo concetto anche il consenso legale e volontario di chi gestisce i servizi cui i dati si ricollegano[20]. Viene quindi inserito per la prima volta in una Convenzione relativa alla cooperazione internazionale un meccanismo che ammette l'esercizio unilaterale transfrontaliero del potere investigativo[21]. Una previsione innovativa, in quanto anche volta ad offrire una prima (seppur molto generica) base giuridica per la più rapida pratica della cooperazione diretta transfrontaliera: benché i dati si trovino fisicamente nell'altrui territorio non vi è alcuna richiesta di cooperazione nei confronti delle autorità estere. Tra le diverse criticità sollevate rispetto all'applicazione in

[19] Cybercrime Convention Committee (T-CY), *Guidance Note #3 Transborder access to data (Article 32)*, 2014, p. 4, reperibile in *https://rm.coe.int/16802e726a,* data ultima consultazione 1.10.2024. Nel documento è esplicitamente indicato che «i funzionari delle forze dell'ordine possono accedere a qualsiasi dato a cui il pubblico può accedere, e a questo scopo possono abbonarsi o registrarsi per servizi disponibili al pubblico».

[20] Si veda l'*Explanatory Report* della Convenzione di Budapest del Consiglio d'Europa, 23 novembre 2001, par. 294, reperibile in *https://rm.coe.int/16800cce5b*, data ultima consultazione 11.10.2024. Sul punto viene specificato che «Chi sia una persona "legalmente autorizzata" a divulgare dati può variare a seconda delle circostanze, della natura della persona e della legge applicabile in questione. Per esempio, l'e-mail di una persona può essere archiviata in un altro paese da un fornitore di servizi o una persona può intenzionalmente archiviare dati in un altro paese. Queste persone possono recuperare i dati e, a condizione che abbiano l'autorità legale, possono volontariamente divulgare i dati alle autorità di polizia o permettere a tali funzionari di accedere ai dati, come previsto nell'Articolo».

[21] Il titolo di legittimazione all'esercizio extra-frontaliero della giurisdizione sarebbe in tal caso rappresentato in via preventiva in occasione della ratifica della Convenzione, come rilevato da G.M. Ruotolo, *Il ruolo del consenso del sovrano territoriale nel transborder data access tra obblighi internazionali e norme interne di adattamento*, in *La comunità internazionale*, 2016, LXXI, n. 2, pp. 183-201.

concreto di tale previsione, oltre alla questione del regime giuridico sul consenso che dovesse applicarsi al soggetto legittimato a divulgare i dati[22], vi è anche la carenza di una specifica forma per la presentazione delle richieste. Difatti, sebbene interessante, questo tentativo di regolamentazione presenta lacune e disomogeneità, potendo essere soggetto a interpretazioni differenti in contesti giuridici diversi. Lo stesso *Explanatory Report* della Convenzione ammetteva l'impossibilità di prevedere un regime completo e giuridicamente vincolante in quest'area in ragione della mancanza, al tempo, di esperienze concrete in materia[23]. Sempre con riferimento ai primi istituti in materia di cooperazione diretta con i fornitori di servizi, appare fondamentale ricordare il meccanismo inserito nell'art. 18 della Convenzione, relativo agli ordini di produzione. Tale istituto, inserito tra le misure volte a regolamentare l'esercizio dei poteri procedurali nazionali delle Parti, consente alle autorità competenti, rispettivamente, di poter ordinare a una persona nel loro territorio di fornire specifici dati informatici archiviati, ovvero, a un fornitore che offre i suoi servizi nel territorio della Parte di presentare le informazioni sugli abbonati (*subscriber information*). A differenza del meccanismo di cui all'art. 32(b) già trattato, infatti, l'articolo 18 fa espresso riferimento a un'ipotesi di richiesta diretta ai fornitori di servizi, motivo per cui si è discusso a lungo della possibilità del suo utilizzo quale base giuridica per la pratica transfrontaliera. Benché sia previsto un collegamento territoriale, questo non è relativo alla sede del fornitore o all'ubicazione dei *server* e delle *e-evidence* che conserva, ma alla prestazione di servizi in un determinato territorio. Va inoltre sottolineato che il meccanismo di cui all'art. 18 è relativo esclusivamente alle informazioni sugli abbonati, descritte nei documenti ufficiali del Consiglio d'Europa come «il dato più spesso ricercato nelle indagini penali»[24]. È poi il paragrafo 3 dell'articolo 18 a definire le informazioni sugli abbonati, includendo sostanzialmente qualsiasi dato posseduto dal fornitore di servizi

[22] Cybercrime Convention Committee (T-CY), *Guidance Note #3 Transborder access to data (Article 32)*, adottata alla 12a Plenaria del T-CY (2-3 dicembre 2014), reperibile in https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680 2e726a, ultima consultazione 2.10.2024. Nel documento, dopo aver riconosciuto che l'articolo 32(b) rappresenta un'eccezione al principio di territorialità permettendo l'accesso transfrontaliero unilaterale senza la necessità di assistenza giudiziaria reciproca (seppur relativamente a circostanze limitate), viene affrontata la questione del consenso. Con riferimento ai fornitori di servizi viene indicato che: «è improbabile che i fornitori di servizi possano acconsentire validamente e volontariamente alla divulgazione dei dati dei loro utenti ai sensi dell'Articolo 32. Normalmente, i fornitori di servizi saranno solo detentori di tali dati; non controlleranno né possederanno i dati, e quindi non saranno in grado di acconsentire validamente». Sostanzialmente, la Guidance Note del 2014 offre una visione diversa rispetto a quella espressa nell'*Explanatory Report,* citato nella nota 21. e cerca di circoscrivere la portata dell'articolo 32(b) affermando che è "improbabile" che i fornitori di servizi possano dare un consenso valido; sfumando ancor più i contorni della materia e ciò sicuramente in considerazione delle preoccupazioni sollevate in quegli anni riguardo a questa pratica.

[23] *Explanatory Report* della Convenzione di Budapest del Consiglio d'Europa, 23 novembre 2001, par. 293, reperibile in *https://rm.coe.int/16800cce5b,* data ultima consultazione 11.10.2024.

[24] Cybercrime Convention Committee (T-CY), *Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention),* 1 marzo 2017, p. 3, reperibile in https://rm.coe.int/16806f943e , data ultima consultazione 11.10.2024.

rispetto ai propri utenti, con esclusione espressa dei dati sul traffico e dei dati di contenuto. Qualche coordinata più puntuale è offerta con la successiva specificazione per cui esse possono includere i dati del servizio, i dati personali dell'abbonato come identità, indirizzi, contatti e informazioni di pagamento ed anche le informazioni sull'installazione dell'apparecchiatura, se previste dal contratto. Come emerge da quanto illustrato, anche in questo caso la formulazione è risultata ambigua e poco definita, aprendo la strada a numerose perplessità relativamente ai contorni giuridici di questo istituto e al ruolo dei fornitori di servizi, i quali sono risultati essere sempre più coinvolti nelle indagini relative alle *e-evidence*, trovandosi a dover bilanciare il rispetto delle norme nazionali sulla protezione dei dati con l'importanza e l'urgenza degli ordini di produzione di dati provenienti dall'estero[25]. Nonostante l'innovatività sottesa alle disposizioni trattate, la loro effettiva applicazione ha creato incertezze, al punto che nel 2016 diversi Paesi europei si sono mostrati preoccupati per la spinta verso la cooperazione diretta con i fornitori di servizi come di norma, piuttosto che utilizzare i canali dell'assistenza legale reciproca[26]. Ed è proprio nella consapevolezza dei necessari adattamenti alla materia che gli stessi sottoscrittori della Convenzione avevano rimandato ulteriori discussioni in ordine a meccanismi simili, in un momento in cui vi sarebbe stata più esperienza sul tema dell'accesso unilaterale.

4. *Gli articoli 6, 7 e 8 del Secondo Protocollo Addizionale sulla cooperazione rafforzata e la divulgazione delle prove elettroniche.* – Seppur nel mese di agosto 2024 sia stato raggiunto un accordo a livello delle Nazioni Unite nel corso dell'ultima sessione di negoziazioni dell'*ad hoc committee* per l'adozione del testo della Convenzione sulla criminalità informatica, il Consiglio d'Europa e la regolamentazione contenuta nella Convenzione di Budapest continuano a rivestire un ruolo cruciale a livello internazionale da oltre vent'anni. Il *Cybercrime Convention Committee* (T-CY), in qualità di organismo di rappresentanti degli Stati che hanno ratificato la Convenzione di Budapest, ha continuato a discutere in ordine alle nuove politiche dell'uso della tecnologia e a prospettare possibili emendamenti dell'accordo multilaterale, sia per quanto concerne il tema della cybercriminalità che la cooperazione per le *e-evidence*. A tal proposito vengono in rilievo le negoziazioni per il Secondo Protocollo Addizionale, volte a raggiungere una regolamentazione comune proprio sul tema della cooperazione internazionale per le *e-evidence*, assicurando strumenti sempre più moderni e rapidi. Tale Protocollo, nonostante i ritardi nelle negoziazioni a causa anche della pandemia da COVID-19, è stato aperto alla sottoscrizione degli Stati nel maggio 2022 ed è

[25] P. De Hert, C. Parlar, J. Sajfert, *The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted Via Soft Law*, in *Computer Law and Security Review*, 2018, 34/2, p. 334.
[26] Nel corso dei lavori e le consultazioni per l'adozione della *Guidance Note* citata nella nota 25.

attualmente in attesa di entrare in vigore a seguito delle prime 5 ratifiche[27]. Il testo si presenta articolato in diverse sezioni, distinguendo tra misure di cooperazione da attuare tra soggetti differenti. Esso include, infatti, una sezione relativa alla cooperazione diretta con entità private, e anche una sezione relativa alle forme di cooperazione internazionale rafforzata tra autorità per la divulgazione di dati memorizzati. Specificatamente, sono gli articoli 6 e 7 ad offrire le nuove basi giuridiche per la cooperazione diretta transfrontaliera tra pubbliche autorità e *service providers* all'estero (purché chiaramente sempre in Stati che ratificheranno il Protocollo). L'articolo 6 persegue questo scopo introducendo un meccanismo di cooperazione diretta transfrontaliera per le richieste di informazioni sui nomi di dominio (*domain name*), da presentare ai fornitori di servizi che si trovino nel territorio di un'altra Parte. In tal senso, al fine di accelerare le procedure, il Protocollo richiede che ogni Parte adotti misure per consentire alle entità nel suo territorio di divulgare tali informazioni in risposta a tali richieste, che tuttavia, non sono vincolanti (*voluntary discolsure*). Tutt'al più, in caso di mancata collaborazione è previsto che lo Stato possa richiederne le motivazioni al fornitore di servizi, consultando eventualmente anche la Parte in cui ha sede per valutare le misure disponibili al fine di ottenere le informazioni. In modo simile, l'art. 7 prevede una procedura di cooperazione diretta transfrontaliera con i fornitori di servizi per l'ottenimento di informazioni sugli abbonati (*subscriber information*). Si ricorderà che è l'articolo 18 della Convenzione di Budapest a definire la portata del concetto di informazioni sugli abbonati, oltre che a prevedere già un meccanismo di richiesta per l'ottenimento diretto di queste *e-evidence*. Tuttavia, il nuovo articolo 7 supera la portata dell'Articolo 18 della Convenzione di Budapest, eliminando del tutto il collegamento territoriale tra lo Stato richiedente e il fornitore[28] ed anche prevedendo una serie di requisiti per le richieste al fine di garantire una maggiore tutela dei soggetti interessati. Eppure, l'aspetto di maggiore rilievo nella nuova previsione, che differenzia in modo significativo il meccanismo di cui all'art. 7 sia dall'art. 18 della Convenzione di Budapest, che dal nuovo articolo 6 per le richieste di nomi di dominio, è relativo al fatto che le richieste di divulgazione di prove elettroniche in questo caso prevedono anche specifici meccanismi di *enforcement;* sicché la collaborazione non è più solo

[27] Risultando finora sottoscritto da 47 Stati, tra Paesi Membri e non Membri del Consiglio d'Europa e ratificato da Serbia e Giappone. Consiglio d'Europa, *Chart of signatures and ratifications of Treaty 224,* reperibile in https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224, data ultima consultazione 2.10.2024.

[28] Si ricordi che l'articolo 18, paragrafo 1, lett. b) della Convenzione di Budapest indica «*a service provider offering its services in the territory of the Party*», sicché il collegamento viene individuato nella fornitura del servizio e pertanto, anche con questa formulazione le richieste potevano essere transfrontaliere.

rimessa alla volontà dei fornitori di servizi (*voluntary disclosure*)[29]. *S*e il fornitore di servizi non ottempera alla richiesta di divulgazione presentata in via diretta nei suoi confronti, è possibile per lo Stato richiedente ricorrere al meccanismo di cooperazione tra pubbliche autorità di cui all'art. 8 del Protocollo Aggiuntivo o ad altre forme di assistenza reciproca[30]. Tale istituto di cooperazione internazionale tra pubbliche autorità, come si rileva dalla rubrica dell'articolo, è infatti preposto a «g*iving effect to orders from another Party for expedited production of subscriber information and traffic data*»[31] stabilendo una procedura di accelerata per rendere vincolanti le richieste dirette precedentemente presentate. La cooperazione diretta transfrontaliera con i fornitori di servizi, pertanto, non risulta più una mera pratica basata sulla libera collaborazione rimessa in capo all'azienda, essendo adesso possibile l'attuazione di un meccanismo successivo per l'ottemperamento della richiesta estera nello Stato in cui il fornitore si trova. In tal senso, nei limiti delineati dall'istituto (quindi con riferimento alle *subscriber information* e i *traffic data*) le entità che operano servizi digitali non potranno limitarsi a dichiarare di non voler divulgare le prove elettroniche o non rispondere alle richieste di divulgazione presentate nei loro confronti entro i termini previsti, accelerando ulteriormente le tempistiche in questi ambiti. Il funzionamento di questi meccanismi, oltre che di interesse ai fini della valutazione della maggiore celerità che assicurano, appare di rilievo anche per riflettere in generale sul loro impatto rispetto al contesto giuridico internazionale delineato in apertura. L'esercizio transfrontaliero dell'attività investigativa risulta oggi sicuramente reso più flessibile grazie a questi nuovi strumenti e alle pratiche di cooperazione diretta diffusosi ma, come dimostra il meccanismo di cui all'art. 8, l'esercizio effettivo della giurisdizione esecutiva resiste a queste aperture e non può essere esercitato extra-territorialmente[32].

---

[29] G. Dalia, *La Natura Transnazionale della Digital Evidence tra Richieste di Cooperazione e Pretese di Sovranità,* in *i-lex - Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, 2023, XVI n.1, pp. 37-48; C. Pirozzoli, *Acquisizione del subscriber data: dalla Convenzione di Budapest al Protocollo addizionale (art. 7),* in *Diritto penale e processo, Speciale Cybercrime*, 2022, VIII, pp. 1045-1049.

[30] Occorre rilevare, infatti, che il Protocollo non elimina né limita alcuna cooperazione tra le Parti o tra le Parti ed entità private che sia altrimenti disponibile – sia attraverso accordi applicabili, intese, leggi nazionali o anche pratiche informali.

[31] È importante ora rilevare anche la differenza di trattamento dei *traffic data* tra la Convenzione di Budapest e il Secondo Protocollo Addizionale. La Convenzione, nell'articolo 20, prevedeva la raccolta in tempo reale di *traffic data*, anche mediante richiesta ai fornitori di servizi, ma limitatamente all'ambito nazionale, senza contemplare espressamente un meccanismo per la richiesta transfrontaliera diretta di questi dati. Il Secondo Protocollo Addizionale, con l'articolo 8, introduce invece una procedura per dare effetto agli ordini tra le Parti per la produzione accelerata di *traffic data* in un contesto transnazionale. Tuttavia, a differenza di quanto previsto per le *subscriber information* (art. 7), il Protocollo non introduce un meccanismo di richiesta diretta transfrontaliera ai fornitori di servizi per i *traffic data*. Questa distinzione nel trattamento delle diverse tipologie di dati solleva interrogativi sulle ragioni di tale approccio differenziato e sulle sue possibili implicazioni pratiche. Sarà dunque fondamentale valutare attentamente lo sviluppo e l'applicazione di questi meccanismi nella prassi, considerando le apparenti incongruità.

[32] Se nel 2016 veniva definita come interessante la distinzione tra *investigative jurisdiction* ed *enforcement jurisdicion,* ma risultavano carenti elementi nella prassi rispetto a questa distinzione,

4.1. *Il bilanciamento tra efficienza temporale e tutela dei diritti.* – A prescindere dai possibili sviluppi che deriveranno nella prassi grazie all'entrata in vigore del Protocollo Addizionale, nuovi meccanismi di cooperazione internazionale più completi e con contorni più chiari risultavano ormai necessari. L'esigenza di celerità che si è discussa all'inizio del contributo è, infatti, esponenzialmente aumentata nel tempo, in considerazione del volume sempre più frequente delle richieste di *e-evidence* di rilievo per indagini e procedimenti penali[33]. Sulla scia di queste considerazioni, dopo aver trattato in via generale degli istituti inseriti nel Protocollo, e aver sottolineato la maggiore celerità che assicurano nel contesto dell'acquisizione transfrontaliera, occorre ora trattare del bilanciamento sotteso a queste novità. Sebbene la collaborazione diretta assicuri una maggiore rapidità, essa solleva il problema della privatizzazione della tutela dei diritti[34] a causa delle minori garanzie rispetto ai classici meccanismi di cooperazione tra parti pubbliche. Il Protocollo affronta questa tematica operando un doppio bilanciamento: da un lato prevede l'implementazione di questi meccanismi più snelli e diretti solo per alcuni tipi di prove elettroniche considerate meno invasive (si vedrà, infatti, che non sono inclusi i c.d. dati di contenuto); e dall'altro, indica le specifiche modalità di richiesta, cercando di mantenere un equilibrio tra efficienza investigativa e protezione dei diritti fondamentali. Partendo dalla possibilità di richiedere direttamente ai fornitori di servizi i nomi di dominio, deve essere considerato che con questo concetto si intendono i dati relativi al soggetto che ha effettuato la registrazione di un determinato dominio (quale informazione in ordine alfabetico, come esempio.com, associata a una serie di dati che permettono di risalire al responsabile del servizio, sito o contenuto associato, come il nome del registrante, e-mail etc.). Si tratta di informazioni che fino a qualche tempo fa erano addirittura pubblicamente accessibili attraverso sistemi come il WHOIS, che ha subito profonde trasformazioni per essere adattato alla crescente tutela della sfera privata; sicché oggi la registrazione e la gestione dei nomi di dominio sono regolate da un sistema gerarchico internazionale, supervisionato dall'ICANN (*Internet Corporation for Assigned Names and Numbers*). Quelle associate ai nomi di dominio sono informazioni che possono rivelarsi cruciali per le indagini relative ad attività illecite online, e la loro divulgazione può permettere l'identificazione di potenziali indirizzi sospetti o connessioni tra attività online illecite. Oltre al fatto che è stata circoscritta la portata di questo meccanismo di cooperazione a queste informazioni, l'ulteriore

---

come rilevato da RUOTOLO, *Il ruolo del consenso del sovrano territoriale*, cit., p. 186, questa differenza di approcci delineata rafforza una distinzione crescente tra i criteri e le logiche della giurisdizione investigativa rispetto a quella esecutiva.

[33] Come rilevato da SPIEZIA, *Minaccia cibernetica, cit.*, p. 16 la richiesta di «*e-evidence* è rilevante in circa 85% del totale delle indagini penali; inoltre, in quasi il 65% delle indagini dove viene in rilievo l'esigenza di acquisire una prova elettronica, occorre una richiesta ad un *service provider across borders* (basato in altra giurisdizione). Combinando le due percentuali risulta che il 55% di tutte le indagini include una richiesta per *cross-border access e-evidence*».

[34] DANIELE, *L'acquisizione delle prove digitali*, cit., p. 1288.

bilanciamento tra esigenza investigativa e tutela dei diritti individuali è rinvenibile nel procedimento di richiesta delineato nell'articolo 6. Invero, ogni domanda di acquisizione deve includere: i dettagli identificativi dell'autorità richiedente; le specifiche precise sul nome di dominio e sulle informazioni richieste; una dichiarazione che attesti la necessità e la pertinenza delle informazioni per una specifica indagine penale; le istruzioni procedurali. Un approccio volto ad assicurare che le richieste siano mirate e proporzionate, evitando indagini a largo spettro, garantendo altresì la possibilità di un controllo procedurale. Un bilanciamento simile sembra essere stato operato anche con riferimento alle richieste dirette di cooperazione transfrontaliera per l'acquisizione delle informazioni sui sottoscrittori di un servizio (*subscriber information).* Seppur, come detto in occasione del riferimento all'articolo 18 della Convenzione di Budapest, si tratti di una categoria più ampia rispetto ai nomi di dominio - anche perché riferita generalmente a qualsiasi tipo di servizio - nei documenti ufficiali del Consiglio d'Europa viene affermato che anche in questo caso «non si tratti di dati particolarmente incisivi sulla vita privata degli interessati, poiché nulla dicono circa abitudini o altre scelte personali». Pertanto, anche per queste richieste viene bilanciata l'esigenza di celerità investigativa con una base giuridica sovranazionale che prevede l'indicazione puntuale dei contenuti delle richieste. In realtà, l'oggettivazione dei requisiti delle richieste non offre solo maggiori garanzie in favore dei soggetti interessati, ma offre anche una tutela nei confronti dei *service providers* esteri, che si troveranno a divulgare i dati in questione in forza di meccanismi più strutturati. L'ulteriore bilanciamento operato è relativo all'inserimento della misura di cui all'art. 8, che permette, come visto, di instaurare un sistema progressivo di cooperazione, sfruttando inizialmente la rapidità del paradigma della cooperazione diretta transfrontaliera, ed eventualmente di instaurare la cooperazione tra pubbliche autorità, cercando di accelerare anche quest'ultima. In tal senso, a livello internazionale si fa riferimento a un *paradigm shift* in questo settore[35], in cui non viene rinnegata la cooperazione pubblica, ma a cui si affianca e, anzi, si cerca di anticipare una cooperazione in ambito penale tra attori pubblici e privati. Una tendenza recentemente confermata anche nel sistema dell'Unione Europea con la previsione di analoghi istituti[36]. Proprio con la consapevolezza di questa ormai consolidata tendenza, dei continui bilanciamenti risultano necessari, al fine di attuare nuove cornici legali nel rispetto dei diritti e degli avanzamenti tecnologici. Da ultimo, appare di interesse sottolineare che il Protocollo tenta di offrire nel suo

[35] S. Tosza, *Internet service providers as law enforcers and adjudicators. A public role of private actors*, in *Computer Law & Security Review*, 2021, XLIII, pp. 1-9.

[36] A. Sachoulidou, *Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation*, in *New Journal of European Criminal Law*, 2024, pp. 1-19. Per approfondimenti in relazione all'Unione Europea si veda O. Marandici, Ş. Milicenco, C. Iordan, A. Oganesean, *Transnational gathering of electronic evidences: challenges and perspectives in the European Union*, in *Revista Institutului Național al Justiției*, 2022, III (62), p. 54.

complesso un'impostazione di bilanciamento tra esigenze di repressione e tutela dei diritti, facendo anche esplicito riferimento ai dati personali. Sul punto, gli articoli 13 e 14, rispettivamente rubricati "*Conditions and safeguards*" e "*Protection of Personal Data*" prevedono non solo che le Parti della Convenzione assicurino tutte le tutele riconosciute dal proprio diritto interno, i diritti umani e le libertà fondamentali (quali valori fondanti del Consiglio d'Europa) ma è, altresì, enucleata una serie specifica di tutele da attuare in ordine alla protezione dei dati personali. Invero, l'art. 14, riflette in larga misura i principi del GDPR dell'Unione Europea[37], e ciò è anche dovuto al ruolo attivo di questa organizzazione sovranazionale alle negoziazioni per il Secondo Protocollo Addizionale[38]. Questa impostazione di garanzie e tutele generale assume particolare rilievo oggi, atteso l'impegno di questa organizzazione nel corso dei lavori per un'analoga convenzione a livello delle Nazioni Unite, che ha portato a insistere per l'inserimento nel nuovo testo di diverse garanzie per i diritti umani (aspetto sul quale vi era un forte disaccordo) e al raggiungimento di una sostanziale riproduzione della Convenzione di Budapest in relazione a molti aspetti.

5. *Limiti e prospettive della nuova disciplina.* – Nonostante gli sforzi compiuti dagli Stati nelle negoziazioni per l'approvazione del Secondo Protocollo Addizionale in argomento, vengono in rilievo alcune criticità e limitazioni, che mettono in luce la complessità del tema, oltre che la necessità di continui sviluppi in questo campo. Il sistema delineato dal Consiglio d'Europa introduce meccanismi nuovi e specifici senza, tuttavia, affrontare in modo complessivo e armonizzato il concetto di prova elettronica[39]. Le uniche (e frammentarie) definizioni sono quelle di: *computer data*, *traffic data* e *subscriber information.* Invero, la definizione di *computer data*, contenuta nell'art. 1(b) della Convenzione di Budapest, è particolarmente ampia e costituisce piuttosto la base su cui si fondano le altre categorie di dati considerate: i *traffic data* definiti nell'art. 1(d) e le *subscriber information* che, come più volte ricordato, sono indicate nell'art. 18 paragrafo 3. Tuttavia, oltre a queste indicazioni talvolta è anche apparso nei documenti e nei testi ufficiali dei lavori del Consiglio d'Europa il concetto di *content data;* individuato come una delle tre categorie di dati che rileva in casi di

[37] Per un'analisi dettagliata della relazione tra l'art. 14 del Secondo Protocollo e i principi del GDPR, nonché per una discussione critica sulle possibili implicazioni per la protezione dei dati personali nell'UE, si veda M. BUCCARELLA, *Il Secondo Protocollo addizionale alla Convenzione di Budapest e le nuove frontiere della cooperazione internazionale in ambito digitale. Quali rischi per la protezione dei dati personali nell'Unione europea?*, in *Quaderni AISDUE*, 2023, pp. 184-203.

[38] Si ricordi che l'Unione Europea è riconosciuta come Membro Osservatore della Convenzione di Budapest e per questo prende parte alle attività del *Convention Committee*. Inoltre, gli Stati Membri sono anche Stati Parte della Convenzione. Per tali motivi la Commissione europea inviava nel febbraio 2019 una raccomandazione al Consiglio richiedendo un mandato per negoziare in favore dell'Unione le disposizioni del nuovo Protocollo in seno al T-CY. Nella raccomandazione in argomento veniva addotta la motivazione della particolare comunanza di interessi tra l'UE e il CoE, oltre che la parziale sovrapposizione del nuovo Secondo Protocollo Aggiuntivo alla Convenzione di Budapest con gli sviluppi della materia all'interno dell'UE. Si veda COM(2019) 71 final, p. 5-6.

[39] ALLAHRAKHA, *Addressing Barriers to Cross-Border Collection of E-Evidence*, cit., p. 5.

investigazioni digitali assieme alle *subscriber information* e i *traffic data*. Di dato di contenuto, però, la Convenzione di Budapest non offre specifiche definizioni se non indirettamente quando nell'articolo 18 par. 3 indica che le informazioni sui sottoscrittori di un servizio sono qualcosa di diverso rispetto ai dati sul traffico (*traffic data*) e ai dati di contenuto (*content data*); ed anche quando nell'articolo 21 intende come dati di contenuto quegli elementi ottenuti dalle conversazioni e comunicazioni intercettate. I dati di contenuto di rilievo nelle indagini penali oggi risultano essere non solo quelle informazioni legate al contenuto delle intercettazioni, rientrando potenzialmente in questa categoria anche tutto ciò che può essere archiviato digitalmente come testi, video, immagini o suoni. Si tratta chiaramente di una parte massiccia del problema legato al mondo digitale interconnesso in quanto anche questi possono essere conservati da remoto. Il nuovo Protocollo Addizionale tace rispetto a questi dati e non introduce nuove misure di cooperazione neppure tra pubbliche autorità, e ciò è sicuramente dovuto alla maggiore invasività che li caratterizza, atteso che, rispetto ai dati finora menzionati e trattati, questi contengono il contenuto effettivo della comunicazione piuttosto che i soli metadati o le informazioni sull'utente. Quello che appare di interesse, tuttavia, è che un approccio maggiormente integrato in tal senso è stato adottato nella *Draft United Nations Convention against Cybercrime,* approvata dall'*ad hoc committee* l'8 agosto 2024. Invero, nell'art. 2 relativo alle definizioni vengono esplicitati i concetti di dati sul traffico, informazioni sul sottoscrittore, dati di contenuto, ed altre ancora; sicché il nuovo strumento ONU sulla cybercriminalità rappresenta un interessante tentativo di sistematizzare le definizioni. Tuttavia, anche in questo caso è risultato necessario mantenere una certa flessibilità nelle sue formulazioni, ad esempio, aggiungendo elenchi esplicativi affiancati da frasi come «include ma non si limita a», lasciando spazio a interpretazioni più ampie. Un'apertura che, da un lato offre la flessibilità necessaria per adattarsi a future sfide tecnologiche ma, dall'altro potrebbe portare a nuove questioni interpretative e applicative tra Stati. Restano, dunque, da valutare gli sviluppi che si verificheranno nella materia o i limiti che si porranno nella prassi rispetto a questi strumenti. Sicuramente, il Consiglio d'Europa con la sua lunga tradizione in materia di repressione della minaccia *cyber* e di cooperazione per le *e-evidence,* continua ad offrire un contesto unico per l'armonizzazione delle norme in questi settori e il nuovo Protocollo Addizionale rafforza la volontà di continuare a progredire mantenendo un equilibrio tra efficacia investigativa e tutela dei diritti individuali.

6. *Conclusioni.* – L'analisi condotta in questo contributo ha evidenziato il ruolo cruciale del fattore temporale nell'evoluzione del quadro normativo relativo all'acquisizione transfrontaliera delle *e-evidence*, con particolare attenzione al diritto penale e internazionale. Questi settori, tradizionalmente caratterizzati da una lenta evoluzione, si trovano oggi a dover affrontare la necessità di un adattamento rapido e continuo, imposto dalla velocità con cui le tecnologie

digitali si sviluppano e dalla natura immediata e globale delle minacce informatiche. Il Secondo Protocollo Addizionale alla Convenzione di Budapest rappresenta un tentativo significativo di bilanciare l'urgenza dell'acquisizione delle prove elettroniche con la tutela dei diritti fondamentali. Tuttavia, come emerso dall'analisi, l'accelerazione delle procedure, da sola, non è sufficiente a risolvere le complesse problematiche legate all'acquisizione transfrontaliera, poiché le dinamiche cambiano costantemente e coinvolgono nuovi attori, richiedendo nuovi bilanciamenti dei valori e dei principi in gioco. Il fattore temporale impone quindi un ripensamento degli strumenti investigativi tradizionali. Ogni volta che il mondo digitale fa un nuovo passo avanti, cambiano le dinamiche della società[40] e con essi necessariamente anche il diritto. La sfida per il futuro sarà, pertanto, non solo di sviluppare quadri normativi sufficientemente flessibili da adattarsi rapidamente ai cambiamenti tecnologici, ma anche promuovere competenze interdisciplinari che integrino aspetti giuridici e tecnici, al fine di rispondere efficacemente alla velocità dei nuovi scenari. In definitiva, solo attraverso un equilibrio dinamico tra innovazione giuridica e competenze adeguate sarà possibile affrontare con successo le sfide della criminalità nell'era digitale nel rispetto della tutela dei diritti.

[40] B. Jerman Blazicniele, T. Klobučar, *Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society*, in *Information & Communications Technology Law*, 2020, XXIX, pp. 66-81.