UNIVERSITÀ
DEGLI STUDI
FIRENZE

Università degli Studi di Firenze
Dipartimento di Ingegneria dell'Informazione (DINFO)
Corso di Dottorato in Ingegneria dell'Informazione
Curriculum: Telecomunicazioni e Sistemi Telematici

Profili giuridici e tecnici dello scambio transnazionale delle prove digitali in ambito penale

Candidata
Sara Conti

Tutors
Dr. Ginevra Peruginelli
Dr. Tommaso Agnoloni
Dr. Tommaso Pecorella

Coordinatore del Corso
Prof. Fabio Schoen

ciclo XXXII, 2016-2019

Università degli Studi di Firenze, Dipartimento di Ingegneria
dell'Informazione (DINFO).

A Bianca

Ringraziamenti

Un sentito ringraziamento ai miei tutors, Ginevra Peruginelli, Tommaso Agnoloni e Tommaso Pecorella, che mi hanno seguita e consigliata in questo percorso di ricerca.

A tutta la mia famiglia e ad Andrea, per esserci sempre. Con il loro incondizionato sostegno mi hanno spronato nei momenti di difficoltà e stanchezza.

Alla mia piccola Bianca che con l'entusiasmo e la gioia con cui ha guardato il mondo in questi suoi primi nove anni di vita, mi ha dato la forza e lo stimolo di arrivare fino a qui.

Grazie a Sebastiano Faro e ai miei colleghi dell'IGSG che mi hanno incoraggiata e supportata in questi anni. A Maria Angela Biasiotti e Fabrizio Turchi, per la loro eccezionale disponibilità e per tutte le opportunità che mi hanno dato nel condurre la mia ricerca per la tesi di dottorato. A Giuseppina Sabato e Simona Binazzi, per il loro preziosissimo ed impagabile aiuto.

Infine, un grazie di cuore alle amiche che mi hanno sopportata.

Indice

Capitolo 1

Introduzione e scopo della ricerca

Il Capitolo, dopo una breve introduzione sul rapporto tra processo penale transnazionale (in cui lo scambio di prove digitali può risultare determinante per la definizione del caso) e nuove tecnologie informatiche, individua la prospettiva abbracciata nel presente lavoro. In particolare, la prima parte del Capitolo pone l'attenzione sull'analisi condotta nei vari Stati membri circa le modalità di raccolta, uso e scambio delle prove digitali attraverso l'EIO – European Investigation Order, ovvero l'Ordine europeo di indagine. L'ultima parte del Capitolo è infine dedicata allo strumento utilizzato per condurre tale analisi: ovvero un questionario fatto circolare tra circa 250 soggetti appartenenti a specifici "target groups" coinvolti nelle procedure di EIO[1].

1.1 Introduzione alla ricerca: il complesso rapporto tra processo penale transnazionale e nuove tecnologie informatiche

Il tema della presente ricerca muove dall'ormai inarrestabile espansione delle tecnologie informatiche nei processi penali.

[1]Parte del paragrafo 1.1. del presente Capitolo relativa al rapporto tra processo penale transnazionale e nuove tecnologie è stata pubblicata in M.A. Biasiotti, S. Conti, F. Turchi, *La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno standard*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), "Cybercrime", Utet giuridica, 2018, pp. 1639-1640.

Nel corso di una normale giornata, semplici attività come effettuare una telefonata, inviare un messaggio su whatsapp, accedere a un social network, persino spostarsi in auto, generano una serie di tracce digitali.

Queste ultime, potenzialmente, possono rappresentare delle prove in un processo penale per dimostrare l'innocenza o la colpevolezza di uno o più soggetti coinvolti in un reato. Tuttavia, l'introduzione, tra gli strumenti conoscitivi del giudice, degli elementi probatori di carattere digitale si caratterizza per essere estremamente problematica sotto molteplici punti di vista.

Innanzitutto, l'aumento dell'uso della tecnologia e delle comunicazioni on line ha prodotto un aumento dell'incidenza della criminalità informatica, e ha portato alla nascita di alcune nuove tipologie di fattispecie criminali. Tuttavia, l'assunto per cui per i reati informatici i riscontri siano da ricercare nelle tracce digitali, mentre per i reati comuni gli elementi probatori siano da rinvenire fra le potenziali prove tradizionali, ormai non è più valido. Le investigazioni nei casi di reati comuni si affidano sempre più sulla ricerca di elementi di prova digitali. Le prove digitali non sono più soltanto quelle prove che possono essere utilizzate nel processo penale a carico o discarico di un c.d. reato cyber, ma anche di un reato comune.

Oggi, potrebbe risultare molto difficile pensare che un crimine non abbia una dimensione per così dire "digitale".

La crescente importanza della prova digitale acquista ancora più peso in considerazione del fatto che il crimine è ormai diventato globale. Lo stesso principio della territorialità dell'azione penale si scontra con la reale portata e la dimensione sempre più transfrontaliera del crimine.

Al fine di perseguire e prevenire efficacemente i reati, le autorità di polizia e giudiziarie devono quindi adattarsi al rapido sviluppo delle tecnologie, lavorando con prove digitali da esse generate e utilizzando altre tecnologie digitali (i.e. tools forensi) per acquisirle e analizzarle. Durante la fase investigativa, tali autorità utilizzano mezzi di ricerca della prova tradizionali, ma dovrebbero anche essere dotati di strumenti investigativi specifici legati alla particolare natura delle prove digitali da ricercare.

A questo scopo è fondamentale che una prova ottenuta in un determinato paese sia ammissibile e utilizzabile in un processo anche incardinato in altro Stato membro, naturalmente purché sia garantito il rispetto dei diritti fondamentali della persona. La mancanza di una legislazione comune e di standard di livello nazionale e internazionale rende questo obiettivo particolarmente difficile da raggiungere.

Le autorità di polizia e quelle giudiziarie si trovano a operare in un quadro normativo incerto: non esiste un quadro giuridico omogeneo fra i vari Stati membri dell'Unione europea, riguardante la raccolta, l'uso e lo scambio di prove digitali. Di volta in volta, si manifesta la necessità di adottare soluzioni che possono anche risultare incoerenti o confuse, sia dal punto di vista giuridico, sia dal punto di vista delle soluzioni tecnologiche.

Merita, inoltre, particolare attenzione il fatto che la tipologia di prova con cui le autorità investigative hanno a che fare è particolare, in quanto è nata e riconosciuta fuori dai contesti normativi. In altre parole, tali tipi di prove prescindono da un riconoscimento formale in una specifica disposizione di legge, in quanto, come spesso avviene quando si tratta del binomio nuove tecnologie e regole, queste ultime seguono il fenomeno tecnologico per "sanare le lacune", e quasi mai sono in grado di anticiparlo[2].

Infine, deve essere tenuta anche in debita considerazione la veloce evoluzione delle tecnologie forensi: le nuove tecnologie possono rapidamente perdere la loro efficacia, in termini di capacità di estrazione di elementi di prova, mano a mano che le organizzazioni criminali diventano consapevoli della loro esistenza e adottano contromisure per renderle tecnicamente inutili o poco efficaci. Anche l'assenza di standard o buone regole per proteggere le tecniche forensi dall'esposizione pubblica delle loro caratteristiche, durante i processi, rende tali misure rapidamente obsolete e poco efficaci. Questo vale soprattutto per le organizzazioni criminali internazionali, che hanno a disposizione risorse economiche praticamente illimitate.

In questo contesto, l'obiettivo di realizzare un quadro normativo europeo organico in materia di scambio della prova digitale ha origine dall'esigenza di rafforzare la cooperazione giudiziaria in materia penale e fa riferimento principalmente alle disposizioni in materia di Mutual Legal Assistance (MLA)[3],

[2] M.A. Biasiotti, *Presente e futuro dello scambio della prova digitale in Europa*, in "Informatica e diritto", 2015, n. 1-2, pp. 35-63.

[3] Council of Europe, *Convention on Mutual Assistance in Criminal Matters*, Strasburgo, 20 aprile 1959, Articolo 1(1). Si veda anche: Id., *Convention on Mutual Assistance in Criminal Matters between the EU countries*, 2000; Id., *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*, Strasburgo, 8 novembre 1990, ETS No. 141, Articolo 7(1); Id., *Convention on the Transfer of Sentenced Persons*, Strasburgo, 21 marzo 1983, ETS No. 112, Articolo 2(1); Id., *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, Strasburgo, 8 novembre 2001, CETS No. 182, Articolo 1(1); Id., *Convention on Cybercrime*, Budapest, 23 novembre 2001, ETS 185, Articolo 23.

già esistenti, e alla nuova frontiera aperta dalla direttiva relativa all'European Investigation Order (EIO)[4]. Quest'ultimo, uno strumento innovativo, congegnato proprio per essere l'unico strumento da utilizzare per l'acquisizione e la circolazione delle prove in ambito europeo relative a procedimenti penali di rilevanza transfrontaliera. Le disposizioni di attuazione della direttiva dovevano essere adottate dagli Stati membri entro il 22 maggio 2017. Come indicato sotto, ad oggi tutti gli Stati membri hanno adottato misure di recepimento, tranne l'Irlanda e la Danimarca (Figura 1.1)[5].

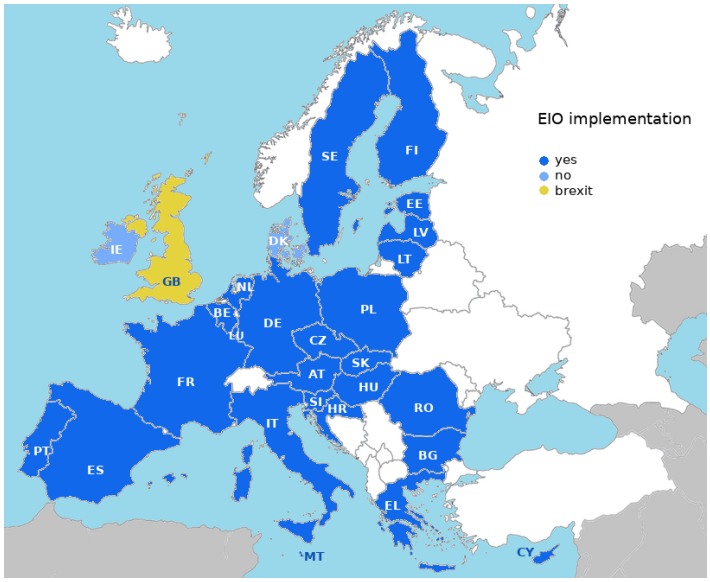

Figura 1.1: Attuazione dell'EIO negli Stati membri

L'EIO dovrebbe facilitare la cooperazione giudiziaria tra Stati membri, introducendo per la prima volta il principio della disponibilità di misure investigative, dando la possibilità all'autorità di un Paese di richiedere all'autorità di un altro Paese, che venga effettuata una vera e propria indagine, con eventuale acquisizione di elementi di prova.

[4]Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale.

[5]Si veda, per quanto riguarda l'attuazione nei vari Stati membri della direttiva sull'EIO, il seguente link: https://eur-lex.europa.eu/legal-content/IT/NIM/?uri=CELEX:32014L0041&qid=1569499604719.

Si tratta, quindi, di uno strumento processuale a disposizione dell'autorità giudiziaria per la ricerca della prova e la circolazione probatoria oltre i confini giurisdizionali di ciascuno Stato membro dell'Unione Europea.

Tuttavia, il recepimento dell'EIO negli Stati membri è un processo ancora in divenire, che presuppone l'integrazione di questo nuovo strumento nel diritto nazionale di ciascun paese. In particolare, l'EIO deve essere recepito nel diritto processuale penale di ciascuno Stato membro, che quindi dovrà essere adattato e modificato. Questo processo di adattamento, nonostante l'obiettivo dell'introduzione dell'EIO sia stato quello di incentivare la cooperazione giudiziaria tra Stati, potrebbe comportare nelle procedure nazionali dei vari paesi lievi divergenze. Divergenze che potrebbero ostacolare lo scambio di prove, anche di natura digitale, acquisite attraverso l'EIO.

La prospettiva abbracciata dalla presente ricerca muove proprio da un'analisi delle modalità di implementazione dell'EIO nei vari Stati membri.

In particolare, il lavoro di ricerca si è incentrato sull'analisi delle modalità di raccolta, uso e scambio transnazionale delle prove digitali attraverso l'EIO, secondo molteplici prospettive:

a) dal punto di vista giuridico (analisi della normativa europea in materia e analisi comparata delle modalità di attuazione dell'EIO nei diversi Stati membri);
b) dal punto di vista tecnologico (analisi comparata delle caratteristiche tecniche delle procedure per lo scambio delle prove digitali nei diversi Stati membri);
c) dal punto di vista del trattamento dei dati personali (analisi della normativa europea sulla protezione dei dati personali e suo impatto sugli strumenti di scambio transnazionale delle prove digitali).

Sono state quindi identificate una serie di criticità nel "trattamento"[6] della prova digitale, ad ognuna delle quali è stata data risposta attraverso l'elaborazione di una proposta, una "roadmap", che contenesse strategie ed azioni comuni per superare gli ostacoli individuati.

L'obiettivo, con questo lavoro, è proprio quello di individuare e di predisporre una serie di azioni comuni per le autorità giudiziarie degli Stati membri (da realizzare nel medio e lungo termine), che si qualifichino come strumento da percorrere per realizzare una sistematica e uniforme raccolta, ma anche uso e scambio transnazionale delle prove digitali nei processi penali.

[6]Inteso nel senso più ampio del termine che comprende la raccolta, uso, conservazione e scambio delle prove.

Al tempo stesso, le strategie elaborate e le azioni individuate nell'ambito di questo lavoro dovrebbero porre le basi per migliorare l'efficienza delle indagini e, in generale, dei procedimenti giudiziari penali, mantenendo le adeguate garanzie a tutela dei diritti fondamentali della persona e rispettando chiari standard operativi di condotta.

La "roadmap" che viene proposta con il presente lavoro, trae spunto dalla attività svolta e dall'esperienza maturata nell'ambito di progetti europei sul tema dello scambio transnazionale delle prove digitali, negli ultimi 4 anni di attività come ricercatrice presso il Consiglio Nazionale delle Ricerche – CNR.

In particolare, è stata fondamentale ai fini del presente lavoro la mia partecipazione nel team di ricerca del progetto europeo Evidence, e, successivamente di Evidence2e-CODEX ed EXEC[7].

L'idea alla base della mia esperienza di ricerca in materia è che sia necessario, nella realizzazione dello scambio delle prove, e in particolare di quelle digitali, passare dalla teoria alla pratica e iniziare a sperimentare quanto realizzato fino ad ora a livello di progetti europei, provando concretamente a implementare lo scambio. Occorre quindi iniziare a verificare se quello che è stato implementato e pensato fino ad ora "sulla carta" possa veramente funzionare se trasportato e implementato nella realtà concreta. Ciò attraverso la proposta di una serie di azioni comuni, attività e strategie che gli Stati membri dovranno attuare nel medio e/o lungo termine al fine di realizzare un efficiente sistema di scambio delle prove in un contesto transnazionale. A questo proposito, diventa fondamentale analizzare alla luce dell'esperienza maturata in materia, le informazioni sulle modalità nazionali di implementazione concreta dell'EIO che si pone oggi quale strumento "principe" per la circolazione probatoria fra diversi Stati membri.

1.2 Metodologia e obiettivi della ricerca: l'indagine condotta nei vari Stati membri UE in materia di scambio delle prove digitali

Il presente lavoro si è proposto di indagare su come la direttiva europea sull'EIO sia stata recepita e attuata nella legislazione nazionale degli Stati

[7]Di questi tre progetti, a cui ho partecipato e partecipo attivamente come ricercatrice, vengono date informazioni più precise ed una descrizione nel prosieguo del lavoro, così come per altre iniziative progettuali a livello europeo sul tema in oggetto. In particolare, il riferimento è nel paragrafo 2.2. del Capitolo 2 del presente lavoro.

membri dell'Unione Europea. In questo modo è stato possibile avere un quadro generale sullo stato dell'arte delle procedure relative allo scambio transnazionale delle prove digitali nei processi penali.

In generale, scopo di un'indagine è quello di raccogliere un ampio bacino di informazioni che riguardano un determinato gruppo di persone, una comunità o un gruppo specifico di soggetti campione che possono essere poi utilizzate, attraverso un processo di analisi, per formulare possibili soluzioni/azioni comuni. L'indagine può essere proposta sia in campo politico (ad esempio, per raccogliere opinioni, valutare exit pools), sia in campo sanitario (per valutare lo stato di salute della popolazione), nel sociale (per scoprire abitudini e necessità della popolazione), nelle ricerche di mercato (per scoprire i bisogni dei diversi gruppi interessati), ma anche in ambito giuridico per avere informazioni, per esempio, sulle modalità di applicazione di un istituto in un determinato ordinamento giuridico, o sulle modalità di attuazione di una determinata normativa.

Ma un'indagine può anche essere utile in prospettiva sovranazionale, per condurre un'analisi comparata sul funzionamento di ordinamenti giuridici diversi o sulle diverse modalità di implementazione e attuazione di atti dell'Unione europea a livello dei singoli Stati membri.

Questa è stata l'idea alla base del presente lavoro: raccogliere, attraverso un'indagine mirata, informazioni ottenute da determinati "target groups". Informazioni che provengono direttamente da coloro che si trovano quotidianamente ad affrontare questioni connesse all'EIO e allo scambio transnazionale delle prove digitali eventualmente ottenute attraverso questo strumento processuale. L'indagine è stata condotta, appunto, attraverso l'elaborazione di un questionario[8]. Il primo passo per la strutturazione del questionario è stato quello di condurre una ricerca approfondita su tutte le iniziative europee in materia di scambio transazionale delle prove digitali ed in materia di EIO e MLA.

Altra importante fonte di informazione sono stati le attività condotte e i risultati ottenuti nei vari progetti europei sul tema (ad esempio Evidence, Evidence2e-CODEX, EXEC) ai cui team di ricerca ho partecipato e partecipo dal 2016 ad oggi.

Queste attività di studio e analisi hanno facilitato l'identificazione di questioni e domande pertinenti da consegnare agli attori dell'indagine. Il secondo passo è stato, infatti, proprio quello di identificare le parti interessate da coinvolgere nella ricerca.

[8]La versione integrale, in lingua inglese del questionario è presentata nell'Appendice del presente lavoro. Il questionario è stato fatto circolare da giugno 2018 a gennaio 2019.

A questo proposito, sono stati individuati i seguenti attori:

- rappresentanti dei Ministeri della Giustizia degli Stati membri dell'UE e anche di alcuni Stati terzi: in questa categoria devono essere ricomprese le autorità giudiziarie dei vari paesi (giudici e pubblici ministeri), personale delle cancellerie che si occupano di EIO (compresi amministrativi e informatici);
- giudici e pubblici ministeri di vari Stati membri che hanno aderito a offerte formative organizzate a livello europeo in materia di EIO;
- avvocati: che svolgevano la propria attività nel settore penale, in particolare in processi transnazionali (membri del CCBE - Council of Bars and Law Societies of Europe[9]);
- rappresentanti di Istituzioni europee che si occupano di cooperazione transfrontaliera: EUROPOL[10], EUROJUST[11], OLAF[12], EJN[13];
- esperti di digital forensics.

[9]Si tratta del Consiglio degli Ordini Forensi d'Europa, un'associazione internazionale senza scopo di lucro che è stata, sin dalla sua creazione, in prima linea nel promuovere le opinioni degli avvocati europei. Si veda https://www.ccbe.eu.

[10]«È l'agenzia dell'Unione europea incaricata dell'applicazione della legge, il cui obiettivo principale è quello di contribuire a realizzare un'Europa più sicura a beneficio di tutti i cittadini. Fornisce assistenza ai 28 Stati membri dell'Unione europea nella loro lotta contro la grande criminalità internazionale e il terrorismo. L'agenzia collabora anche con molti Stati partner non membri dell'UE e con organizzazioni internazionali». Si veda https://www.europol.europa.eu/it/about-europol.

[11]Si tratta di un organismo istituito nel 2002 (con Decisione 2002/187/GAI del Consiglio modificata dalla Decisione 2009/426/GAI del Consiglio, del 16 dicembre 2008) per supportare e implementare il coordinamento e la cooperazione tra autorità nazionali nella lotta contro le forme gravi di criminalità transnazionale che interessano l'Unione europea. Ciascuno dei 28 Stati membri designa un proprio rappresentante presso Eurojust: tali rappresentanti possono rivestire, nel proprio paese, il ruolo di pubblici ministeri, giudici o funzionari di polizia con pari prerogative. Si veda http://www.eurojust.europa.eu/Pages/home.aspx.

[12]L'Ufficio europeo per la lotta antifrode è stato istituito dalla Commissione europea con Decisione n. 352 del 28 aprile 1999, con l'obiettivo di contrastare le frodi, la corruzione e qualsiasi attività illecita lesiva degli interessi finanziari della Comunità europea. Si veda https://ec.europa.eu/anti-fraud/home_it.

[13]L'European Judicial Network è una rete di punti di contatto nazionali per favorire la cooperazione giudiziaria in materia penale. I vari punti di contatto sono designati da ciascuno Stato membro tra le autorità centrali responsabili della cooperazione giudiziaria internazionale e le autorità giudiziarie o altre autorità competenti con responsabilità specifiche nel settore della cooperazione giudiziaria internazionale. Si veda https://www.ejn-crimjust.europa.eu/ejn/EJN_DynamicPage/IT/1.

Tutti questi soggetti sono stati coinvolti nella ricerca grazie alla rete di collegamenti creata negli ultimi 4 anni nell'ambito dei progetti europei sopra citati. L'esperienza concreta nelle iniziative progettuali sul tema mi ha permesso, infatti, di entrare in contatto con diversi "stakeholders" che a vario titolo avevano a che fare con le procedure di EIO.

Una prima versione del questionario, in lingua inglese, è circolato on line tra circa 100 soggetti appartenenti alla prima e ultima delle diverse categorie sopra elencate, e coinvolte fino ad oggi nei 3 progetti europei citati, in un numero equilibrato per ciascuno dei "target group" e per diverse aree geografiche.

Come detto, la circolazione del questionario è avvenuta on line ed ha sfruttato la piattaforma di comunicazione scelta nell'ambito dei progetti Evidende2e-CODEX ed EXEC, quale canale per le comunicazioni con i vari stakeholders/partners; inoltre, è stato fatto circolare anche tra tutti i partners/stakeholders che avevano partecipato al progetto Evidence.

Dal punto di vista geografico, possiamo dire che il questionario è circolato praticamente in tutta la zona dell'Unione: Austria, Repubblica ceca, Spagna, Croazia, Lituania e Lussemburgo, Bulgaria, Germania, Francia, Grecia, Italia, Paesi Bassi, Portogallo, Svezia, Danimarca e Belgio secondo la distribuzione che segue (Figura 1.2).

By Country

Austria	3	Greece	1
Belgium	1	Italy	2
Bulgaria	3	Lithuania	1
Croatia	3	Luxembourg	1
Czech Republic	9	Netherlands	1
Denmark	1	Portugal	1
France	1	Spain	2
Germany	1	Sweden	1

Figura 1.2: Distribuzione degli Stati membri che hanno completato il questionario

Dal punto di vista delle categorie di soggetti che hanno compilato il questionario, sono 31 i rappresentanti dei vari "target groups" di riferimento

(rappresentanti dei Ministeri di Giustizia ed esperti di digital forensics) che hanno completato tutte le risposte, su 96 soggetti che hanno avuto accesso al questionario on line ma che non hanno completato la procedura (Figura 1.3).

Report

Completed	31
Pending	65

Figura 1.3: Totale accessi al questionario

Soltanto le risposte di coloro che hanno compilato tutto il questionario sono state poi oggetto dell'analisi: tali soggetti sono rappresentati come segue (Figura 1.4).

By Position

Administrative Position	8
Judge	9
Other	4
Public Prosecutor	7
Technical Position	3

Figura 1.4: Distribuzione delle categorie di soggetti che hanno completato il questionario

In particolare, 9 giudici e 7 pubblici ministeri, 8 soggetti con ruoli amministrativi e 3 con ruoli tecnici presso le cancellerie delle Corti dei vari Stati membri, hanno completato il questionario. Inoltre anche 4 rappresentanti di categorie diverse da quelle indicate: ovvero esperti di digital forensics.

In particolare, il questionario è stato suddiviso in 5 sezioni (Figura 1.5):

A) una sezione generale che riguarda lo "status quo" dell'attuazione della direttiva EIO a livello nazionale (Sezione A);

B) una sezione giuridica che include questioni più specifiche sulla gestione pratica delle richieste di EIO da parte delle autorità nazionali (Sezione B);
C) una sezione tecnica, che comprende domande sulla gestione tecnica/informatica delle richieste da parte delle autorità nazionali e sulle operazioni e azioni collegate (Sezione C);
D) una sezione denominata amministrativa, più specificatamente dedicata alle attività di training condotte in materia (Sezione D);
E) infine una sezione sulle questioni relative alla protezione dei dati che possono venire in rilievo quando si tratta di EIO e di scambio di prove digitali (Sezione E).

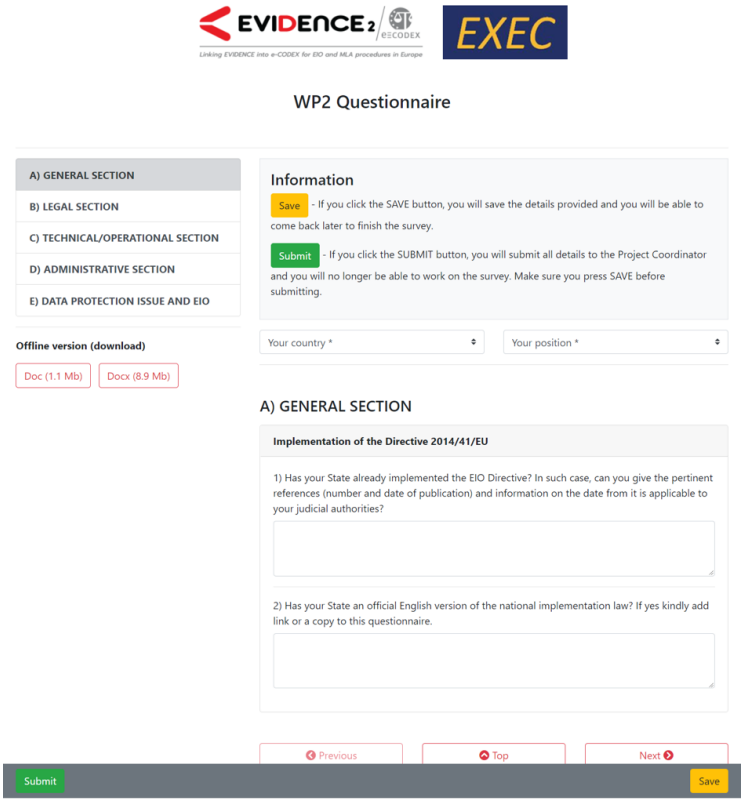

Figura 1.5: Divisione in sezioni del questionario

Per accedere al questionario, ciascun partecipante ha dovuto registrarsi con e-mail nel sistema (Figura 1.6). Una e-mail poteva essere registrata una sola volta ed è sempre stata associata a uno stesso questionario, il che significa che ogni partecipante poteva inviare un solo questionario tramite quel particolare indirizzo di posta.

Successivamente alla registrazione, il sistema predisponeva una conferma e creava un questionario associato all'e-mail registrata (Figura 1.7).

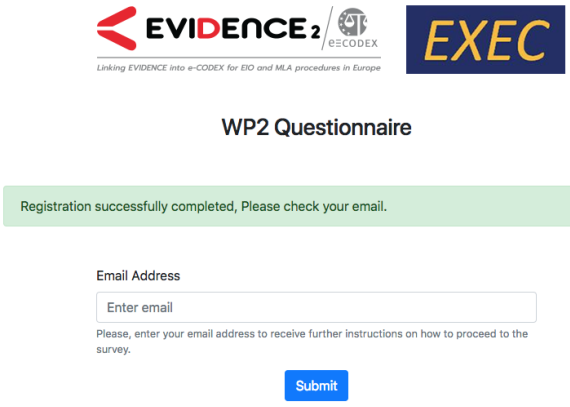

Figura 1.6: Pagina di registrazione al questionario

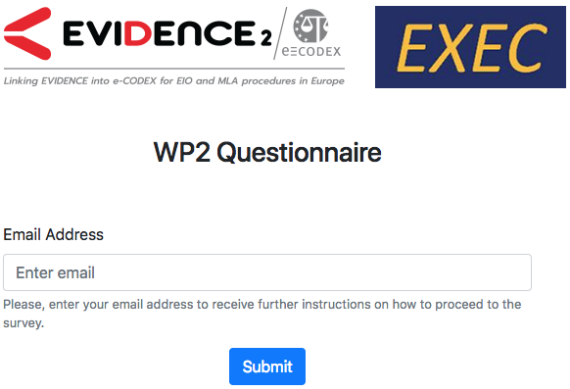

Figura 1.7: Pagina di login per la compilazione del questionario

Il questionario è stato organizzato in sezioni e queste in sottopagine corrispondenti al contenuto/argomento specifico trattato da ciascuna sezione. Le domande erano a scelta singola, a scelta multipla e anche a testo libero. In alcuni casi, e tenendo conto della particolare domanda, ciascun partecipante aveva anche la possibilità di caricare sulla piattaforma determinati documenti.

Ai fini della compilazione del questionario, l'utente poteva utilizzare i pulsanti "Precedente", "Superiore" o "Avanti" per spostarsi tra le varie sezioni o all'interno di una determinata sezione tra le sue pagine secondarie.

Ogni pagina secondaria offriva inoltre all'utente la possibilità di "Salvare" o "Inviare" il questionario. Se l'utente faceva clic sul pulsante "Salva", tutte le risposte date alle domande che erano già state fornite potevano essere registrate e salvate dal sistema.

Inoltre, l'utente era così in grado di tornare in una fase successiva per completare l'indagine (in un'altra sessione di login). Se l'utente faceva clic sul pulsante "Invia", il questionario veniva definitivamente sottomesso e non c'era più possibilità di procedere con la compilazione.

Le risposte fornite dai vari utenti che hanno completato il questionario sono state tutte analizzate nel presente lavoro. Tuttavia, particolare attenzione è stata data alle risposte dei seguenti Stati membri: Austria, Repubblica Ceca, Spagna, Croazia, Lituania, Lussemburgo.

La decisione di analizzare con maggiore profondità le informazioni provenienti dai rappresentanti dei paesi sopra elencati è strettamente connessa alla mia esperienza e attività di ricerca nei progetti europei Evidence, Evidence2e-CODEX, infine EXEC.

Infatti, le mie attività di studio si sono concentrate proprio sugli ordinamenti giuridici di tali Stati anche in un'ottica comparata con il nostro.

Quindi, l'analisi delle risposte al questionario è stata organizzata facendo precedere delle considerazioni generali su tutte le risposte date dai vari Stati membri, seguite da un'analisi più specifica delle risposte dei paesi oggetto della presente ricerca.

Inoltre, una versione ridotta del questionario (relativa alle sole parti di interesse per gli avvocati) è stata fatta circolare attraverso i canali del CCBE[14]. Mentre un'altra versione ridotta è stata utilizzata nell'ambito di un

[14]Gli organi centrali del CCBE hanno provveduto a far circolare attraverso e-mail ai propri membri la versione ridotta del questionario. Il paragrafo 5.1 del Capitolo 5 del presente lavoro è dedicato alla presentazione dei risultati del questionario compilato dagli

seminario organizzato da EJTN[15] in Firenze, con la collaborazione del Consiglio Nazionale delle Ricerche, sulle modalità di raccolta delle prove digitali[16], alla presenza di giudici e pubblici ministeri dei vari Stati membri che avevano aderito all'iniziativa formativa di EJTN (quindi diversi da giudici e pubblici ministeri espressamente incaricati dai Ministeri di Giustizia di partecipare al questionario on line).

Infine, un'ultima versione ridotta del questionario è stata utilizzata nell'ambito di un meeting tecnico organizzato dal Consiglio Nazionale delle Ricerche in collaborazione con i progetti Evidence2e-CODEX ed EXEC, alla presenza di rappresentanti delle Istituzioni europee sopra citate, che si è svolto a L'Aja, sempre sul tema delle modalità di raccolta e uso delle prove digitali in ambito transnazionale[17].

Per quanto riguarda i numeri totali dei partecipanti alla indagine, 250 sono stati i soggetti che hanno completato i 4 questionari.

Le risposte provenienti da "target groups" diversi e utilizzando modalità on line, ma anche in presenza nell'ambito dei due meeting, ha permesso di avere un'analisi completa dello "status quo" delle procedure e modalità di attuazione dell'EIO nei vari Stati membri, ricevendo feedback dal lato non solo dei rappresentanti dell'autorità giudiziaria coinvolti nelle procedure di EIO, ma anche rappresentanti dell'Ordine degli Avvocati europei che si occupano della materia, rappresentanti di Istituzioni europee che si occupano di cooperazione transfrontaliera, infine esperti di digital forensics.

Il feedback complessivo ricevuto ha quindi fornito un importante risultato in merito alle procedure EIO e MLA in atto, sottolineando allo stesso tempo le barriere e gli ostacoli esistenti per una piena attuazione di tali strumenti legali.

Questo ha permesso di individuare azioni comuni e strategie per superare puntualmente tali ostacoli e barriere al fine di garantire un'efficace e

avvocati del CCBE.

[15]European Judicial Training Network, ovvero la Rete europea di formazione giudiziaria è la principale piattaforma e promotrice della formazione e dello scambio di conoscenze della magistratura in Europa. Si occupa di organizzare formazione per giudici, pubblici ministeri in tutta Europa. Si veda http://www.ejtn.eu.

[16]Il paragrafo 5.2 del Capitolo 5 del presente lavoro è dedicato alla presentazione dei risultati del meeting/seminario di EJTN.

[17]Il paragrafo 5.3 del Capitolo 5 del presente lavoro è dedicato alla presentazione dei risultati del meeting/seminario de L'Aja.

funzionale raccolta, uso e scambio delle prove digitali nei processi penali transnazionali.

1.3 Organizzazione della tesi

Per quanto riguarda la struttura del mio lavoro, questa riflette la metodologia descritta nel paragrafo precedente.

Dopo una introduzione dell'oggetto del lavoro e la descrizione della metodologia adottata nel Capitolo 1, il successivo Capitolo 2 è dedicato all'analisi del quadro europeo in materia di scambio transnazionale delle prove digitali nei processi penali.

In particolare, viene definito che cosa si intende per "prova digitale" ai fini del presente studio e vengono spiegate e descritte non solo le iniziative e politiche europee volte al rafforzamento della cooperazione giudiziaria in materia penale ma anche la legislazione dell'Unione sul tema. Ovvero gli strumenti di Mutua assistenza giudiziaria (Mutual Legal Assistance – MLA) e l'Ordine europeo di indagine (European Investigation Order – EIO).

Il Capitolo 3 è dedicato alla presentazione e all'analisi dei risultati del questionario, con particolare riferimento ai risultati delle prime 2 sezioni (A-B) e della sezione D, ovvero le sezioni giuridico-amministrative.

Il Capitolo 4 è dedicato invece alla presentazione dei risultati della sezione tecnica (sezione C) del questionario, con particolare riferimento alla descrizione dello "status quo" dei sistemi di informazione nazionali utilizzati per lo scambio transnazionale delle prove digitali nell'ambito dei processi penali.

Il Capitolo 5, dopo la presentazione dei risultati del questionario circolato tra i membri del CCBE e nei due seminari organizzati in presenza a Firenze e L'Aja, propone le azioni e strategie comuni volte al superamento delle barriere e degli ostacoli individuati nelle procedure di scambio delle prove digitali attraverso l'EIO.

Il Capitolo 6 è incentrato sui profili di "data protection" che possono venire in rilievo nello scambio delle prove digitali. Dopo un attento esame della nuova disciplina europea in materia di trattamento dei dati personali viene analizzato l'impatto della stessa sull'implementazione dell'EIO e in generale sulle procedure di MLA.

Infine, nel Capitolo 7 sono presentate le conclusioni del lavoro ed i possibili sviluppi futuri.

Capitolo 2

Il quadro europeo in materia di scambio transnazionale delle prove digitali

Il Capitolo, dopo aver definito il significato di "prova digitale" ai fini del presente lavoro, descrive le iniziative e le politiche adottate a livello europeo per la creazione di un quadro comune in materia di cooperazione giudiziaria penale e per il rafforzamento degli strumenti esistenti in materia di scambio delle prove digitali nei processi penali transnazionali. In particolare, ampio spazio è stato dato alle iniziative progettuali sul tema: tra gli altri, ai progetti Evidence, Evidence2e-CODEX ed EXEC. Successivamente, il Capitolo si incentra sullo stato dell'arte della legislazione dell'Unione europea in materia: in particolare, sugli strumenti di Mutua assistenza legale e sull'EIO[1].

[1]La versione in inglese del paragrafo 2.1 del presente Capitolo relativo alla definizione di prova digitale è stata pubblicata in S. Avveduto, S. Conti, D. Luzi, L. Pisacane, *The conceptual representation of the Electronic Evidence*, in M.A. Biasiotti, J.P. Mifsud Bonnici, J. Cannataci, F. Turchi (eds.), "Handling and exchanging electronic evidence across Europe", Springer International Publisher, 2018. Il paragrafo 2.2 del presente Capitolo relativo alle iniziative e politiche europee per il rafforzamento della cooperazione giudiziaria penale è stato pubblicato in M.A. Biasiotti, S. Conti, F. Turchi, *La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno standard*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), "op. cit.", pp. 1648-1652. Il paragrafo 2.3 del presente Capitolo relativo alla legislazione europea in materia di cooperazione giudiziaria penale e di EIO è stato pubblicato in S. Conti,

2.1 La prova digitale ai fini del presente studio: la natura transnazionale

Conoscere la definizione e il significato di un determinato istituto giuridico, oppure degli strumenti idonei a dimostrare un fatto o una circostanza, rappresenta un punto di partenza fondamentale per qualsiasi studio o ricerca. E questo vale anche in relazione al presente lavoro, in cui risulta di vitale importanza avere una definizione chiara e precisa di cosa si intenda per prova digitale.

A questo scopo, ho mutuato la definizione elaborata nell'ambito del progetto europeo Evidence, alla cui identificazione ho partecipato attivamente: «La prova elettronica è un qualsiasi dato risultante dall'output di un dispositivo analogico e/o digitale che abbia valore probatorio e che sia stato generato da, elaborato da, memorizzato su o trasmesso da, qualsivoglia dispositivo elettronico. La prova digitale è quella prova elettronica che sia stata generata o convertita in un formato numerico»[2].

Si tratta di una definizione che riesce ad abbracciare una nozione molto ampia di prova digitale: in quanto ricomprende sia le prove nate digitali ma anche quelle che, nel loro ciclo di vita, vengono successivamente trasformate e poi memorizzate o scambiate in formato digitale[3].

Questa nozione ampia ben si presta ad essere utilizzata anche in contesti transnazionali. Infatti, è ormai evidente che la presenza della prova digitale non è correlata quasi mai alla giurisdizione territoriale di un determinato Paese dove il presunto reato è stato commesso o dove è in corso l'attività investigativa. Si assiste sempre di più alla instaurazione di processi penali che travalicano i confini nazionali, dove la necessità di acquisire prove anche di natura digitale non si limita al territorio di un determinato Stato.

La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia, in "Informatica e diritto", 2015, n. 1-2, pp. 153-164 ed in parte in M.A. Biasiotti, S. Conti, F. Turchi, op. cit., pp. 1645-1646.

[2] «Electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated by, processed by, stored on or transmitted by any electronic device. Digital evidence is that electronic evidence which is generated or converted to a numerical form», definizione elaborata nell'ambito del progetto europeo Evidence che viene descritto nel paragrafo successivo del presente Capitolo.

[3] M.A. Biasiotti, M. Epifani, F. Turchi, *Opportunità e sfide per la prova elettronica*, in "Informatica e Diritto", 2015, n. 1-2, pp. 19-29.

Sono tre gli aspetti caratteristici di questa natura transnazionale della prova digitale.

Il primo riguarda la localizzazione e conservazione della prova digitale.

Proprio per la sua natura, per il crescente utilizzo delle tecnologie e per la globalizzazione dei procedimenti penali, la prova digitale può essere memorizzata e conservata ovunque nel mondo. E ciò vale soprattutto per i reati informatici che di fatto possono "non avere confini" nazionali.

Il secondo aspetto riguarda la sede dell'Internet Service Provider - ISP (di solito una società privata).

Gli ISPs hanno accesso o possiedono informazioni digitali che possono essere potenzialmente utili come prove in un processo. Tuttavia molti di questi soggetti privati non hanno sede legale nello stesso Paese dove un determinato reato è investigato o perseguito. E quindi può risultate arduo per l'autorità di un determinato Stato estero ottenere informazioni rilevanti per un determinato processo penale.

Infine, l'ultimo aspetto riguarda proprio la natura transnazionale del presunto crimine: nel caso di certi reati, basti pensare ad esempio ai reati informatici, il crimine spesso viene commesso coinvolgendo diverse giurisdizioni, rendendo più difficile la raccolta, l'uso e la conservazione di informazioni utilizzabili come prove.

Questi sono tutti aspetti che hanno reso e rendono necessaria la creazione di un quadro comune europeo in materia di scambio delle prove digitali fra diversi Stati membri, che tenga in considerazione le peculiarità delle prove digitali e che ne disciplini in maniera adeguata la raccolta, lo scambio, l'utilizzo e la conservazione.

2.2 Stato dell'arte delle politiche e iniziative delle Istituzioni europee per il rafforzamento della cooperazione giudiziaria in materia penale

Negli ultimi anni a livello europeo sono state molte le iniziative e le politiche adottate, volte alla creazione di un quadro comune in materia di cooperazione giudiziaria penale ed al rafforzamento degli strumenti già esistenti per lo scambio transnazionale delle prove digitali nei processi penali.

Fondamentale per l'elaborazione e strutturazione dei questionari è stato proprio lo studio delle varie iniziative europee sul tema: è stato infatti possibile strutturare l'indagine tenendo conto degli orientamenti e delle politiche che si sono affermate negli ultimi anni nell'area europea.

Le Istituzioni europee, coinvolte a vario titolo e con varie competenze nel rafforzamento della cooperazione giudiziaria in materia penale, hanno concretamente iniziato a collaborare, già da alcuni anni, in gruppi di lavoro, sulle modalità che possono essere adottate per consentire lo scambio delle prove a livello europeo con l'intento di facilitare anche l'operatività e il successo dell'EIO.

Già nel lontano 2016, il Consiglio europeo, nelle conclusioni di un suo documento[4] aveva individuato tre azioni per il miglioramento della giustizia penale e della cooperazione giudiziaria in Europa, relativamente al cyberspazio:

- semplificazione delle procedure di assistenza giudiziaria reciproca e, ove applicabili, delle procedure di mutuo riconoscimento reciproco, attraverso l'utilizzo di moduli standardizzati e strumenti elettronici anch'essi standardizzati;
- miglioramento della cooperazione con i fornitori di servizi attraverso lo sviluppo e l'uso di moduli e strumenti allineati per la richiesta di specifiche categorie di dati;
- avvio di un processo di riflessione su possibili criteri di collegamento per la competenza esecutiva dell'autorità giudiziaria nel cyberspazio.

Alcune delle azioni che erano state indicate nel documento sicuramente necessitavano di un'ulteriore riflessione e di concreti interventi che sono stati alla base di un ampio dibattito a livello europeo e anche negli Stati membri.

Proprio sulla scorta di tale dibattito, il Consiglio europeo aveva chiesto alla Commissione di presentare entro il giugno 2017 risultati tangibili relativamente alle tre linee di azione.

Nel contesto sopra delineato, la Commissione europea ha dato ampio rilievo all'esigenza di realizzare un "Secure online portal" per consentire lo scambio transnazionale delle prove digitali. Questo ha rappresentato il tentativo di dare una risposta concreta alle esigenze di creare un quadro europeo comune e sicuro per lo scambio delle prove digitali in ambito penale.

[4] Consiglio europeo, *Conclusioni del Consiglio sul miglioramento della giustizia penale*, 9 giugno 2016, in https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf.

A tale scopo, la Commissione ha provveduto alla nomina di due gruppi di esperti: un "Expert group – on Reliable electronic platform MLA and EIO requests"[5] e l'"Horizontal Working Party on Cyber Issues and JHA Counsellors"[6], volti entrambi a porre le basi per la creazione di tale piattaforma sicura per lo scambio transnazionale delle prove digitali nei processi penali.

In particolare, i lavori del primo gruppo hanno mirato a definire prioritariamente la natura che una piattaforma per lo scambio delle prove digitali dovrebbe avere per poter essere considerata sicura, affidabile e di non difficile gestione da parte della Commissione e degli Stati membri. In particolare due sono state le alternative proposte, ovvero realizzazione di una piattaforma a livello:

- centralizzato, e quindi direttamente gestito dalla Commissione europea a cui tutti gli Stati membri dovrebbero connettersi e collegare i propri database nazionali; o,
- decentralizzato, in cui gli Stati dialogano direttamente senza alcun intervento di gestione delle richieste e della trasmissione da parte della Commissione europea, mantenendo localmente i database nazionali.

La Commissione, quindi, era stata chiamata a decidere, confrontandosi con gli Stati membri, sulle possibili strade da percorrere proposte dall'"Experts Group", per poter al più presto dotarsi di un sistema di trasmissione on line delle prove digitali.

È chiaro che l'opzione di una gestione/conservazione centralizzata delle prove digitali da parte dell'Unione europea richiedeva necessariamente che

[5]I lavori dell'Experts Group si sono concentrati sull'analisi dei *Principles and Options for an e-evidence exchange platform – Discussion Paper prepared by DG Justice and Consumers for the Expert Group on e-evidence.*

[6]Sebbene la Commissione abbia notevoli competenze interne, ha bisogno di una consulenza specialistica di esperti esterni come base per la definizione di solide politiche. Tali informazioni possono essere fornite da gruppi di esperti o consulenti esterni, o assumere la forma di studi. Il gruppo di esperti è un organo consultivo che può essere istituito dalla Commissione o dai suoi servizi per ottenere consulenze e conoscenze specialistiche, è composto da membri del settore pubblico e/o privato e si che si riunisce più di una volta. Riunire competenze provenienti da varie fonti può voler dire anche raccogliere i pareri delle diverse parti interessate. I gruppi di esperti della Commissione sono di due tipi: ufficiali – istituiti da una decisione della Commissione e informali – istituiti da un servizio della Commissione che ha ottenuto il consenso del commissario e vicepresidente responsabile e del Segretariato generale. I gruppi di esperti della Commissione sono soggetti alle regole orizzontali stabilite con Decisione della Commissione C(2016)3301 e che deve essere letta insieme alla comunicazione della Commissione C(2016)3300.

ci fosse già disponibile una base normativa comune relativa al trattamento centralizzato dei dati e delle prove digitali, con particolare attenzione alla regolamentazione della tutela dei dati personali, della sicurezza della trasmissione dei dati e della catena di custodia delle prove stesse. Soluzione questa che, sulla carta, era sembrata più complicata da gestire e ancora oggi vi è ampio dibattito sul tema.

Oltre alla questione della natura del sistema, a livello europeo si è discusso ampiamente anche sulle caratteristiche che il sistema avrebbe dovuto soddisfare e che sembravano prescindere dalla natura centralizzata o decentralizzata dello stesso. A questo proposito, all'esito dell'"Expert Meeting on Principles and options for an e-evidence exchange platform"[7] i vari esperti partecipanti all'"Expert group on Reliable electronic platform MLA and EIO requests" hanno posto l'attenzione su alcuni punti ritenuti di fondamentale importanza per la realizzazione di un quadro comune in materia e che riguardavano:

A) gli utilizzatori (users) del sistema/piattaforma per lo scambio;
B) i requisiti di sicurezza della piattaforma;
C) il luogo di archiviazione delle richieste e delle prove digitali;
D) le funzionalità della piattaforma: in particolare, la grandezza e la possibilità di traduzione multilingue delle richieste.

Sul fronte degli users, l'obbiettivo che si stava, e che si sta ancora perseguendo a livello europeo, è senza dubbio quello di avere un sistema costruito in modo da raggiungere una platea più ampia possibile: giudici, pubblici ministeri nonché le forze di polizia degli Stati membri e altri attori che possono venire in rilievo nel complesso procedimento dello scambio delle prove digitali (ad es. personale amministrativo e tecnico delle cancellerie delle Corti, ma anche avvocati).

Per quanto riguarda la sicurezza della piattaforma, gli orientamenti dimostrano di tendere sempre verso la realizzazione di un sistema che guarda alle esigenze di protezione sotto punti di vista diversi e in maniera globale. Non solo quindi il sistema dovrà assicurare modalità di autenticazione e autorizzazione tali da garantire l'affidabilità della richiesta e della risposta, ma dovrà al tempo stesso fornire un livello di cifratura atto a garantire la sicurezza dello scambio; infine, dovrà assicurare un livello di sicurezza sia per la richiesta sia per la trasmissione delle prove digitali.

[7] Experts Meeting on the *Setting Up of a Reliable and Secure e-platform for the European Investigation Order on Mutual Legal Assistance (MLA) (16 novembre 2009)*..

Sul terzo punto, ovvero sul luogo in cui verranno archiviate le richieste di trasmissione anche di prove digitali, la questione oggetto di discussione riguardava di nuovo la scelta di un sistema centralizzato o decentralizzato. Infatti, in base all'architettura, cambia il modo in cui i dati verranno gestiti, dato che i sistemi sono diversi da uno Stato membro all'altro rendendo difficilmente percorribile la possibilità di collegarli in maniera sistematica.

Questione questa ancora oggi molto dibattuta a livello comunitario.

Infine, sullo specifico punto riguardante il volume di grandezza delle prove da trasmettere, il dibattito ha riguardato la questione se il sistema possa consentire un invio della prova digitale basato su tecniche diverse da quelle tradizionali (corriere sicuro, posta).

Si è discusso molto, ad esempio, se la trasmissione possa essere facilitata attraverso l'invio di un link per effettuare il download dei file, oppure se la semplificazione della procedura di scambio possa essere realizzata soltanto attraverso l'invio di metadati cui segue l'invio solo di alcuni dati selezionati.

Per quanto riguarda il secondo gruppo di lavoro sopra citato, che si occupa in modo specifico dei "Cyber Issues", particolare attenzione è stata posta dai vari esperti proprio sul tema specifico dello scambio della prova digitale.

In una riunione tenutasi a Bruxelles il 20 gennaio 2017 il gruppo di esperti ha ribadito che il rafforzamento della cooperazione in materia penale rimane il fattore chiave per la lotta contro i reati informatici e il terrorismo e che questa passa necessariamente anche attraverso tre canali distinti ma strettamente collegati tra loro:

- incremento della consapevolezza degli strumenti a disposizione per la realizzazione di uno scambio sicuro delle prove digitali;
- aumento della reciproca fiducia tra Stati membri attraverso la predisposizione di procedure comuni e uniformi;
- realizzazione di sistemi che consentano lo scambio sicuro e affidabile delle informazioni e delle prove digitali tra le forze di polizia, le autorità giudiziarie e gli altri attori coinvolti nei processi penali.

Questo gruppo ha sottolineato, in modo particolare, l'importanza strategica proprio in tema di prove digitali, di creare sinergie e sviluppare la cooperazione fra i vari stakeholders coinvolti, tra i quali un ruolo prioritario viene riconosciuto agli ISPs, e di costruire, insieme a questi, seguendo un metodo condiviso, la base normativa e il dialogo necessario a generare e aumentare la tanto auspicata fiducia reciproca.

Le iniziative europee sopra descritte dimostrano che già da diversi anni il tema del rafforzamento della cooperazione giudiziaria in materia penale e, in particolare, lo sviluppo di piattaforme sicure per lo scambio transnazionale delle prove digitali nei processi penali, rappresenta un elemento fondamentale per garantire adeguati livelli di uniformità nelle procedure dei diversi Stati membri.

A livello europeo il crescente interesse per la tematica dello scambio transnazionale delle prove digitali è dimostrato anche dai numerosi progetti che sono stati finanziati direttamente dalla Commissione e che cercano di dare soluzioni concrete al dibattito sul tema. Alcuni di questi progetti si sono occupati direttamente della tematica oggetto del presente lavoro, mentre altri sono stati incentrati su tematiche connesse: ad esempio la semplificazione delle procedure che consentono lo scambio delle prove digitali (c.d. e-MLA).

Da sottolineare, in relazione ai vari progetti europei direttamente o indirettamente legati al tema dello scambio transnazionale delle prove digitali, come sia stata molto efficace la linea scelta dalla Commissione di finanziare progetti tra loro complementari e con un comune raggio d'azione il cui punto di arrivo è rappresentato dal rafforzamento della cooperazione giudiziaria e dal trattamento standardizzato delle informazioni in materia penale.

Tra questi progetti europei merita particolare attenzione Evidence (European Informatics Data Exchange framework for Courts and Evidence), finanziato dalla Commissione europea nell'ambito del 7 Programma Quadro, iniziato nel marzo 2013 e conclusosi nell'ottobre 2016. Il progetto si pone proprio in linea con le iniziative europee sopra descritte, ovvero si è posto quale obiettivo finale la creazione di un comune quadro in materia di scambio transnazionale delle prove digitali.

In particolare, obiettivo di Evidence è stato quello di identificare, definire e valutare un insieme di azioni che avrebbero dovuto essere condotte a livello dell'Unione europea e di misure nazionali per poter consentire di scambiare la prova digitale tra le autorità competenti.

L'approccio adottato dai team di ricerca del progetto è stato un approccio multidisciplinare e sempre in stretta collaborazione con i diversi "stakeholders".

Questi i punti su cui il progetto ha basato la propria azione di ricerca:

– analisi comparativa dei sistemi normativi esistenti nei vari Stati membri UE partners del progetto, relativamente agli aspetti inerenti allo scambio della prova digitale;

- identificazione e definizione delle azioni necessarie per consentire le modifiche normative da promuovere a livello nazionale al fine di facilitare lo scambio sicuro delle prove digitali;
- definizione di standard tecnico (per la rappresentazione dei dati e dei metadati) per favorire lo scambio della prova digitale fra paesi diversi, al tempo stesso preservando i requisiti di utilizzabilità e sicurezza della prova digitale, con particolare attenzione alla tutela di tutti gli aspetti legati al trattamento dei dati personali[8].

Le attività di ricerca svolte nell'ambito del progetto Evidence si sono anche incentrate sull'obiettivo di creare una rete stabile di esperti forensi e di favorire la comunicazione tra i principali attori del processo penale (ad esempio, autorità giudiziarie, forze di polizia, ecc.) in modo da stimolare un dibattito continuo e mirato, e al tempo stesso uno scambio di idee, sui principali temi di interesse oggetto del progetto. Con ciò, Evidence ha dimostrato ancora una volta di essere in linea con gli orientamenti della Commissione di utilizzare, per questa particolare tematica, gruppi di esperti che si occupano, vuoi sotto il profilo tecnico (esperti forensi), vuoi sotto il profilo più strettamente giuridico (e mi riferisco all'autorità giudiziaria) di scambio transnazionale delle prove digitali. Obiettivo finale del progetto Evidence è stato quello di fornire alla Commissione europea, una "road map" (linee guida, raccomandazioni, guide operative, standard tecnici, ecc.) per creare un quadro comune a livello europeo per l'applicazione uniforme e sistematica delle nuove tecnologie per la raccolta, il trattamento e lo scambio di prove digitali[9].

La "road map" si è basata sull'individuazione di soluzioni e azioni comuni da intraprendere che nell'intento del team di ricerca del progetto avrebbero dovuto aiutare i *policy maker* a livello europeo a facilitare l'adozione e/o l'introduzione di una normativa uniforme in materia di trattamento e scambio della prova elettronica.

Altro progetto rilevante in materia, anche se non direttamente finalizzato allo scambio delle prove digitali, è il progetto e-CODEX finanziato per realizzare un'infrastruttura realizzata per migliorare l'accesso dei cittadini e delle imprese alle procedure giudiziarie transnazionali fra diversi Stati membri dell'Unione europea.

[8] M.A. Biasiotti, *Presente e futuro dello scambio della prova digitale in Europa*, cit.
[9] *Ibidem*.

Proprio l'infrastruttura creata nell'ambito di e-CODEX potrebbe rappresentare lo strumento idoneo per lo scambio della prova digitale in Europa.

In particolare, il progetto coinvolge 25 partner: 19 Paesi europei[10]; 3 Paesi europei non-UE (Isola Jersey, Norvegia, Turchia); 2 associazioni di categoria (CCBE e CNUE[11]); infine, un organismo di normalizzazione (OASIS[12]).

Il progetto e-CODEX, per raggiungere l'obiettivo sopra descritto, ha proposto e realizzato una serie di soluzioni creando un'infrastruttura per la trasmissione e lo scambio di informazioni nel contesto di procedure giudiziarie transnazionali:

- *e-Delivery*, per la trasmissione di informazioni in modo sicuro e affidabile attraverso le frontiere;
- *e-Signature*, per la firma elettronica dei documenti e la convalida delle firme elettroniche;
- *e-Document*, per lo scambio di documenti comuni;
- *e-Identity*, per l'identificazione dei soggetti tramite carte d'identità nazionali[13].

Finora, il progetto e-Codex ha concentrato i propri sforzi di ricerca sulla realizzazione di una tale infrastruttura per la comunicazione delle informazioni relativa alla richiesta di mutua assistenza giudiziaria. Tuttavia, l'infrastruttura realizzata nell'ambito del progetto e-CODEX potrebbe offrire un'ottima base di partenza per la realizzazione di un sistema sicuro ed uniforme di scambio anche delle prove digitali raccolte ed ottenute attraverso l'EIO.

Un passo in avanti in questo obiettivo è rappresentata dal fatto che la comunità di e-CODEX sta tentando di adeguare la procedura creata con l'infrastruttura per allinearla alle esigenze sottese alla direttiva sull'EIO.

Inoltre, la Commissione europea si sta già muovendo in tale ottica, avendo finanziato recentemente il progetto Evidence2e-CODEX (Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe).

Il progetto ha la durata di 21 mesi (marzo 2018-novembre 2019) ed è stato finanziato nell'ambito della call "e-Justice" nel "Topic: JUST-JCOO-

[10]Si tratta in particolare di: Austria, Belgio, Repubblica Ceca, Estonia, Francia, Germania, Grecia, Ungheria, Italia, Irlanda, Lituania, Malta, Paesi Bassi, Polonia, Portogallo, Romania, Spagna, Svezia, Regno Unito.

[11]Si tratta del Consiglio dei Notariati dell'Unione Europea.

[12]Organizzazione per la promozione delle norme sulle informazioni strutturate.

[13]M.A. Biasiotti, *Presente e futuro dello scambio della prova digitale in Europa*, cit.

CRIM-AG-2016: Action grants to support transnational projects to promote judicial cooperation in criminal matters".

Come si può evincere già dal titolo, il progetto mira, nello specifico contesto delle procedure MLA e dell'EIO, a sviluppare un "case study" per lo scambio sicuro ed affidabile delle prove digitali in Europa mettendo insieme l'infrastruttura veloce, sicura e affidabile realizzata dal progetto e-CODEX con quanto proposto dal progetto EVIDENCE sull'adozione di un linguaggio formale di scambio[14]. Questo caso di studio dovrebbe rappresentare un "building block" verso la realizzazione di una piattaforma sicura per lo scambio transnazionale delle prove digitali.

In parallelo al progetto sopra descritto, la Commissione ha anche finanziato EXEC (Electronic Xchange of e-Evidences with e-CODEX).

Il progetto, della durata di 24 mesi (febbraio 2018-febbraio 2020), ha come obiettivo quello di consentire agli Stati membri partecipanti di scambiare gli ordini di indagine europei e relative prove digitali, completamente in formato elettronico attraverso soluzioni di back-end nazionali esistenti o in alternativa, attraverso l'implementazione di soluzioni "reference" fornite dalla Commissione europea[15]. L'infrastruttura di scambio per facilitare la consegna elettronica di EIO e prove digitali collegate dovrebbe essere quella realizzata dal progetto e-CODEX basata su e-CODEX Building Blocks.

Altro progetto che merita di essere citato, è il progetto e-MLA (2016-2019), coordinato dall'Interpol che si pone come obbiettivo quello di modernizzare e razionalizzare i processi di trasmissione delle richieste di MLA nel quadro delle procedure esistenti a livello dell'Unione europea e del Consiglio d'Europa (CoE).

L'iniziativa progettuale mira senza dubbio ad aumentare l'efficacia della cooperazione giudiziaria in materia penale. Infatti, obiettivo ultimo del progetto è proprio la realizzazione di uno strumento elettronico molto pratico che permetta alle autorità competenti di scambiare informazioni correlate a procedure di assistenza reciproca, in conformità con gli impegni dei trattati esistenti, con la legislazione nazionale e con le altre iniziative a livello europeo sul tema. Anche il progetto LIVE_FOR[16] è incentrato sulle tematiche in oggetto e merita di essere brevemente descritto.

[14]Si veda a tale proposito https://evidence2e-codex.eu.

[15]Si tratta del progetto e-Evidence della Commissione europea per la creazione di un'infrastruttura per lo scambio delle prove digitali in contesti penali transnazionali.

[16]Si veda a tale proposito http://live-for.eu/.

In particolare, gli obiettivi del progetto sono:

- identificare lo stato dell'arte dell'attuazione dell'EIO negli Stati membri dell'UE;
- individuare le principali differenze tra le legislazioni degli Stati membri che possono influenzare il ritardo nell'attuazione del meccanismo di scambio introdotto con l'EIO;
- preparare una raccolta di "best practicies" adottate e seguite nei diversi Stati membri in merito all'attuazione dell'EIO;
- sviluppare programmi di formazione e migliorare la competenza delle autorità giudiziarie competenti all'esecuzione delle richieste di EIO.

Infine, un accenno al progetto EUROCORD[17], che ha lo scopo di definire e diffondere un codice di buone pratiche al fine di adattare gli attuali sistemi giuridici dei vari Stati membri alla procedura introdotta dalla direttiva sull'EIO.

Gli obiettivi specifici del progetto sono i seguenti:

- analisi della legislazione nazionale sull'attuazione dell'EIO e degli strumenti europei volti a favorire la cooperazione giudiziaria in materia penale in Europa. Concretamente, il progetto ha condotto l'analisi in relazione ai seguenti paesi: Spagna, Italia e Polonia;
- revisione delle pratiche giudiziarie adottate negli Stati membri analizzati in materia di raccolta delle prove in procedimenti penali transnazionali, ma anche in procedimenti civili;
- attività di formazione sul tema della cooperazione giudiziaria in materia penale per sensibilizzare maggiormente tutti coloro che si occupano del tema.

Tutte le iniziative europee sopra descritte ed i progetti europei sul tema dimostrano un'attenzione veramente molto ampia sulla tematica oggetto della presente tesi.

A livello europeo, ma anche a livello dei singoli Stati membri, è sempre più pressante l'esigenza di creare un'infrastruttura comune di scambio delle prove digitali in ambito penale tra paesi diversi.

E i progetti europei sul tema hanno contribuito, e contribuiscono, a creare i "building blocks" per la creazione di tale infrastruttura sicura.

La mia partecipazione alle attività di ricerca condotte nell'ambito dei progetti europei Evidence, Evidence2e-CODEX ed EXEC è stata fondamentale per avere ben chiaro quale sia il quadro europeo in materia di scambio

[17] Si veda a tale proposito http://eurocoord.eu/about/objectives/.

transnazionale delle prove digitali nei processi penali. E questo mi ha permesso di analizzare le informazioni ottenute con i questionari, da un lato, da una prospettiva molto ampia e concreta (in quanto non mi sono basata su informazioni derivate soltanto da uno studio della dottrina in materia, ma ho maturato un'esperienza a diretto contatto con gli "attori europei" dello scambio transnazionale delle prove digitali nel processo penale). Dall'altro lato, la prospettiva con cui ho analizzato le informazioni è orientata verso un'ottica comparata (infatti, i team di ricerca dei progetti erano provenienti da diversi paesi europei). E in definitiva, l'esperienza concreta mi ha permesso di individuare possibili proposte di azioni da intraprendere sia a livello europeo che nazionale, per la realizzazione di un sistema sicuro ed efficace di scambio delle prove digitali. Proposte ed azioni che tenessero conto delle esigenze e richieste dei soggetti direttamente coinvolti nel procedimento di scambio delle prove digitali.

2.3 Stato dell'arte della legislazione dell'Unione europea sull'implementazione della cooperazione giudiziaria in materia penale: gli strumenti di Mutua assistenza legale e l'European Investigation Order

Per avere informazioni complete circa lo "stato dell'arte" in Europa in materia di scambio transnazionale delle prove digitali in ambito penale è determinante, oltre ad uno studio sulle iniziative e politiche adottate in materia, anche uno studio approfondito della legislazione dell'Unione.

Oggetto del presente lavoro è infatti anche l'esame di tale legislazione, al fine di avere un quadro chiaro e preciso circa l'attuazione della cooperazione giudiziaria in materia penale, ed in particolare sull'attuazione delle procedure relative all'EIO.

Preliminarmente, occorre tenere presente che negli ultimi anni l'esponenziale sviluppo delle tecnologie digitali e la continua globalizzazione delle reti di computer hanno determinato fondamentali cambiamenti nella società. Cambiamenti che hanno avuto anche un impatto negativo, determinando l'emergere di nuovi tipi di crimini/delitti informatici o anche la commissione

di c.d. crimini comuni attraverso l'uso degli strumenti informatici. In altre parole, l'aumento della tecnologia e delle comunicazioni on line ha prodotto, in generale, un aumento dell'incidenza della criminalità informatica, ed ha portato alla nascita di quelle che sembrano essere alcune nuove tipologie di attività criminali[18].

La digitalizzazione della nostra vita quotidiana ha, inoltre, determinato la produzione di dati e tracce digitali che possono essere identificate come prove da utilizzare e valutare nell'ambito di un processo penale.

Tuttavia, la crescente considerazione di alcuni dei principali inconvenienti legati all'utilizzo delle prove digitali (si veda, prima fra tutte, la mancanza di un'uniforme regolamentazione delle stesse nell'ambito dei vari Stati membri) ha anche fatto emergere la necessità di creare uno scenario giuridico europeo comune, che possa incidere sulla disciplina nazionale in materia.

Sotto questo profilo, l'Unione europea ha rappresentato una figura fondamentale nel tentativo di combattere la criminalità informatica attraverso iniziative volte principalmente a realizzare forme di cooperazione in materia penale tra le autorità competenti dei vari Stati membri.

L'art. 34 del Trattato Ue prevedeva, a tale proposito, che il Consiglio europeo potesse adottare decisioni quadro e convenzioni.

Nell'ambito di tale competenza è stata adottata la Convenzione del 29 maggio 2000 relativa all'assistenza giudiziaria in materia penale tra gli Stati membri[19], con l'obiettivo di "migliorare la cooperazione giudiziaria tramite la modernizzazione delle disposizioni in vigore nel settore, in particolare estendendo i casi in cui può essere richiesta l'assistenza giudiziaria e agevolando il funzionamento della stessa, che sarà al contempo più rapido flessibile ed efficace"[20]. In particolare, nella Convenzione si fa esplicito riferimento (negli artt. 10, 11 e da 17 a 22 relativi alle intercettazioni di telecomunicazioni)

[18] S. Mason, *Electronic Evidence*, III ed., LexisNexis Butterworths, 2012, pp. 495-496.

[19] Convenzione stabilita dal Consiglio conformemente all'articolo 34 del trattato sull'Unione europea, relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea. La Convenzione del 2000 mira ad integrare la Convenzione europea di assistenza giudiziaria in materia penale firmata a Strasburgo dai membri del Consiglio d'Europa il 20 aprile 1959. L'art. 1 della Convenzione del 2000 espressamente stabilisce che: «La presente convenzione è volta a completare le disposizioni e facilitare l'applicazione tra gli Stati membri dell'Unione europea della convenzione europea di assistenza giudiziaria in materia penale del 20 aprile 1959». Si veda https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:42000A0712(01)&from=IT.

[20] Relazione esplicativa sulla Convenzione del 29 maggio 2000 relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea.

all'obiettivo di tenere conto nel settore della cooperazione giudiziaria anche delle più importanti innovazioni e sviluppi della tecnologia.

Sebbene la Convenzione non parli esplicitamente di prove digitali (e in generale nemmeno di prove in forma "tradizionale"), tuttavia risulta rilevante in materia, data la possibilità di comprendere nella richiesta di cooperazione giudiziale da parte di uno Stato membro verso un altro, anche tali tipi di prove.

Tra le decisioni quadro in materia penale, deve invece essere menzionata la Decisione quadro adottata il 24 febbraio 2005, n. 222 sugli attacchi contro i sistemi informatici[21], che mirava ad implementare maggiormente la cooperazione "tra le autorità giudiziarie e le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge, mediante il ravvicinamento delle legislazioni penali[22].

La decisione quadro contemplava tre tipologie di condotte punibili, in presenza delle quali ciascuno Stato membro doveva adottare tutte le misure necessarie al fine di prevenire e reprimere ogni tipo di "accesso o danneggiamento intenzionale e senza diritto" ai sistemi informatici:

- accesso illecito ai sistemi di informazione;
- interferenza illecita per quanto riguarda i sistemi;
- interferenza illecita per quanto riguarda i dati.

Sebbene non espressamente dedicata al tema dello scambio transnazionale delle prove digitali, tuttavia la decisione citata merita di essere segnalata quale strumento per garantire un rafforzamento della cooperazione giudiziaria in materia penale.

Altra decisione quadro rilevante, in questo caso proprio in materia di prove, era la Decisione quadro 2008/978 del Consiglio del 18 dicembre 2008 relativa al mandato europeo di ricerca delle prove (MER)[23], diretto all'acquisizione di oggetti, documenti e dati da utilizzare nei procedimenti penali. Si trattava di uno strumento adottato allo scopo di conservare e sviluppare uno spazio di libertà, sicurezza e giustizia e per favorire la cooperazione

[21]Decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32005F0222&from=IT.

[22]Preambolo alla Decisione quadro 2005/222.

[23]Decisione quadro 2008/978/GAI relativa al mandato europeo di ricerca delle prove diretto all'acquisizione di oggetti, documenti e dati da utilizzare nei procedimenti penali, https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0072:0092:IT:PDF.

giudiziaria tramite l'applicazione del principio del reciproco riconoscimento delle decisioni giudiziarie.

Tale strumento ha inteso superare la Decisione quadro 2003/577/GAI del Consiglio, del 22 luglio 2003, relativa all'esecuzione nell'Unione europea dei provvedimenti di blocco dei beni o di sequestro probatorio[24], che «rispondeva alla necessità dell'immediato riconoscimento reciproco delle decisioni al fine di prevenire atti di distruzione, trasformazione, spostamento, trasferimento o alienazione di mezzi di prova. Essa verte tuttavia soltanto su una parte della cooperazione giudiziaria in materia penale che riguarda i mezzi di prova, mentre il successivo trasferimento degli stessi rimaneva disciplinato dalle procedure di assistenza giudiziaria»[25].

Infatti, il MER, secondo il considerando n. 7 della Decisione «può essere utilizzato per acquisire, ad esempio, gli oggetti, i documenti o i dati che provengono da un terzo o risultanti dalla perquisizione di locali, ivi compresa la perquisizione domiciliare, i dati storici sull'uso di servizi, comprese le operazioni finanziarie, verbali di dichiarazioni, interrogatori e audizioni e altri documenti, compresi i risultati di speciali tecniche investigative.»

Quindi l'intento del Legislatore comunitario era quello di migliorare ulteriormente la cooperazione giudiziaria tramite l'applicazione del principio del reciproco riconoscimento delle decisioni giudiziarie, nella forma di un MER diretto all'acquisizione di oggetti, documenti e dati da utilizzare nei procedimenti penali.

Nonostante che il mandato europeo di ricerca delle prove abbia rappresentato il primo concreto riconoscimento del principio di reciproco riconoscimento delle decisioni nell'ambito del diritto penale e uno strumento fondamentale per lo sviluppo della cooperazione giudiziaria tra Stati membri in materia penale, tuttavia ha avuto un ambito di applicazione limitato riferendosi soltanto alle prove (anche digitali) già esistenti.

Inoltre il MER è stato abrogato con il Reg. (UE) 2016/95 del Parlamento europeo e del Consiglio del 20.1.2016, relativo all'abrogazione di alcuni atti nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale[26].

[24]Si veda https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32003F0577&from=IT.

[25]Considerando n. 5 della Decisione quadro 2008/978/GAI.

[26]Gazzetta ufficiale dell'Unione europea L 26/11.

Con l'entrata in vigore del Trattato di Lisbona le procedure volte all'armonizzazione delle legislazioni penali degli Stati membri sono in qualche modo cambiate: infatti, l'art. 83 del Trattato sul Funzionamento dell'Unione europea (TFUE) stabilisce che «il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni».

Le sfere di criminalità di cui parla il Trattato sul funzionamento dell'Unione europea sono:

- terrorismo;
- tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori;
- traffico illecito di stupefacenti;
- traffico illecito di armi;
- riciclaggio di capitali;
- corruzione;
- contraffazione di mezzi di pagamento;
- criminalità organizzata;
- criminalità informatica.

Quindi, lo strumento a disposizione dell'Unione europea per stabilire un insieme minimo di regole che permettano di realizzare un ravvicinamento delle legislazioni in materia penale, ed anche in materia di criminalità informatica, è rappresentato dalle direttive.

In particolare, le Direttiva 2013/40/Ue e la Direttiva 2014/41/Ue hanno dato un contributo rilevante al tema trattato nel presente lavoro.

La Direttiva 2013/40 del Parlamento e del Consiglio del 12 agosto 2013[27] sostituisce la Decisione 2005/222/UE in materia di attacchi contro i sistemi informatici: nonostante la direttiva contempli le medesime condotte della decisione quadro[28], tuttavia la sua adozione ha mirato non soltanto ad implementare e migliorare la cooperazione tra autorità giudiziarie e di polizia nel contrasto alla criminalità informatica, ma anche a realizzare il ravvicina-

[27]Si veda https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32013L0040&from=EN.

[28]Si vedano a tal fine gli artt. 3-7 della Direttiva 2013/40.

mento del diritto penale degli Stati[29]. In particolare, la direttiva si propone di stabilire norme minime comuni integrate con sanzioni rigorose ed effettive al fine di rendere efficace la lotta alla criminalità informatica e, al contempo, garantire e sviluppare uno spazio di libertà, sicurezza e giustizia.

La Direttiva 2014/41/UE è relativa all'ordine europeo di indagine penale e, come più volte sottolineato nel corso del presente lavoro, riveste un'importanza fondamentale in relazione proprio alla raccolta delle prove in ambito penale e, quindi, anche delle prove digitali. La direttiva mira a sostituire il vecchio quadro esistente per l'acquisizione delle prove: ad esempio, la disciplina introdotta dalla Decisione quadro 2003/577/GAI risultava frammentaria essendo relativa soltanto all'esecuzione nell'Unione europea dei provvedimenti di blocco dei beni o di sequestro probatorio.

La decisione, come sopra sottolineato, rispondeva soltanto alla «necessità dell'immediato riconoscimento reciproco dei provvedimenti intesi a impedire atti di distruzione, trasformazione, spostamento, trasferimento o alienazione di prove solo però con riferimento alla fase di blocco o sequestro».

Tuttavia, poiché un provvedimento di blocco o di sequestro deve essere accompagnato da una distinta richiesta di trasferimento della fonte di prova nello Stato che emette il provvedimento (lo "Stato di emissione") in conformità delle norme applicabili all'assistenza giudiziaria in materia penale, ne derivava una procedura in due fasi che comprometteva l'efficienza di tale strumento.

Inoltre, tale regime coesisteva con gli strumenti tradizionali di cooperazione giudiziaria quindi le autorità competenti se ne avvalevano raramente nella pratica.

Con la Direttiva 2014/41/UE invece viene creato un «sistema globale di acquisizione delle prove nelle fattispecie aventi dimensione transfrontaliera»[30]: con l'ordine europeo di indagine lo Stato di emissione ottiene che

[29]Considerando n. 1 della Direttiva 2013/40: «Gli obiettivi della presente direttiva sono ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione, stabilendo norme minime relative alla definizione dei reati e delle sanzioni rilevanti, e migliorare la cooperazione fra le autorità competenti, compresi la polizia e gli altri servizi specializzati degli Stati membri incaricati dell'applicazione della legge, nonché le competenti agenzie e gli organismi specializzati dell'Unione, come Eurojust, Europol e il suo Centro europeo per la criminalità informatica, e l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)».

[30]Considerando n. 6 della Direttiva 2014/41: «Nel programma di Stoccolma, adottato dal Consiglio europeo del 10-11 dicembre 2009, il Consiglio europeo ha considerato di

venga compiuto in un altro Stato membro (c.d. di esecuzione) un determinato atto di indagine senza che siano necessarie ulteriori formalità e in modo veloce ed efficace.

A questo proposito, l'art. 9 della Direttiva stabilisce che «l'autorità di esecuzione riconosce un ordine europeo di indagine, trasmesso conformemente alle disposizioni della presente direttiva, senza imporre ulteriori formalità e ne assicura l'esecuzione nello stesso modo e secondo le stesse modalità con cui procederebbe se l'atto d'indagine in questione fosse stato disposto da un'autorità dello Stato di esecuzione». E l'art. 12 continua indicando che «l'autorità di esecuzione compie l'atto di indagine senza ritardo».

In definitiva, l'obiettivo della direttiva in esame è quello di rendere più veloci ed efficaci le investigazioni transfrontaliere, mettendo a disposizione degli Stati membri uno strumento in grado di garantire la speditezza dei procedimenti penali e al contempo in grado di far fronte alla volatilità dei dati digitali che possono venire in rilievo durante un'attività di indagine.

La realizzazione di un tale ambizioso obiettivo di libera circolazione della prova si fonda, prioritariamente, sulla reciproca fiducia tra gli Stati dell'Unione.

La creazione di un clima di reciproca fiducia tra i diversi Stati dell'Unione presuppone che le varie culture giudiziarie condividano il medesimo percorso evolutivo democratico proteso al rispetto dei diritti fondamentali.

Solo la condivisione, tra i diversi ordinamenti, di uno standard tendenzialmente uniforme di garanzie può certificare la validità e, dunque, l'affidabilità del dato probatorio.

Pur nella consapevolezza delle molteplici difficoltà e resistenze che si frappongono alla realizzazione di un simile obiettivo di armonizzazione, appare, tuttavia, corretto sostenere che solo attraverso un sistema condiviso di reciproca ammissibilità della prova e di uniformità nelle procedure di scam-

perseguire ulteriormente l'istituzione di un sistema globale di acquisizione delle prove nelle fattispecie aventi dimensione transfrontaliera, basato sul principio del riconoscimento reciproco. Il Consiglio europeo ha rilevato che gli strumenti esistenti nel settore costituiscono una disciplina frammentaria e che è necessaria una nuova impostazione che, pur ispirandosi al principio del riconoscimento reciproco, tenga conto altresì della flessibilità del sistema tradizionale di assistenza giudiziaria. Il Consiglio europeo ha pertanto chiesto la creazione di un sistema globale in sostituzione di tutti gli strumenti esistenti nel settore, compresa la Decisione quadro 2008/978/GAI del Consiglio, che contempli per quanto possibile tutti i tipi di prove, stabilisca i termini di esecuzione e limiti al minimo i motivi di rifiuto».

bio, può essere effettivamente ed efficacemente realizzato un miglioramento e rafforzamento della cooperazione giudiziaria.

Più nello specifico, dal punto di vista della procedura, l'EIO si concretizza in una particolare decisione giudiziaria emessa o convalidata da un'autorità competente di uno Stato membro ("Stato di emissione"), che ordina all'autorità giudiziaria di un altro Stato membro ("Stato di esecuzione") di compiere uno o più atti di indagine specifici al fine di acquisire delle prove o per ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione (art. 1). A titolo esemplificativo si può trattare di sequestri, intercettazioni ambientali o telefoniche, o acquisizione diretta di documentazione a valore probatorio.

L'EIO deve essere emesso da un organo giurisdizionale o da un magistrato inquirente, oppure deve essere convalidato da questi ultimi, prima della trasmissione all'autorità di esecuzione (art. 2). L'EIO è trasmesso dall'autorità di emissione all'autorità di esecuzione con ogni mezzo che consenta di conservare una traccia scritta e che permetta allo Stato di esecuzione di stabilirne l'autenticità (art. 7).

Il riconoscimento e l'esecuzione dell'EIO avvengono senza alcuna ulteriore formalità. L'autorità competente dello Stato di esecuzione è tenuta ad adottare immediatamente tutte le misure necessarie, come sopra già specificato in riferimento all'art. 9 della Direttiva.

A differenza degli strumenti di cooperazione descritti in precedenza, l'EIO si applica a tutte le misure di indagine finalizzate a ottenere una prova. Il fatto che le prove siano già esistenti o meno non è rilevante per l'EIO.

In conclusione, l'EIO è uno strumento con il quale si intende introdurre a livello europeo un quadro giuridico unico e completo per la cooperazione in materia penale, in particolare in relazione allo scambio delle prove (comprese quelle digitali).

Tuttavia molteplici sono i profili di complessità di questa normativa, che hanno alimentato ampi dibattiti a livello europeo e nazionale.

Da un lato, se è evidente che le tecnologie dell'informazione possano offrire lo strumento ideale di scambio di tutta la documentazione richiesta/trasmessa nel corso della procedura, dall'altro, l'uso di tali strumenti informatici non uniformi potrebbe porre problemi di sicurezza, segretezza, non corretta e certa identificazione delle autorità dello Stato di emissione e di quello di esecuzione.

In aggiunta, sorgono già alcune perplessità sull'operatività del nuovo strumento normativo, legate alla sentita necessità di predisporre particolari forme di tutela dei diritti fondamentali dei soggetti coinvolti nell'esecuzione e messa in atto degli strumenti di cooperazione.

Infatti, l'aumento delle misure investigative intrusive attuabili oltre i confini nazionali, quali ad esempio l'intercettazione delle telecomunicazioni, richiede un quadro normativo che contempli anche modalità e strumenti rivolti alla protezione dei dati personali che possono venire in rilievo quando viene data esecuzione all'EIO. Occorre, in altre parole, che la riservatezza dei dati personali degli individui coinvolti nelle procedure di EIO sia rispettata e sia garantita al tempo stesso l'integrità dei medesimi dati.

La complessità della normativa sull'EIO e delle procedure connesse è stata oggetto di specifiche sezioni e sottosezioni del questionario, le cui informazioni sono state analizzate con il presente lavoro.

In particolare, due sottosezioni hanno mirato ad ottenere informazioni sulle autorità giudiziarie competenti nei singoli Stati membri ad emanare ed eseguire l'EIO, mentre una sottosezione è interamente dedicata alle modalità e forme di trasmissione dell'EIO.

Capitolo 3

Gli aspetti giuridici e l'implementazione dell'EIO, l'analisi dei risultati del questionario on line

Il Capitolo analizza i risultati delle risposte al questionario circolato on line e completato da 31 partecipanti all'indagine (rappresentanti di 16 Stati membri dell'Unione europea), appartenenti a diversi "target groups" (giudici e pubblici ministeri, personale amministrativo e tecnico delle Corti, infine esperti di digital forensics). In particolare, dopo aver analizzato i risultati di una prima sezione "Generale", sullo stato di implementazione dell'EIO nei vari Stati membri, il paragrafo 3.2 presenta tutta una serie di domande strettamente collegate agli aspetti "legali/giuridici" della procedura di EIO. Le questioni affrontate rivestono particolare importanza per individuare lo stato dell'arte delle procedure in atto nei singoli Stati membri a seguito dell'attuazione della Direttiva 2014/41/UE e per identificare anche quelli che potrebbero essere possibili ostacoli allo scambio delle prove digitali derivanti da diversità delle procedure nazionali concernenti l'EIO[1].

[1]Il Capitolo 3 del presente lavoro è il frutto della mia partecipazione alle attività di studio e ricerca condotte nell'ambito dei progetti europei Evidence2e-Codex ed EXEC, nel corso del triennio di dottorato. In particolare, l'analisi condotta e i risultati descritti nel presente Capitolo sono stati presentati ai seguenti seminari/meetings: 1. *Meeting*

3.1 Analisi della sezione "Generale" del questionario e risultati

La sezione generale del questionario ha riguardato la raccolta di informazioni relative allo stato di implementazione della Direttiva 2014/41/EU sull'ordine europeo di indagine negli Stati membri dell'Unione europea.

Le domande poste ai partecipanti all'indagine sono state essenzialmente due:

Q1. Il suo Stato ha implementato la Direttiva sull'EIO? In caso positivo, indichi i riferimenti alla normativa di attuazione (numero e data di pubblicazione) e indichi anche la data a partire dalla quale le autorità giudiziarie del suo Stato dovranno utilizzare le procedure di EIO

Q2. Il suo Stato ha una versione inglese ufficiale della normativa di implementazione nazionale dell'EIO? In caso positivo indichi il link a cui è possibile reperirla oppure alleghi al presente questionario una copia.

Tutti i 31 utenti che hanno avuto accesso al questionario sono stati in grado di completare queste due domande, dalle caratteristiche molto generali.

I risultati hanno dimostrato che gli Stati membri partecipanti all'indagine sono interessati all'attuazione e al funzionamento dell'EIO in quanto tutti hanno recepito e attuato la direttiva EIO, ad eccezione della Danimarca.

Per quanto riguarda gli Stati membri oggetto di una più approfondita analisi nel presente lavoro, tutti e sei hanno risposto di avere adottato provvedimenti nazionali di attuazione della Direttiva.

La tabella sottostante, riporta una traduzione delle risposte date ed una breve descrizione dei provvedimenti adottati da Austria, Repubblica Ceca, Spagna, Croazia, Lituania e Lussemburgo.

---

the Technical Community: Validation of the Evidence (L'Aja, 26-27 marzo 2019) organizzato nell'ambito dei progetti europei Evidence2e-CODEX ed EXEC; 2. *e-Evidence co-funded project coordination Meeting* (Bruxelles, Commissione europea, 23 luglio 2019). Il paragrafo 3.2.7 del presente Capitolo relativo agli strumenti internazionali di lotta alla criminalità informatica è stato pubblicato in S. Conti, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, cit., pp. 154-158. Il paragrafo 3.2.9 relativo alle iniziative di training in materia di EIO per le autorità giudiziarie è in corso di pubblicazione (gennaio 2020) in S. Conti, G. Peruginelli, *La tutela dei dati personali nel settore giudiziario: l'importanza dei modelli e-learning*, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), "Dati e Algoritmi. Diritto e diritti nella società digitale", Il Mulino.

Tabella 3.1: Implementazione nazionale della Direttiva 2014/41/UE

MS di interesse	**Implementazione nazionale**	**Link alla versione online**	**Versione inglese**
Austria	BGBl, Legge n. 28/2018; Data di pubblicazione: 15/05/2018	www.ris.bka.gv.at/Bundesrecht	NO
Rep. Ceca	Provvedimento no. 178/2018 Sb., in vigore dal 19 luglio 2018.	Non disponibile	NO
Spagna	Legge n. 3/2018 di modifica della Legge n. 23/2014, pubblicata nella Gazzetta Ufficiale spagnola n. 142 del 12 giugno 2018, in vigore dal 2 luglio 2018	Non disponibile	NO
Croazia	“Act on the Amendments to the Act on Judicial Cooperation in Criminal Matters with Member States of the European Union”, del 4 Ottobre 2017 ed entrato in vigore il 26 Ottobre 2017 (Gazzetta Ufficiale croata n. 102/07 del 18 ottobre 2017)	Non disponibile	NO
Lituania	Legge No XIII-397 del 2017	Non disponibile	YES
Lussemburgo	“Loi du 1er août 2018 portant 1° transposition de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d’enquête européenne en matière pénale“, in vigore da settembre 2018	Non disponibile	NO

La sezione "Generale" sull'attuazione dell'EIO negli Stati membri ha individuato due possibili ostacoli alla creazione di un quadro comune europeo in materia di scambio delle prove, e in particolare delle prove digitali:

- frammentazione delle diverse leggi di attuazione: in alcuni Stati sono state emanate più leggi di attuazione e non un unico provvedimento;
- mancanza di una versione inglese di ciascuna legge/disposizione nazionale di attuazione.

Tali ostacoli possono essere superati da un'azione di ciascuno Stato membro, a livello nazionale, volta a prevedere:

- un consolidamento delle leggi e disposizioni di attuazione in un unico quadro giuridico nazionale che faciliti la sua comprensione e applicazione;
- almeno una breve sintesi ufficiale, in lingua inglese, della normativa di attuazione e la possibilità di renderla disponibile on line.

3.2 Analisi della sezione "B" del questionario e risultati

La sezione in esame presenta una serie di domande strettamente collegate agli aspetti "legali/giuridici" della procedura di EIO.

Le questioni affrontate nella sezione rivestono particolare importanza per individuare il livello di attuazione della Direttiva 2014/41/UE a livello nazionale e per identificare anche quelli che potrebbero essere possibili ostacoli allo scambio delle prove digitali, derivanti da diversità nelle procedure concernenti l'EIO in ciascuno degli Stati membri.

3.2.1 Analisi della sezione "B1" del questionario: EIO e procedure di MLA

Il primo gruppo di domande della sezione mira a verificare il rapporto tra gli strumenti di MLA e l'EIO negli Stati membri interessati.

In particolare ai partecipanti all'indagine sono state richieste le seguenti domande:

Q1. A partire dal 22 maggio 2017 l'EIO è diventato l'unico strumento in ambito UE per la raccolta e il trasferimento di tutti i tipi di prove, incluse

le prove digitali. Il suo Stato ha già provveduto a sostituire gli strumenti di MLA con l'EIO?

Q2. In caso di sostituzione, questa è stata totale o parziale?

Q3. In caso di sostituzione parziale, in che modo le due procedure convivono nel suo Stato?

Per quanto riguarda la prima domanda (Q1), i risultati generali hanno mostrato che quasi tutti i paesi partecipanti all'indagine hanno già sostituito i precedenti strumenti giuridici in materia di cooperazione giudiziaria penale (strumenti di MLA) con l'EIO (Figura 3.1). Le uniche eccezioni sono rappresentate dalla Danimarca e dal Lussemburgo. Quest'ultimo, al momento del completamento del questionario, non aveva ancora implementato la direttiva EIO, in quanto la legge di recepimento della Direttiva è entrata in vigore nel settembre 2018.

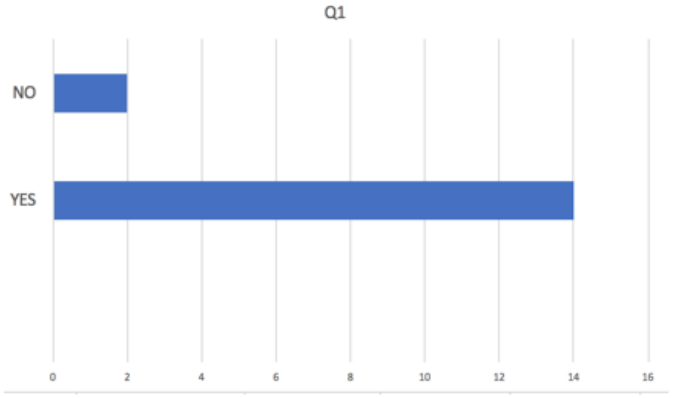

Figura 3.1: Q1, rapporto tra MLA e EIO

Per quanto riguarda la seconda domanda della sezione (Q2), le risposte, come evidenziato nella successiva figura (Figura 3.2), hanno dimostrato che per la maggior parte degli Stati membri (circa 45% dei partecipanti all'indagine) la sostituzione tra strumenti di MLA ed EIO è stata completa, mentre solo in pochi casi la sostituzione è stata parziale (circa 30%). Ovvero, a seguito del recepimento da parte degli Stati membri della Direttiva sull'EIO, quest'ultimo rappresenta l'unico strumento per compiere uno o più atti di indagine in un altro Stato membro e per lo scambio delle prove, anche di-

gitali. Laddove la risposta non è stata data (circa 25%), nella figura viene riportato il campo "Vuoto" (Empty).

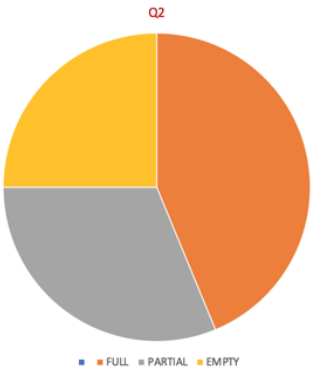

Figura 3.2: Q2, tipologia di sostituzione

Nel caso in cui la sostituzione tra i due diversi tipi di strumenti sia parziale, la terza domanda (Q3) è volta a verificarne proprio le modalità di coesistenza.

Gli Stati membri che hanno dichiarato di aver adottato una sostituzione parziale (circa 30%), hanno anche indicato che tale sostituzione opera in una modalità combinata (ovvero vengono utilizzate sia le procedure di MLA sia l'EIO). Tuttavia, solo la metà di coloro che avevano optato per la sostituzione parziale ha dato una risposta sulle modalità di combinazione delle diverse procedure di cooperazione (Figura 3.3).

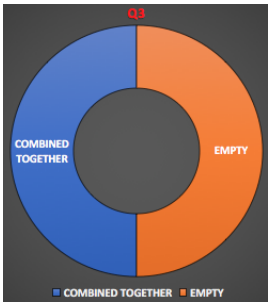

Figura 3.3: Q3, modalità di combinazione tra i due strumenti

Per quanto riguarda la situazione specifica negli Stati oggetto del presente lavoro, dal questionario risulta che la sostituzione tra gli strumenti di MLA e l'EIO è stata completa. Le procedure di MLA sono utilizzate solo laddove sia richiesta cooperazione giudiziaria in materia penale verso Stati membri che non applicano la procedura EIO ovvero con Stati terzi non UE.

Il secondo gruppo di domande della sezione B1 è dedicato alla individuazione delle modalità di gestione delle richieste di MLA e all'analisi delle metodologie e dei mezzi di trasmissione delle richieste stesse. In particolare i partecipanti all'indagine hanno risposto sulle seguenti tematiche:

Q4. Come sono trasmesse le richieste di MLA?

Q5. Le modalità elettroniche di trasmissione sono accettate nel suo Stato?

Q6. È richiesto un quadro giuridico specifico per l'utilizzo di una piattaforma on line per la trasmissione?

Q7. Il flusso di lavoro relativo alle richieste di MLA è simile a quello in caso di utilizzo dell'EIO?

Q8. Gli stessi modelli/moduli (“forms”) utilizzati per le richieste di EIO possono essere utilizzati anche in caso di MLA?

In generale, le risposte alla prima domanda relativa alle modalità di trasmissione delle richieste di MLA (Q4), hanno indicato che i mezzi tradizionali (posta e fax) sono quelli prevalenti, mentre una buona percentuale di Stati membri utilizza, in casi urgenti, anche la trasmissione della richiesta via e-mail. Una piccola percentuale degli Stati membri che hanno partecipato all'indagine (circa 15%) dichiara di utilizzare anche altre modalità di trasmissione, ad esempio piattaforme elettroniche come e-Codex (Figura 3.4).

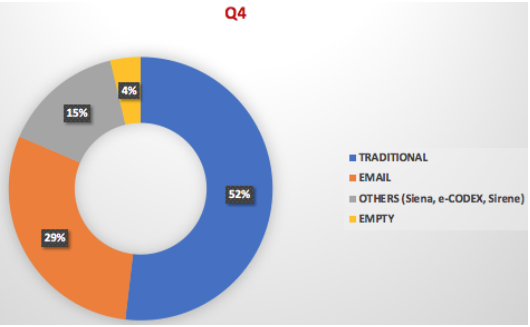

Figura 3.4: Q4, trasmissione delle richieste MLA

Per quanto riguarda la situazione specifica nei paesi presi in considerazione dal presente lavoro, tutti hanno confermato l'utilizzo di mezzi tradizionali di trasmissione delle richieste. In particolare, in Austria e in Repubblica Ceca, la modalità di trasmissione delle richieste MLA via posta risulta essere la più utilizzata. Spagna, Lituania e Lussemburgo invece utilizzano come modalità prevalente di trasmissione delle richieste quella via e-mail. In Croazia invece le richieste di MLA vengono trasmesse con canali tradizionali in via centralizzata, ovvero attraverso il Ministero della Giustizia.

La successiva domanda (Q5) mira a verificare più nello specifico se, anche se non utilizzati concretamente, i mezzi elettronici di trasmissione siano generalmente accettati dagli Stati membri partecipanti all'indagine.

I risultati dimostrano che i mezzi elettronici di trasmissione sono generalmente accettati, soprattutto nei casi di urgenza, anche se alcuni Stati membri richiedono che la versione originale della richiesta sia anche inviata per posta, al fine di consentire all'autorità dello Stato membro in cui deve essere eseguita la richiesta, di valutarne l'autenticità. Per quanto riguarda nello specifico gli Stati membri oggetto del presente lavoro, la situazione è allineata a quella sopra descritta: accettano tutti la trasmissione elettronica anche se questa non rappresenta lo strumento prevalente per la trasmissione delle richieste (Figura 3.5).

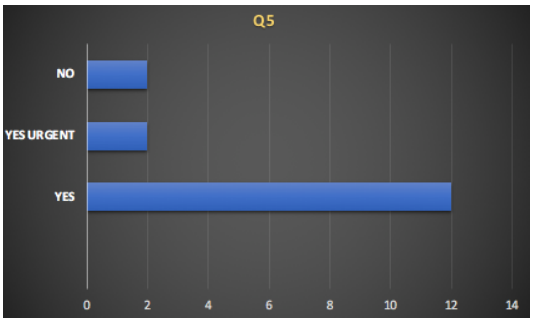

Figura 3.5: Q5, utilizzo mezzi elettronici di trasmissione MLA

La domanda (Q6) esamina se sia richiesto nell'ordinamento nazionale degli Stati membri un quadro giuridico specifico che permetta all'autorità giudiziaria di utilizzare una piattaforma on line per lo scambio di richieste nell'ambito dell'MLA.

La maggior parte degli Stati membri ha risposto che tale quadro giuridico non è richiesto, tuttavia 5 Stati membri che hanno partecipato all'indagine hanno dato risposta positiva senza tuttavia fornire indicazioni su provvedimenti e/o leggi specifiche che autorizzino l'utilizzo di tali piattaforme.

Per quanto riguarda nello specifico gli Stati membri oggetto del presente lavoro, tutti hanno dichiarato che non esiste nei rispettivi ordinamenti la necessità di un quadro giuridico per utilizzare una piattaforma on line di scambio, ad eccezione dell'Austria (tuttavia, come sopra detto, non è stato poi specificato di quale quadro giuridico si tratti) (Figura 3.6).

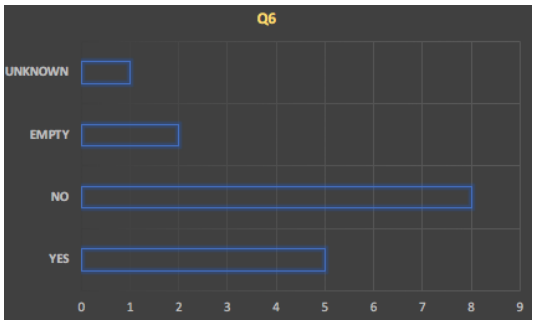

Figura 3.6: Q6, quadro giuridico specifico per scambio richieste di MLA

Per quanto riguarda la domanda (Q7), in generale risulta che quasi tutti gli Stati membri hanno dichiarato che il flusso di lavoro in caso di richieste di MLA è simile a quello in caso di EIO, come dimostrato dalla Figura 3.7.

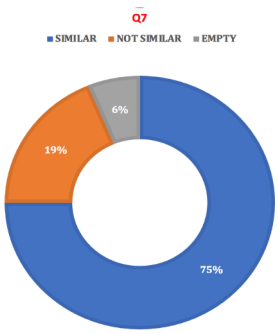

Figura 3.7: Q7, tipologia flusso lavoro in caso di MLA vs. EIO

Per quanto riguarda nello specifico gli Stati membri oggetto del presente lavoro, sono generalmente allineati con i risultati sopra indicati. Unica eccezione, la Repubblica Ceca che ha dichiarato che le richieste di MLA sono trasmesse attraverso il Ministero della Giustizia mentre le richieste di EIO sono emesse e inviate direttamente dall'Ufficio giudiziario competente nel territorio. In altre parole, le autorità giudiziarie competenti emettono e inviano l'EIO direttamente all'autorità competente dello Stato di esecuzione mentre in caso di MLA occorre l'intervento dell'autorità centrale.

I risultati della domanda (Q8) specificano che, anche se i flussi di lavoro sono simili, tuttavia i moduli/modelli utilizzati per la richiesta sono diversi a seconda che si tratti di MLA o EIO, e variano da Stato a Stato[2].

Per quanto riguarda nello specifico gli Stati membri oggetto del presente lavoro, tutti dichiarano di utilizzare "forms" diverse per le richieste (Figura 3.8).

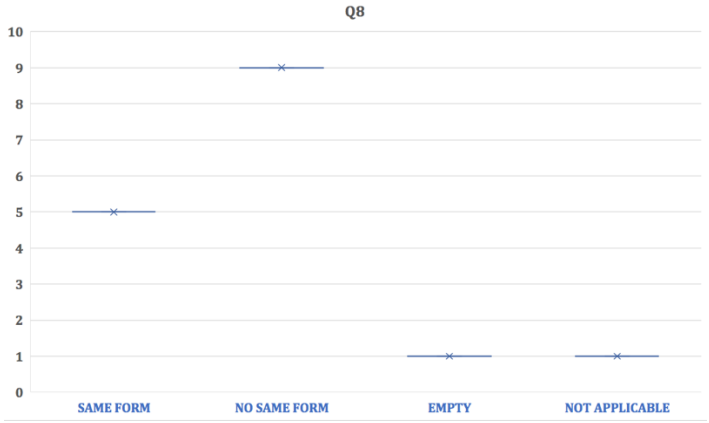

Figura 3.8: Q8, tipologia moduli utilizzati per le richieste di MLA vs. EIO

L'analisi dei risultati della sezione B1 del questionario, sul rapporto tra EIO e MLA, ha individuato l'esistenza di tre barriere che possono impedire o comunque rallentare, un efficace utilizzo degli strumenti di cooperazione giudiziaria in materia penale:

[2]Il riferimento nella Figura 3.8 "not applicable" riguarda la Danimarca, che non ha attuato la Direttiva 2014/41/UE.

– in caso di sostituzione parziale degli strumenti di MLA con l’EIO, non è sempre chiaro come funzioni questa relazione e quando i primi siano preferibili al secondo;
– lo strumento di trasmissione delle richieste di MLA è principalmente quello tradizionale (posta e fax);
– esistono diversi tipi di moduli MLA in uso nei vari Stati e questo può creare difficoltà di comprensione e possibili errori nella procedura.

Queste barriere possono essere superate da un’azione di vari attori che, a diverso titolo, concorrono a definire il quadro europeo in materia di cooperazione giudiziaria penale. In particolare:

– gli Stati membri, a livello nazionale, dovrebbero chiarire quando le procedure di MLA devono essere preferite all’EIO, con l’elaborazione di Linee guida per le autorità giudiziarie che si occupano di richieste di MLA ed EIO;
– gli Stati membri dovrebbero utilizzare strumenti elettronici, come le e-mail per la trasmissione, oppure potrebbero utilizzare piattaforme sicure e affidabile sviluppate nell’ambito di azioni progettuali europee (si pensi ad esempio alla piattaforma e-CODEX);
– gli Stati membri dovrebbero concordare un formato comune da utilizzare per le richieste di MLA, anche per le richieste agli ISPs. In questo caso dovrebbero essere incentivate le azioni progettuali europee finalizzate allo scopo di creare “forms”/moduli uniformi per le richieste in tutta l’area europea.

3.2.2 Analisi della sezione “B2” del questionario: le procedure di emissione e trasmissione dell’EIO

Questa sezione mira ad acquisire informazioni pertinenti sull’emissione e la trasmissione di richieste di EIO e anche ad avere una panoramica circa il volume di utilizzo della procedura di richiesta di indagine tramite EIO.

In particolare, le domande poste ai partecipanti all’indagine sono state le seguenti:

Q1. Esiste un obbligo interno per le autorità giudiziarie locali di comunicare a un’autorità nazionale centrale il numero di EIO emessi e ricevuti?

Q2. In tal caso, c’è la possibilità di avere rapporti statistici sull’ammontare di EIO già emessi o ricevuti? È possibile conoscerne il numero preciso?

Q3. Se questo obbligo non esiste, esiste un altro sistema che consenta la raccolta di informazioni sulla quantità di EIO emessi ed eseguiti dalle autorità nazionali locali?

Q4. Esiste un database nazionale centralizzato o esistono database locali per la raccolta e l'archiviazione di EIO? In quest'ultimo caso, quale è il livello di decentramento (ad es. singole banche dati per ciascuna Corte di appello, banche dati regionali, ecc.)

In relazione alla prima domanda (Q1), i risultati dimostrano (Figura 3.9) che la maggior parte degli Stati membri prevede per le autorità giudiziarie locali un obbligo di riferire a un'autorità nazionale centrale sul numero di EIO emessi e ricevuti.

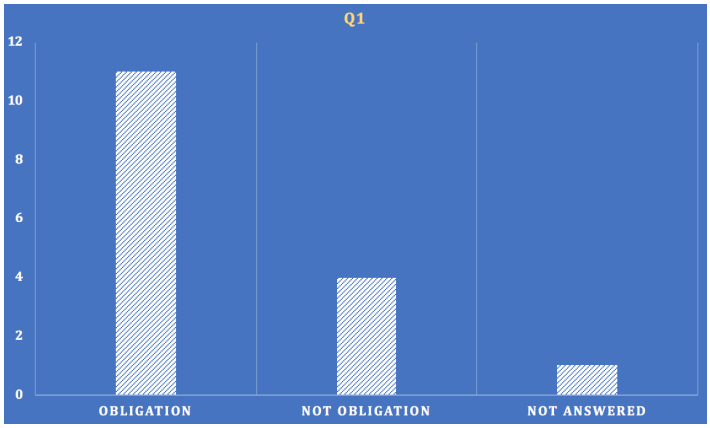

Figura 3.9: Q1, obbligo comunicazione EIO emessi e ricevuti

Per la maggior parte degli Stati membri l'obbligo di riferire sugli EIO inviati o ricevuti sussiste annualmente, quando al termine dell'anno giudiziario vengono redatte dalle competenti autorità giudiziarie le relazioni sull'attività di cooperazione giudiziaria. In alcuni Stati membri l'obbligo di riferire sussiste soltanto a fronte di una precisa richiesta da parte del proprio Ministero della Giustizia.

Per quanto riguarda gli Stati membri oggetto del presente lavoro, sono quasi tutti allineati con i risultati sopra descritti, ad eccezione dell'Austria, che ha dichiarato che non vi è alcun obbligo interno in merito alla comunicazione del numero di richieste di EIO.

La seconda domanda (Q2) mira a verificare la possibilità per quegli Stati membri che hanno l’obbligo di riferire sulle richieste di EIO, di avere report statistici sull’ammontare degli EIO nel corso di un determinato anno giudiziario. Le risposte hanno dato i risultati illustrati nella Figura 3.10.

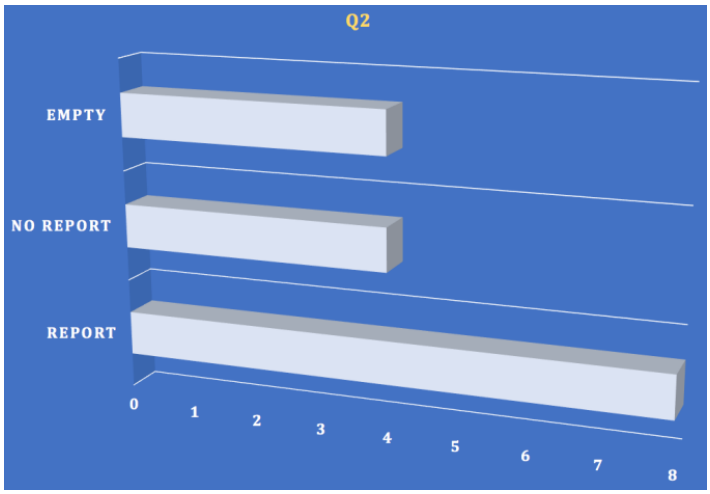

Figura 3.10: Q2, report statistici sul numero di EIO

In generale, la maggior parte degli Stati membri dichiara che esiste una possibilità generale di ottenere statistiche sull’ammontare di EIO già emessi o ricevuti.

Per quanto riguarda l’ammontare delle richieste di EIO, ricevute nell’arco dell’anno giudiziario di riferimento, l’intervallo va da un massimo di 940 ad un minimo di 23 richieste.

Per quanto riguarda l’ammontare delle richieste di EIO emesse, vanno da un massimo di 319 a un minimo di 9.

Per quanto riguarda gli Stati membri oggetto del presente lavoro sono stati forniti i seguenti numeri soltanto da due paesi:

- Spagna: dal 1 gennaio - 30 settembre 2018, sono stati ricevuti 940 EIO e 6 soltanto sono stati emessi;
- Lituania: dal 15 giugno 2017 - 31 dicembre 2017, sono stati 180 gli EIO emessi e 105 ricevuti per l’esecuzione.

La terza domanda (Q3) di questa sezione B2 riguarda il caso di quegli Stati membri in cui l’obbligo per le autorità giudiziarie locali di riferire a

un'autorità nazionale centrale sul volume di richieste di EIO emesse e ricevute non esiste formalmente (si trattava di 4 Stati membri). Pertanto, la domanda mirava ad ottenere informazioni sull'esistenza di fonti alternative per raccogliere comunque le informazioni sul numero esatto di richieste di EIO.

Tutti e 4 gli Stati hanno dichiarato di disporre di soluzioni alternative per la raccolta delle informazioni, senza tuttavia specificarne le modalità.

L'ultima domanda (Q4) si concentra sull'esistenza di database nazionali o locali per la raccolta e l'archiviazione di EIO.

La Figura 3.11 mostra che più del 50% degli Stati membri che hanno partecipato all'indagine non ha un database, né nazionale né locale. Per quanto riguarda gli Stati membri oggetto del presente lavoro, solo la Spagna, la Croazia e la Repubblica Ceca hanno dichiarato di disporre di una banca dati nazionale, mentre Austria, Lituania e Lussemburgo hanno risposto negativamente.

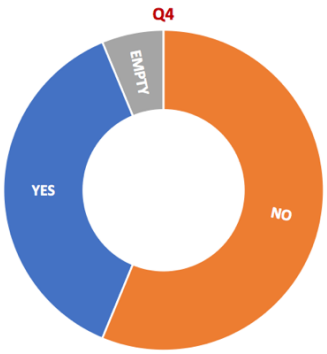

Figura 3.11: Q4, database nazionale vs. database locale

Più in dettaglio:

- Spagna: esiste un unico database nazionale in cui tutti le autorità giudiziarie regionali che sono coinvolte in una procedura di EIO introducono i dati di ciascuna richiesta. Ciò significa che le diverse autorità locali competenti in materia hanno accesso al database nazionale ed hanno la possibilità di aggiungere e aggiornare i dati;
- Croazia: è presente il sistema "eSpis" che è un sistema informativo unico per la gestione e il lavoro dell'autorità giudiziaria, utilizzato nelle varie Corti del paese;

– Repubblica Ceca: esiste un database nazionale presso il Ministero della giustizia; tuttavia esistono anche database locali ai quali ha comunque accesso l'autorità giudiziaria centralizzata.

Per quanto riguarda la specifica sezione B2, dalle informazioni raccolte possiamo affermare che un'unica barriera è emersa verso la creazione di un comune quadro giuridico in materia di EIO: mancanza di un obbligo generale per molti degli Stati membri di disporre di un meccanismo ufficiale di reporting delle richieste di EIO emesse e ricevute.

Questa barriera può essere superata da un'azione a livello nazionale di ciascuno Stato membro al fine di:

– rendere obbligatorio per le singole autorità giudiziarie locali riferire all'autorità centrale in merito al numero di EIO con una cadenza fissa (ad esempio fine dell'anno giudiziario);
– creare una banca dati nazionale per l'archiviazione dei dati relativi al numero di EIO emessi e ricevuti.

3.2.3 Analisi della sezione “B3” del questionario: l'autorità competente ad emanare l'EIO

Questa sezione mira ad acquisire informazioni sulle autorità giudiziarie di ciascuno Stato membro competenti ad emanare l'EIO. Questa sezione permette di avere una mappa nazionale degli attori coinvolti nella gestione e nel flusso di lavoro dell'EIO emesso.

Q1. Nel suo Stato chi è il soggetto che può richiedere l'emanazione di un EIO?

La prima domanda è focalizzata sull'identificazione di quei soggetti che possono richiedere l'emanazione di un EIO e che sono indicati all'art. 1, n. 3 della Direttiva 2014/41/UE[3]. Tutti gli Stati membri che hanno partecipato al questionario hanno dato una risposta precisa a questa domanda, con i risultati illustrati nella Figura 3.12.

[3]L'emissione di un EIO può essere richiesta da una persona sottoposta ad indagini o da un imputato, ovvero da un avvocato che agisce per conto di questi ultimi, nel quadro dei diritti della difesa applicabili conformemente al diritto e alla procedura penale nazionale.

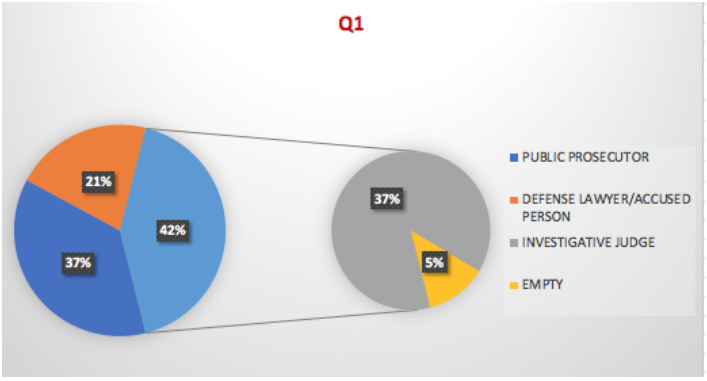

Figura 3.12: Q1, soggetti che possono richiedere un EIO

In quasi tutti gli Stati membri la situazione è molto uniforme e rispecchia il dettato dell'articolo sopra citato: le autorità giudiziarie incaricate di richiedere l'emissione di un EIO sono i pubblici ministeri, giudici inquirenti e le persone indagate o imputate, ovvero un avvocato che agisce per conto di questi ultimi. In generale, l'indagato o imputato può solo proporre l'ammissibilità di una prova nel processo, spetta poi all'autorità giudiziaria responsabile decidere sull'acquisizione.

La seconda domanda di questa sezione (Q2) si concentra sull'identificazione dell'autorità di emissione di un EIO in ciascuno Stato membro.

Q2. Nel suo Stato qual è l'autorità che è competente ad emanare un EIO?

Le risposte (Figura 3.13) hanno confermato che gli Stati membri sono abbastanza allineati anche per quanto riguarda l'identificazione dell'autorità competente ad emanare l'EIO. In alcuni Stati membri, sono riconosciute quali autorità competenti anche specifiche autorità amministrative. Pertanto, le autorità competenti ad emanare l'EIO sono i pubblici ministeri, i giudici investigativi e in alcuni paesi, come sopra specificato, anche le autorità amministrative che agiscono in qualità di "autorità investigativa" nei procedimenti penali.

Ad esempio l'Austria e la Croazia riconoscono tra le autorità competenti ad emanare l'EIO anche le autorità amministrative.

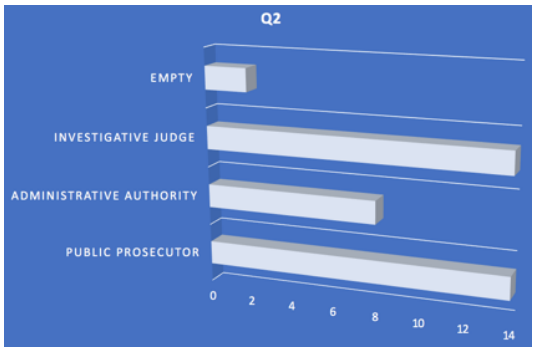

Figura 3.13: Q2, autorità di emissione dell’EIO

Le domande (Q3) e (Q4) devono essere analizzate insieme, in quanto sono complementari tra loro e limitate solo a quegli Stati membri che hanno dichiarato nella risposta precedente (Q2) che nel loro paese anche autorità amministrative specifiche hanno la competenza all’emissione di un EIO.

Q3. Nel caso sia competente anche un’autorità amministrativa, saprebbe indicare di quale autorità si tratta?

Q4. In quest’ultimo caso, prima di essere trasmesso all’autorità di esecuzione, l’EIO è convalidato? Esiste una procedura di convalida da parte di un’autorità giudiziaria? In caso affermativo, qual è l’autorità giudiziaria competente?

I risultati (Figura 3.14) mostrano che in quei paesi in cui la capacità di emanare l’EIO è assegnata a un’autorità diversa da quella giudiziaria, la maggior parte degli Stati membri ha saputo individuare l’autorità amministrativa competente, ovvero l’autorità amministrativa nazionale competente in materia di tasse e dogane. Secondo l’articolo art. 2, lett. c, ii) della Direttiva, infatti, l’autorità di emissione può essere oltre ad un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero competente nel caso interessato, anche “qualsiasi altra autorità competente, definita dallo Stato di emissione che, nel caso di specie, agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l’acquisizione di prove in conformità del diritto nazionale”.

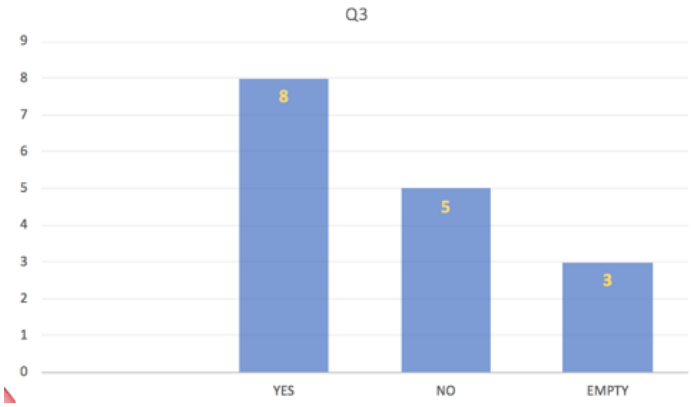

Figura 3.14: Q3, autorità amministrativa competente ad emanare EIO

Per quanto riguarda l'esistenza di una procedura di convalida della conformità dell'EIO alle condizioni previste dalla normativa, la metà degli Stati membri che hanno risposto di riconoscere la competenza ad emanare un EIO in capo ad un'autorità amministrativa, hanno escluso la necessità di una procedura di convalida (Figura 3.15). In altre parole, l'autorità amministrativa ritenuta competente può emettere direttamente l'EIO e trasmetterlo all'autorità di esecuzione senza alcuna convalida da parte dell'autorità giudiziaria.

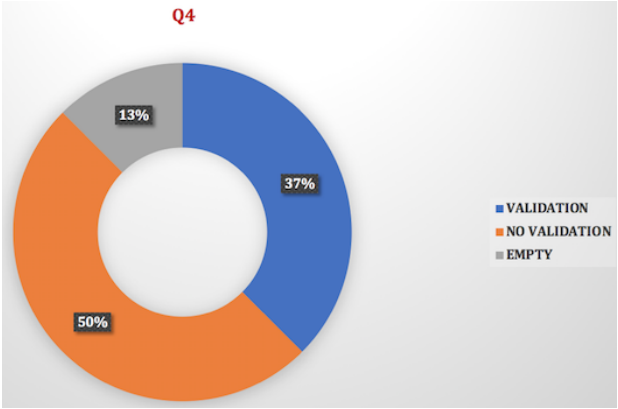

Figura 3.15: Q4, procedura di validazione

Per quanto riguarda gli Stati membri oggetto del presente lavoro, tutti sono generalmente allineati nel senso di non prevedere procedure di validazione, fatta eccezione per l’Austria. Se un’autorità amministrativa fiscale emette un EIO, il Presidente del “Bundesfinanzgericht” (tribunale fiscale federale) deve successivamente convalidarlo.

L’ultima domanda (Q5) di questa sezione è relativa alla possibilità per l’autorità di emissione di trovare in maniera semplice e veloce l’indirizzo e i riferimenti dell’autorità di esecuzione competente per l’esecuzione dell’EIO.

Q5. Esiste nel suo Stato una procedura in base alla quale l’autorità emittente può trovare l’indirizzo e i riferimenti dell’autorità competente per l’esecuzione dell’EIO? (ad es. uso di EJN Atlas, database della Corte, ecc.)

Le risposte degli Stati membri (Figura 3.16) hanno confermato che il sistema EJN-ATLAS[4] è lo strumento più comune e utilizzato per l’identificazione, in modo rapido, dell’autorità locale competente che può ricevere l’EIO ed eseguirlo (circa 60% dei partecipanti all’indagine). Alcuni Stati membri hanno inoltre dichiarato di utilizzare in alternativa a EJN-ATLAS, i punti di contatto nazionali EUROJUST (circa 15%). Solo due Stati membri utilizzano anche un terzo strumento rappresentato dalle banche dati giudiziarie locali (circa 15%).

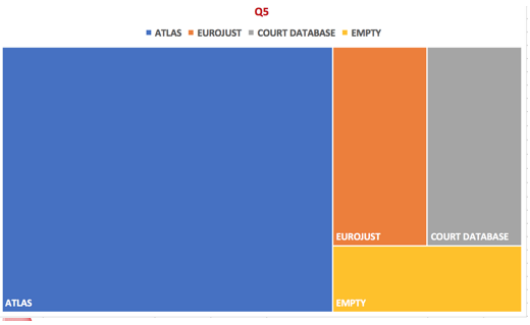

Figura 3.16: Q5, individuazione autorità di esecuzione EIO

[4]Si tratta di una banca dati di EJN che consente l’identificazione dell’autorità locale competente che può ricevere la richiesta di cooperazione giudiziaria e fornisce un canale rapido ed efficiente per la trasmissione diretta delle richieste in base alla misura selezionata (ad esempio se viene selezionato nel catalogo lo strumento EIO, si aprirà il relativo catalogo con indicazione delle autorità competenti ad emanare la richiesta per ciascuno Stato membro).

Per quanto riguarda gli Stati membri oggetto del presente lavoro, sono completamente allineati con gli altri paesi circa l'utilizzo degli strumenti per l'identificazione delle autorità di esecuzione dell'EIO.

Per quanto riguarda la specifica sezione B3, sulla base delle risposte fornite, è stata identificata una possibile barriera per la creazione di un quadro comune in materia di EIO: la scarsa chiarezza circa l'individuazione e la competenza delle autorità amministrative quando agiscono in qualità di autorità competente nell'ambito delle procedure EIO. Questa barriera può essere superata da un'azione condotta a livello nazionale dai singoli Stati membri in cooperazione con EJN-ATLAS volta a creare un database con informazioni chiare e aggiornate che permettano di identificare in modo preciso e veloce quali siano nei vari Stati membri le autorità amministrative riconosciute quali autorità competenti ad emanare un EIO.

3.2.4 Analisi della sezione "B4" del questionario: l'autorità competente ad eseguire l'EIO

La sezione B4 del questionario riguarda l'individuazione dell'autorità competente in ciascuno Stato membro per l'esecuzione dell'EIO.

La sezione consta delle seguenti domande:

Q1. Nel suo Stato qual è l'autorità competente a ricevere un EIO e ad assicurarne l'esecuzione? Riesce a identificare precisamente quale sia questa autorità?

Q2. Nel suo Stato un'autorità amministrativa o altra autorità diversa da quella giudiziaria può essere competente a eseguire un EIO?

Le risposte alle domande offrono una panoramica allineata in quasi tutti gli Stati membri, compresi quelli oggetto del presente lavoro.

In particolare, possiamo affermare analizzando le risposte, che la quasi totalità degli Stati membri che hanno partecipato all'indagine (circa 90%) ha dichiarato che i pubblici ministeri e i giudici e magistrati dei tribunali locali rappresentano l'autorità di esecuzione competente ai sensi della Direttiva 2014/41/UE. In alcuni Stati membri (37%), anche i tribunali amministrativi con competenze in materia penale possono avere competenza esecutiva, come mostrato nelle Figure 3.17 e 3.18. In questo ultimo caso tutti gli Stati membri che riconoscono la competenza di tali autorità amministrative non richiedono poi una procedura di validazione da parte dell'autorità giudiziaria, tranne l'Austria.

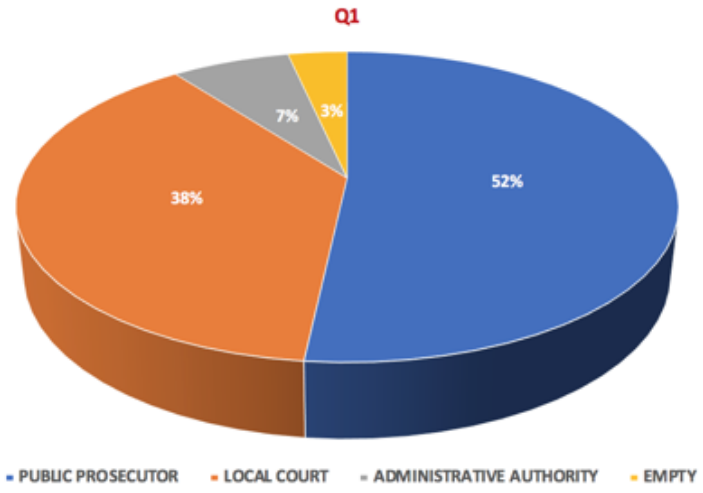

Figura 3.17: Q1, autorità competente ad eseguire l’EIO

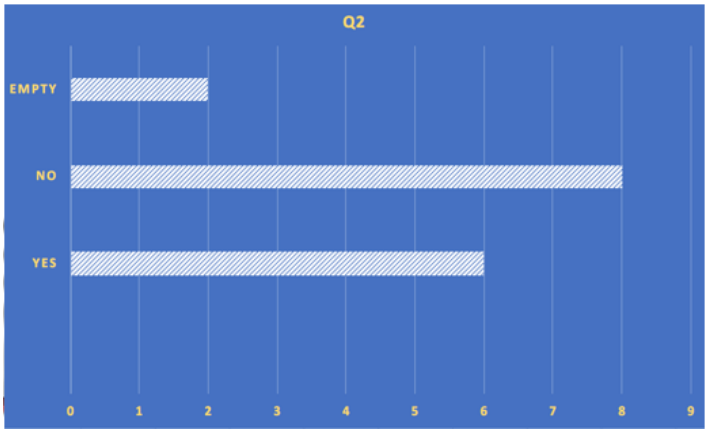

Figura 3.18: Q2, autorità amministrativa competente ad eseguire l’EIO

Per quanto riguarda la specifica sezione B4, dai risultati del questionario le barriere per l'individuazione dell'autorità di esecuzione dell'EIO sono le seguenti:

- difficoltà di identificazione dell'autorità di esecuzione da parte dell'autorità di emissione nelle fasi iniziali del processo penale, in quanto la competenza ad eseguire l'EIO non è ben identificata nei contesti domestici. Ciò è ancora più difficile in quegli Stati membri che hanno una struttura federale/distrettuale;
- obsolescenza e mancanza di granularità delle informazioni disponibili nei sistemi sovranazionali per l'identificazione delle autorità di esecuzione in ciascuno Stato membro (ad esempio indicazione dei punti di contatto nazionali in EJN-Atlas in maniera generica senza indicazione della specifica corte competente o ufficio).

Queste barriere possono essere superate da un'azione di diversi Stati membri a livello nazionale in collaborazione con EJN-ATLAS al fine di:

- fornire una comunicazione regolare agli organismi che gestiscono e aggiornano i sistemi disponibili in uso (punti di contatto nazionali EJN-Atlas) da parte di ciascuno Stato membro sull'autorità di esecuzione competente a livello nazionale;
- aggiornamento regolare dei sistemi in uso per l'individuazione dell'autorità competenze all'esecuzione dell'EIO (il riferimento è soprattutto a EJN-Atlas).

3.2.5 Analisi della sezione "B5" del questionario: modalità di trasmissione dell'EIO

Questa sezione si concentra sulla procedura e sulle modalità in uso negli Stati membri per la trasmissione delle richieste di EIO.

Q1. Come vengono trasmessi gli EIO?

Gli utenti hanno avuto la possibilità di scegliere tra 3 opzioni:

- via posta;
- per e-mail;
- qualsiasi altro canale di comunicazione.

I risultati del questionario hanno dimostrato che la modalità di trasmissione più usata è quella tradizionale, ovvero l'invio tramite posta. Alcuni Stati membri accettano anche e-mail o altri canali di comunicazione, come mostrato nella Figura 3.19.

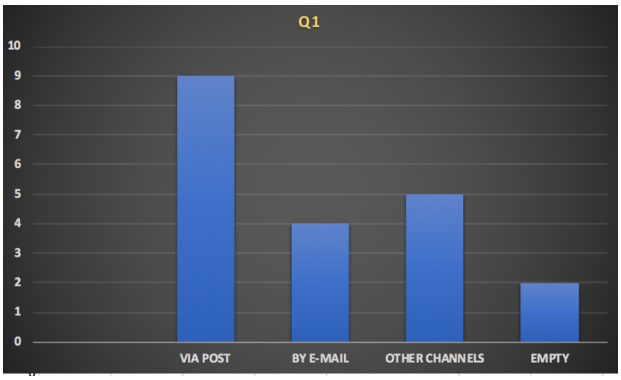

Figura 3.19: Q1, modalità di trasmissione dell’EIO

Negli Stati membri oggetto del presente lavoro, alcuni usano solo i mezzi tradizionali, ovvero posta o fax (Lituania, Croazia e Repubblica Ceca); mentre la Spagna oltre ad utilizzare i canali tradizionali ammette anche la modalità di trasmissione tramite e-mail. Infine, l’Austria utilizza anche la piattaforma implementata da e-CODEX, oltre ai normali canali tradizionali.

La seconda domanda (Q2) mira a scoprire se ci siano forme allineate ed uniformi tra i vari Stati membri in ordine alla trasmissione delle richieste di EIO.

Q2. Sono utilizzati moduli standard allineati per la trasmissione di EIO?

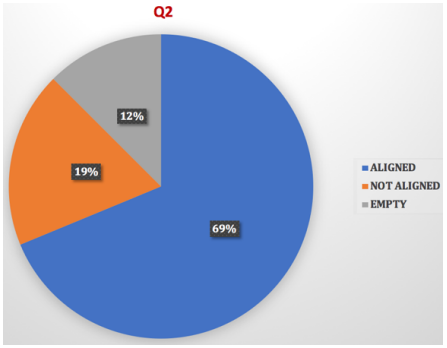

Figura 3.20: Q2, utilizzo di moduli standard per trasmissione EIO

La Figura 3.20 conferma che la maggioranza degli Stati membri utilizza delle “forms” standard per la trasmissione dell’EIO.

Q3. Usi qualche strumento automatizzato per le traduzioni di EIO? In caso contrario, puoi descrivere il metodo di traduzione?

Alla terza domanda della sezione, sull'esistenza di strumenti automatizzati per la traduzione delle richieste di EIO, la maggioranza degli Stati membri ha risposto in modo negativo. Alla base della scelta di non utilizzare strumenti di tale genere è la scarsa fiducia che gli Stati hanno verso queste tecnologie automatizzate, ritenendole non affidabili e quindi in generale non utilizzate dalle autorità competenti in materia. Solo l'Italia ha dichiarato l'esistenza di alcuni strumenti automatizzati per la traduzione.

Gli altri Stati membri hanno dichiarato che, se necessario, la traduzione è assegnata a società di traduzione private che però sono autorizzate dal Ministero di Giustizia del singolo paese.

Q4. Sono riscontrate particolari difficoltà nella procedura di trasmissione di EIO?

Le risposte, riportate in Figura 3.21, erano quasi totalmente negative, il che significa che le autorità competenti degli Stati membri che hanno partecipato al questionario affermano di non affrontare difficoltà durante la procedura di trasmissione di EIO.

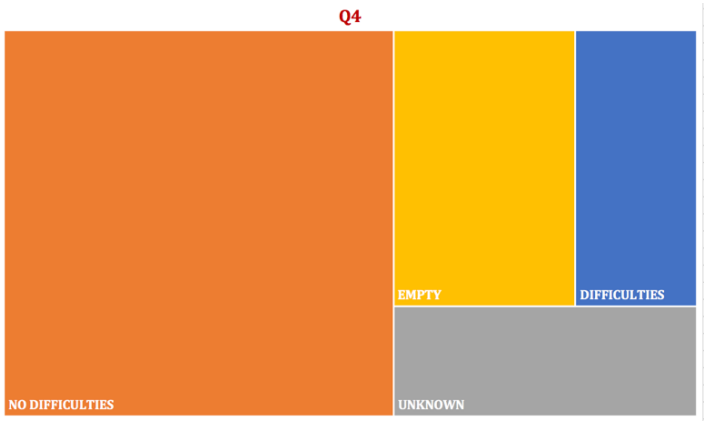

Figura 3.21: Q4, difficoltà nella procedura di trasmissione di EIO

Gli Stati membri oggetto dell'indagine sono quasi tutti allineati con i risultati mostrati, dichiarando di non avere difficoltà nella trasmissione. Unica eccezione è rappresentata dalla Spagna che ha dichiarato che i ritardi e com-

plessità legati alla trasmissione di prove digitali o file di grandi dimensioni potrebbero costituire un ostacolo all'efficacia e speditezza della procedura.

La domanda successiva (Q5) mira ad indagare la situazione qualora ad essere trasmessi siano file di grandi dimensioni.

Q5. Ha trovato qualche difficoltà in caso di trasmissione di file di grandi dimensioni?

Più specificamente, agli Stati membri è stato anche chiesto di sottolineare se la trasmissione di file di grandi dimensioni rappresenti una possibile barriera nella procedura. I risultati (Figura 3.22) mostrano che in alcuni paesi questa difficoltà è già emersa e sentita come incidente negativamente sulla procedura: infatti, molto spesso il file di grandi dimensioni deve essere inviato in porzioni e a più riprese, causando possibili ritardi. Tuttavia, nella maggior parte dei casi il problema dei file di grandi dimensioni non è ancora sentito come tale.

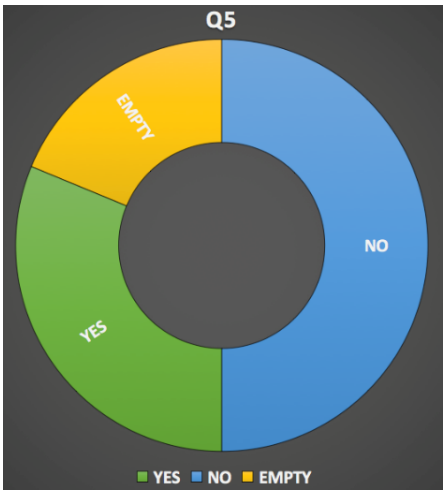

Figura 3.22: Q5, problematicità dei file di larghe dimensioni

Per quanto riguarda gli Stati membri oggetto del presente lavoro, soltanto la Lituania e la Spagna hanno dichiarato di aver affrontato difficoltà in caso di trasmissione di file di larghe dimensioni dovuto alla impossibilità di inviare tali file attraverso lo strumento da loro utilizzato, ovvero via e-mail.

Le domande (Q6) e (Q7) di questa sezione devono essere considerate unitariamente, in quanto si riferiscono entrambe ad ottenere informazioni

circa il livello di collaborazione tra autorità dei diversi Stati membri nel corso della procedura di esecuzione dell'EIO.

In particolare,

Q6. È a conoscenza di collaborazioni e contatti tra autorità nazionali/-locali degli Stati membri durante l'esecuzione di un EIO?

Q7. In caso affermativo, ha conoscenza di particolari difficoltà nello stabilire contatti e collaborazioni durante la procedura di esecuzione dell'EIO?

I risultati hanno mostrato (Figure 3.23 e 3.24) che quasi tutti gli Stati membri interagiscono attivamente durante l'esecuzione di un EIO, tuttavia non esistono canali ufficiali, ma le varie forme di collaborazione e le modalità in cui avvengono sono lasciate all'iniziativa del singolo paese. Gli Stati membri, come dimostrato dalle risposte al questionario, ritengono che questa possibilità di dialogo sia utile prima di emettere l'EIO o durante l'esecuzione dell'EIO al fine di comprendere meglio, ad esempio, i requisiti richiesti dalle disposizioni nazionali nello Stato di emissione o di esecuzione, o al fine di accordarsi in caso di necessità di azioni urgenti. Solo alcuni degli Stati membri oggetto del presente lavoro (Austria, Croazia e Repubblica Ceca) hanno dichiarato di non interagire durante l'esecuzione di un EIO.

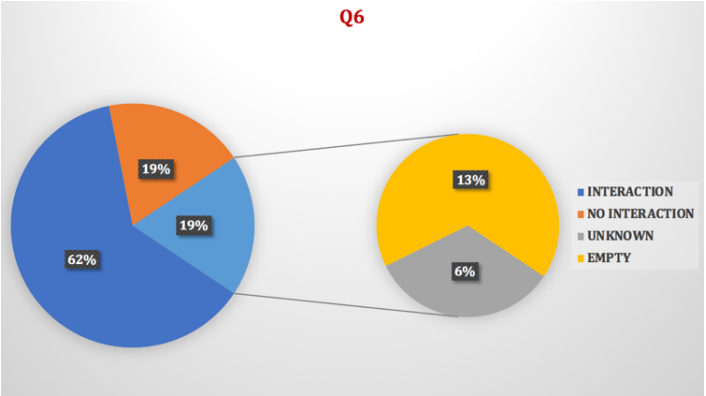

Figura 3.23: Q6, forme di collaborazione tra Stati durante esecuzione EIO

La domanda (Q7) mira ad ottenere informazioni più dettagliate sulle modalità di collaborazione tra Stati membri, in particolare sulle possibili difficoltà incontrate nel corso della loro collaborazione in caso di esecuzione dell'EIO.

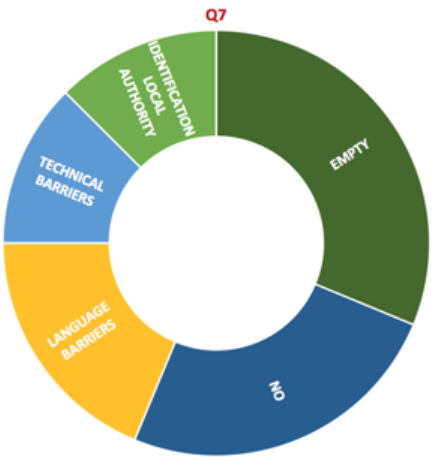

Figura 3.24: Q7, tipologia di difficoltà incontrate dagli Stati membri

Le difficoltà che si sono riscontrate in tutti gli Stati membri che hanno partecipato all’indagine, sono state principalmente:

- barriere linguistiche: in quanto manca in generale tra le autorità dei singoli Stati membri competenti in materia di EIO una buona padronanza della lingua inglese (che potrebbe essere considerata quale lingua comune di riferimento);
- barriere tecniche, poiché gli strumenti a supporto dell’identificazione dei punti di contatto locali (con indicazione delle autorità locali competenti in materia) non sono sempre aggiornati con le informazioni necessarie (es. EJN-ATLAS).

Per quanto riguarda la specifica sezione B5, sulle modalità di trasmissione dell’EIO, gli ostacoli che sono stati individuati dagli Stati membri sono i seguenti:

- modalità di trasmissione prevalentemente tradizionale (posta e fax), con le possibili conseguenze negative in caso di trasmissione di file di larghe dimensioni;
- mancanza di reti di collaborazione stabile, ufficiale e strutturata tra le autorità competenti durante l’esecuzione degli EIO.

Queste barriere possono essere facilmente superate da un’azione a livello nazionale dei diversi Stati membri supportati dalle iniziative progettuali europee volte all’adozione di strumenti avanzati e uniformi per il trat-

tamento e scambio delle prove digitali (si pensi ad esempio al progetto Evidence2e-CODEX oppure EXEC).

In particolare; tali azioni dovrebbero mirare a:

- adottare strumenti elettronici quali la posta elettronica laddove la trasmissione sia solo via posta tradizionale o via fax, oppure implementare in ciascuno Stato membro l'uso della piattaforma sicura e affidabile e-CODEX;
- migliorare il dialogo tra le autorità durante l'esecuzione dell'EIO anche laddove questo dialogo esista ma non sia strutturato stabilmente e in maniera uniforme.

3.2.6 Analisi della sezione "B6" del questionario: cooperazione tra Stato membro e ISP nell'acquisizione di dati

Questa sezione mira principalmente ad avere un quadro completo per comprendere lo "status quo" della cooperazione in Europa tra le autorità competenti in materia di EIO e gli ISPs. Si tratta di una sezione molto importante, in quanto in molti casi sono proprio gli ISPs che detengono informazioni utilizzabili come prove nei processi penali.

Le prime domande erano le seguenti:

Q1. Esiste nel suo Stato qualche procedura di cooperazione con l'ISP in caso di EIO?

Q2. In caso affermativo, che tipo di dati copre la richiesta dell'EIO?

I risultati (Figura 3.25) mostrano che in realtà la maggioranza degli Stati membri che hanno partecipato all'indagine, non hanno relazioni regolari ed istituzionalizzate/ufficializzate con gli ISPs poiché la maggior parte delle risposte alla domanda (Q1) è stata negativa. In altre parole, i risultati hanno dimostrato che non esistono procedure standardizzate di collaborazione. Gli Stati membri oggetto specifico del presente lavoro sono tutti allineati allo scenario rappresentato.

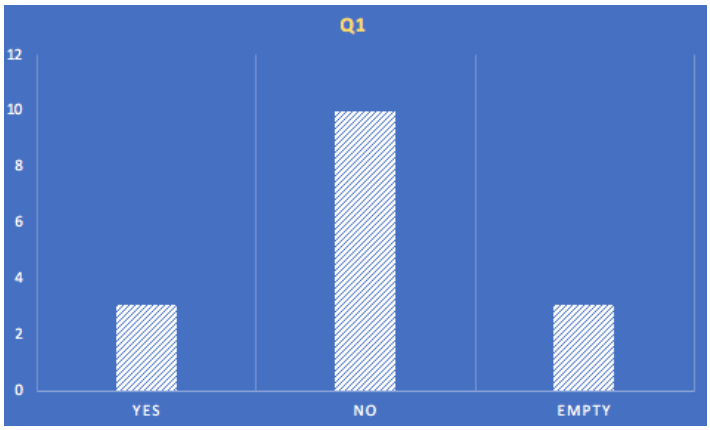

Figura 3.25: Q1, esistenza di forme di collaborazione con ISP

Per quanto riguarda la domanda (Q2) sul tipo di dati che le autorità degli Stati membri effettivamente richiedono agli ISPs, i risultati (Figura 3.26) hanno mostrano che la situazione è molto equilibrata, poiché i tre tipi di dati indicati (dati relativi agli abbonati, metadati e dati di contenuto) sono quasi sempre richiesti insieme da tutti i paesi partecipanti all’indagine.

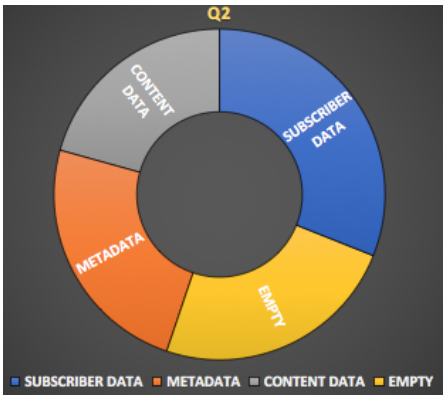

Figura 3.26: Q2, tipologia di dati richiesti all’ISP

La seconda serie di domande (Q3) e (Q4) mira a capire in che modo gli Stati membri comunicano con gli ISPs.

Q3. Se è necessario acquisire dati dall'ISP:
invia direttamente la sua richiesta all'ISP?
utilizza l'EIO?

I risultati (Figura 3.27) hanno mostrano che la maggior parte degli Stati membri utilizza l'EIO (tra questi tutti i paesi oggetto della presente indagine) per richiedere dati agli ISPs. In particolare circa il 45% di coloro che hanno risposto al questionario dichiara di utilizzare l'EIO, mentre il 20% invia la richiesta direttamente all'ISP.

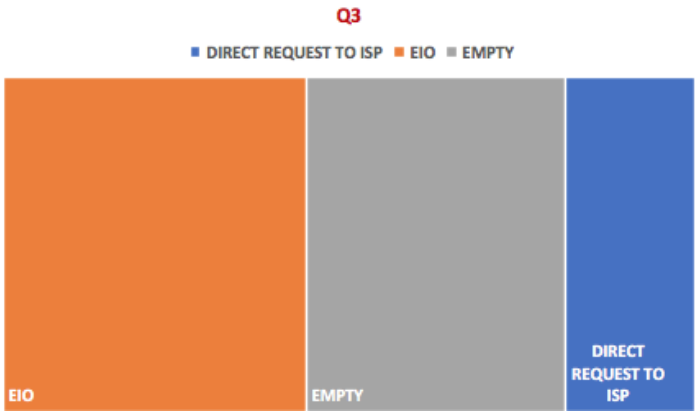

Figura 3.27: Q3, modalità di richiesta a ISP

Per quanto riguarda la domanda (Q4), l'obiettivo era capire in quale forma venisse inoltrata la richiesta all'ISP, se fosse utilizzato un modello standard o si trattasse di una richiesta a testo libero.

Q4. Ha un modulo standard per tale richiesta?

Le risposte (Figura 3.28) hanno dimostrano che l'opzione per la richiesta a testo libero sia la più utilizzata, anche se alcuni Stati membri dichiarano di aver adottato un modello standard (ovvero il modello dell'EIO per quegli Stati che hanno dichiarato di usare tale strumento).

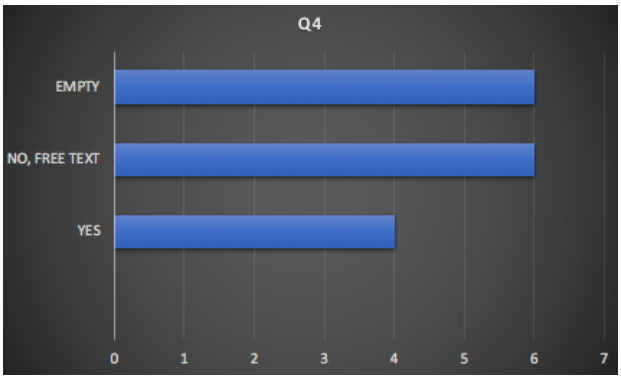

Figura 3.28: Q4, forma della richiesta dati all’ISP

Andando più nel dettaglio sulla modalità di cooperazione tra autorità competente e ISP, la domanda (Q5) indaga se la risposta dell’ISP possa essere considerata rapida o, in caso contrario, se l’ISP dia una motivazione per il ritardo nella risposta.

Q5. Di solito la risposta da parte dell’ISP può essere considerata rapida? In caso contrario, l’ISP usa motivare il ritardo?

I risultati (Figura 3.29) mostrano che gli ISPs sono molto attivi nella risposta alle richieste delle autorità nazionali (il risultato migliore è un tempo medio di 2-6 ore per la risposta se la richiesta è molto urgente). Inoltre, qualora la risposta sia tardiva, l’ISP in generale provvede a fornire una motivazione.

Figura 3.29: Q5, rapidità e motivazione nella risposta dell’ISP

Infine, le domande (Q6) e (Q7) si riferiscono al modo in cui i dati richiesti sono trasferiti alle autorità richiedenti dall'ISP e quale sia il formato più comune del file inviato.

Q6. In che modo l'ISP trasferisce i dati richiesti?

Q7. In quale formato? (L'ISP trasferisce i dati richiesti)

I risultati (Figura 3.30) della domanda (Q6) hanno rivelato che in generale gli ISPs trasmettono i dati via e-mail all'autorità richiedente. In alcuni casi, gli Stati membri hanno indicato come mezzo di trasmissione quello elettronico, senza specificare quale sia lo strumento specifico. Gli Stati membri che hanno dichiarato di utilizzare opzioni diverse rispetto alle precedenti, non hanno poi specificato quale sia effettivamente il mezzo usato, si potrebbe ipotizzare che lo strumento utilizzato sia quello tradizionale (fax, posta, corriere).

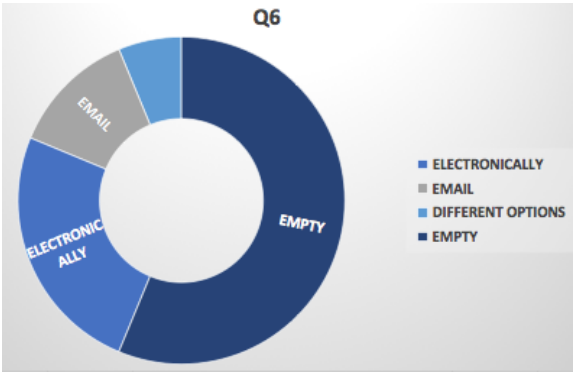

Figura 3.30: Q6, modalità di trasferimento dei dati da parte dell'ISP

Solo due Stati membri tra quelli oggetto del presente lavoro (Croazia e Lituania) hanno risposto a questa domanda, specificando di ricevere le informazioni richieste dall'ISP per via elettronica.

Per quanto riguarda il formato utilizzato per comunicare i dati, dai risultati della domanda (Q7) (Figura 3.31) si può affermare che lo scenario europeo non è armonizzato, in quanto tutti i formati indicati come possibili sono utilizzati: da pdf a word. Nel caso in cui alla domanda è stato risposto di utilizzare un formato diverso da word, excel o pdf, poi non è stato specificato di che formato si tratti.

Per quanto riguarda la specifica sezione B6 le barriere individuate nella cooperazione tra ISP e autorità competenti degli Stati membri sono:

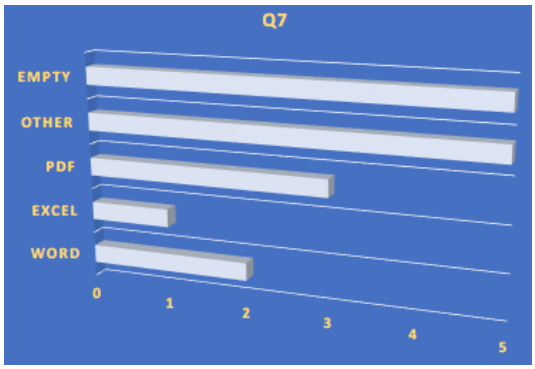

Figura 3.31: Q7, formati utilizzati per la trasmissione dati da parte ISP

- mancanza di relazioni istituzionalizzate e regolari tra Stati membri e ISP;
- utilizzo frammentato di diversi strumenti giuridici per la richiesta di informazioni agli ISPs anche a causa della mancanza di un quadro giuridico comune dell’UE (richieste a testo libero direttamente all’ISP, EIO);
- diversità di modelli e moduli utilizzati per la richiesta di dati dal momento che manca un “template” comune;
- utilizzo di diversi mezzi di trasmissione delle richieste e diversi formati dei dati comunicati.

Questi ostacoli possono essere superati da un’azione a livello dell’Unione che miri a finanziare nuovi progetti in collaborazione anche con gli ISPs, progetti finalizzati a:

- creare un framework comune e standardizzato di collaborazione tra autorità competenti degli Stati membri e gli ISPs, al fine di facilitare il flusso di richieste e la consegna dei dati detenuti dagli stessi ISPs;
- elaborare linee guida uniformi sugli strumenti giuridici da utilizzare per richiedere dati agli ISPs da parte degli Stati membri dell’UE;
- creare un modello comune e uniforme per la richiesta di dati che gli Stati membri devono utilizzare per ottenere informazioni all’ISP;
- adottare uno standard formale comune da utilizzare per il confezionamento dei dati e la loro trasmissione elettronica.

3.2.7 Analisi della sezione "B7" del questionario: EIO e strumenti internazionali di lotta alla criminalità informatica

Questa sezione mira a comprendere le relazioni tra l'EIO e la Convenzione di Budapest nei vari Stati membri che partecipano all'indagine.

La Convenzione di Budapest è stata adottata nel 2001 dal Consiglio d'Europa in materia di criminalità informatica[5].

Il Consiglio d'Europa, organizzazione internazionale fondata nel 1949 con sede a Strasburgo, ha quale obiettivo fondamentale quello di assicurare il rispetto di tre principi fondamentali: la democrazia pluralista, il rispetto dei diritti umani e l'identità culturale europea, tentando di dare soluzioni concrete ai problemi sociali in Europa. Per realizzare tali obiettivi il Consiglio d'Europa mira ad assicurare una più ampia e solida unità tra i suoi membri, nella convinzione che solo attraverso una stretta cooperazione internazionale sia possibile garantire adeguata protezione alla società stessa.

Lo strumento principale d'azione del Consiglio d'Europa consiste, infatti, nel predisporre e favorire la stipulazione di accordi o convenzioni internazionali tra gli Stati membri (ed anche con Stati terzi), che costituiscono la base per l'armonizzazione delle legislazioni negli Stati medesimi.

Ed è stata proprio la necessità di una tale armonizzazione che ha determinato l'adozione da parte del Consiglio d'Europa della Convenzione di Budapest.

Negli ultimi decenni, infatti, lo sviluppo delle tecnologie informatiche, oltre ad aver aperto la strada a nuove opportunità lavorative e di comunicazione, ha anche determinato un aumento vertiginoso dei crimini commessi attraverso l'utilizzo di strumenti informatici e delle reti di comunicazione. Incremento a cui non è corrisposta, in molti Stati, un'adeguata criminalizzazione delle diverse e nuove fattispecie criminose; a questo problema si aggiunge quello per cui ogni Paese ha la propria legislazione in materia di criminalità informatica e, quindi, in materia di raccolta, trattamento e utilizzo delle prove digitali che possono essere rilevanti in qualsiasi tipo di reato (anche non informatico). La legislazione nazionale si basa sulla territorialità,

[5]Per la versione inglese della Convenzione si veda www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; il testo non ufficiale in italiano tradotto dal Dr. Giovanni Ilarda e dal dr. Giovanni Pasqua è reperibile al seguente indirizzo www.intertraders.eu/diritto/convenzioni/Budapest_2001.pdf.

mentre quando si tratta di criminalità informatica (sia che si tratti di reati informatici veri e propri sia di reati comuni commessi attraverso strumenti informatici ovvero di reati per i quali le prove digitali diventano rilevanti), spesso si travalicano i confini nazionali.

Un altro problema da affrontare in materia di criminalità informatica ha sicuramente riguardato la difficoltà di effettuare le attività investigative in maniera uniforme nei vari Paesi e, molto spesso, si è assistito al rischio che l'acquisizione e la conservazione di dati digitali possano risultare non corrette, non soltanto per la difficoltà nella raccolta stessa ma anche per la possibilità che nei vari Paesi possano essere adottati procedure e standards disomogenei. In altre parole, i diversi Paesi possono presentare discipline diverse in materia di attività investigative e possono presentare anche sostanziali differenze circa l'utilizzo delle tecnologie per la raccolta e conservazione delle prove digitali connesse alle varie tipologie di reati.

I problemi sopra indicati, unitamente ai continui sviluppi e ampio uso della tecnologia informatica, hanno dato luogo a specifiche necessità di condurre attività di investigazione in modo più efficace ed hanno aumentato la pressione nei confronti dei sistemi penali nazionali affinché venissero adottati strumenti e procedure uniformi nella gestione dei crimini informatici e dei dati digitali connessi a tali reati, ovvero connessi a reati comuni commessi attraverso strumenti informatici. La Convenzione di Budapest mira, appunto, a realizzare una politica comune finalizzata non soltanto alla protezione contro la criminalità informatica ma anche alla prevenzione della stessa, attraverso l'adozione di una legislazione comune in materia ed incentivando/incoraggiando la cooperazione internazionale. Si tratta dell'unica convenzione internazionale vincolante in materia di crimini informatici e di prove digitali connesse a qualsiasi tipo di reati (il riferimento, come già sopra indicato, è ai reati informatici propriamente detti, ai reati comuni commessi attraverso l'utilizzo di strumenti informatici, ovvero reati nei quali le prove digitali siano rilevanti), il cui obiettivo principale è stato proprio quello di indurre i Paesi che l'hanno ratificata ad adeguare i rispettivi diritti penali sostanziali e procedurali alle disposizioni indicate nella Convenzione medesima. In altre parole, la Convenzione stabilisce che ciascuno Stato che l'abbia ratificata provveda a tipizzare una serie di offese legate all'utilizzo di strumenti informatici o di Internet, rispetto alle quali sono previsti poteri processuali necessari ai fini delle indagini e del perseguimento di tali reati ovvero ai fini della raccolta, acquisizione e conservazione delle prove digitali connesse.

A tale proposito la Sezione I del Capitolo II prevede, a livello di diritto penale sostanziale, una serie di misure che devono essere adottate a livello nazionale dai vari Stati membri della Convenzione al fine di prevenire e reprimere in modo efficace la criminalità informatica attraverso la definizione di uno standard minimo di offese. In particolare, la Sezione è divisa in cinque titoli: nel primo titolo sono inclusi tutti quei reati contro la riservatezza, integrità e la disponibilità dei dati informatici e dei sistemi informatici[6]; mentre nei titoli due e tre vengono incluse tutte quelle fattispecie criminose in cui gli strumenti informatici e Internet sono utilizzati come mezzi per attaccare determinati interessi giuridici già oggetto di protezione da parte dell'ordinamento. Infine, il titolo IV disciplina i reati contro la proprietà intellettuale ed i diritti collegati, mentre il titolo V disciplina altre forme di responsabilità e le relative sanzioni (tentativo e complicità nella commissione di un reato, e responsabilità delle persone giuridiche).

A livello procedurale, nella sezione II del capitolo II della Convenzione sono previste alcune misure e poteri in capo alle competenti autorità nazionali ai fini delle indagini penali, per i reati indicati nella Sezione I della Convenzione medesima, per altri reati commessi attraverso l'utilizzo di strumenti informatici e di comunicazione e per la raccolta di tutte le prove in formato digitale connesse a qualsiasi tipo di reato. Da un lato, la Convenzione adatta tradizionali misure procedurali, quali la ricerca e il sequestro, al nuovo ambiente tecnologico; dall'altro lato, sono state create nuove misure (relative ad esempio alla rapida preservazione/conservazione di dati informatici immagazzinati/conservati attraverso un sistema informatico ed alla raccolta in tempo reale di dati informatici) grazie alle quali è possibile ovviare alla volatilità dei dati digitali connessi ai vari tipi di offese commesse attraverso l'utilizzo di computer o di Internet[7].

[6]In particolare l'art. 2 della *Convenzione di Budapest* disciplina le ipotesi di accesso illegale ad un sistema informatico, l'art. 3 le ipotesi di intercettazioni abusive, gli artt. 4 e 5 le ipotesi di attentati all'integrità dei dati; mentre l'art. 6 individua le ipotesi di abuso di apparecchiature qualora la fabbricazione, la vendita, l'approvvigionamento per l'uso, la distribuzione o qualsiasi altro tipo di utilizzazione di tali apparecchiature sia effettuata con lo scopo di commettere un reato.

[7]Si vedano in particolare gli artt. da 16 a 21 della *Convenzione sulla criminalità informatica* relativi alla preservazione rapida di dati informatici conservati attraverso strumenti informatici, perquisizione e sequestro di dati informatici conservati infine raccolta in tempo reale di dati informatici.

Infine, la Convenzione stabilisce alcuni principi fondamentali in materia di cooperazione internazionale e mutua assistenza prevedendo, in tal senso, uno sforzo il più ampio possibile per gli Stati membri: non soltanto nell'ambito delle indagini o dei procedimenti relativi a crimini informatici definiti dalla Convenzione stessa, ma anche con riferimento alla raccolta delle prove, naturalmente in formato digitale, connesse a qualsiasi tipo di reato.

La Convenzione, quindi, rappresenta il primo strumento multilaterale contro la criminalità informatica che richiede alle parti contraenti di reprimere certe condotte illecite e di adoperarsi per adottare misure adeguate ed omogenee che favoriscano la cooperazione fra Stati, sia per quanto riguarda le indagini penali, sia per quanto riguarda la repressione dei reati.

Ma, soprattutto, richiede che tale uniformità riguardi anche la raccolta e conservazione delle prove digitali non solo nel caso in cui si persegua un crimine informatico ma anche nell'ipotesi di qualsiasi tipo di reato in cui tali tipi di prove siano rilevanti.

In questo contesto, si comprende molto bene come sia stato importante per l'indagine condotta nel presente lavoro, individuare il rapporto tra l'applicazione della Convenzione e l'utilizzo dell'EIO negli Stati membri.

In particolare, il primo gruppo di domande della sezione è il seguente:

Q1. Il suo Stato ha ratificato la Convenzione di Budapest?

Q2. L'articolo 29 della Convenzione di Budapest regola la “conservazione rapida dei dati informatici memorizzati”. L'Articolo 32 dell'EIO regola la conservazione delle prove elettroniche. Come si applicano questi due strumenti in pratica nel suo Stato?

Q3. Il suo Stato ha provveduto a notificare alla Commissione l'uso della convenzione di Budapest (ai sensi dell'articolo 34, paragrafi 3 e 4, della direttiva EIO)?

La prima domanda di questa sezione (Q1) fornisce una panoramica sullo “status quo” dell'attuazione della Convenzione di Budapest negli Stati membri dell'UE coinvolti in questo sondaggio.

I risultati (Figura 3.32) dimostrano che quasi tutti gli Stati membri che hanno partecipato al sondaggio hanno firmato e attuato la Convenzione, e questo vale sicuramente per quei Paesi che sono oggetto specifico del presente lavoro.

Figura 3.32: Q1, ratifica della Convenzione di Budapest

La seconda domanda (Q2) indaga il rapporto tra gli strumenti forniti rispettivamente dalla Convenzione e dalla Direttiva sull'EIO per la conservazione delle prove elettroniche e, in particolare, su come tali strumenti interagiscono reciprocamente nella pratica.

Gli Stati membri in generale hanno dichiarato che i due strumenti sono entrambi utilizzati tenendo conto delle circostanze particolari del caso e anche delle esigenze di speditezza della procedura: in questo caso, gli Stati membri hanno tutti confermato l'utilizzo dell'EIO.

La domanda (Q3) ha chiesto agli Stati membri di indicare se, di solito, notificano l'uso della Convenzione di Budapest alla Commissione europea, ai sensi dell'art. 34 par. 3 e 4 della Direttiva EIO.

Gli Stati membri hanno dichiarato (Figura 3.33) che in realtà non hanno provveduto a notificare tale uso alla Commissione.

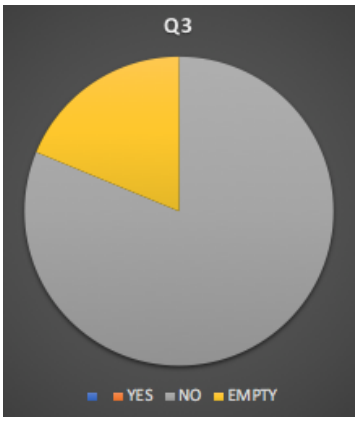

Figura 3.33: Q2, notifica Convenzione art. 34 par. 3 Direttiva EIO

Gli Stati membri oggetto del presente lavoro sono allineati a questi risultati, salvo la Repubblica Ceca che non ha fornito risposta.

Gli Stati membri in generale hanno specificato che la Convenzione di Budapest rappresenta la base giuridica per la richiesta di conservazione dei dati informatici quando uno dei paesi firmatari non è uno Stato membro dell’UE; mentre la cooperazione tra gli Stati membri dell’UE in materia di conservazione, acquisizione e raccolta di prove è regolata dall’EIO. Sembra che l’EIO acceleri la procedura di trasmissione.

I risultati del questionario non hanno evidenziato ostacoli, forse anche a causa del fatto che la Convenzione di Budapest è in vigore da molti anni e il suo raggio d’azione è diventato ormai abbastanza chiaro.

3.2.8 Analisi della sezione “B8” del questionario: la lingua dell’EIO

Questa sezione mira a comprendere quale lingua, tra quelle ufficiali dell’UE può essere utilizzata in aggiunta alla lingua ufficiale di ciascuno Stato membro per completare o tradurre l’EIO quando tale Stato membro è lo Stato di esecuzione. Ai sensi dell’art. 5 par. 3 della Direttiva 2014/41/UE, l’autorità competente dello Stato di emissione traduce l’EIO in una delle lingue ufficiali dello Stato di esecuzione o in una qualsiasi altra lingua o lingue ufficiali delle Istituzioni dell’UE indicata dallo Stato di esecuzione stesso.

Q1. Il suo Stato ha notificato una seconda lingua per l’EIO?

Le risposte alla domanda (Q1) di questa sezione (Figura 3.34) mostrano che quasi tutti gli Stati membri che hanno partecipato all'indagine hanno notificato una seconda lingua per l'EIO (10), insieme alla loro lingua ufficiale nazionale. Solo 6 Stati membri dichiarano di non aver notificato una seconda lingua per l'EIO (tra questi Spagna, Croazia e Repubblica Ceca).

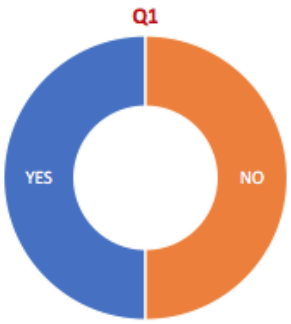

Figura 3.34: Q1, notificazione di una lingua diversa dalla nazionale

Per quanto riguarda gli Stati membri oggetto specifico del presente lavoro, la scelta della seconda o di più lingue in cui può essere completato o tradotto l'EIO è stata la seguente:

- l'Austria accetta qualsiasi altra lingua ufficiale degli Stati membri dell'UE sulla base di accordi bilaterali, mentre non è richiesta alcuna traduzione in relazione alle lingue ufficiali di Repubblica Ceca, Francia, Ungheria, Italia, Polonia e Slovacchia;
- la Croazia non accetta nessuna altra lingua tranne quella ufficiale nazionale, pertanto l'EIO dovrebbe essere tradotto in croato. Tuttavia, in casi urgenti in generale è accettata una traduzione in inglese dell'EIO;
- in Repubblica Ceca è accettato solo il ceco e lo slovacco. Anche in questo Stato in caso di urgenza è comunque accettata una traduzione in inglese dell'EIO;
- in Lituania viene identificata la lingua inglese come seconda lingua ufficiale in cui può essere completato e tradotto l'EIO;
- il Lussemburgo accetta la lingua inglese e francese;
- la Spagna accetta solo la lingua ufficiale nazionale. Anche in questo Stato in caso di urgenza è comunque accettata una traduzione in inglese dell'EIO.

Andando più in dettaglio sull’analisi della lingua dell’EIO, agli Stati membri è stata posta la seguente domanda (Q2):

Q2. Se il suo Stato che agisce come Stato di esecuzione ha indicato di utilizzare solo la propria lingua nazionale per l’EIO, ciò potrebbe rappresentare un ostacolo in casi urgenti?

I risultati (Figura 3.35) di questa domanda hanno rivelato che in generale la mancanza della indicazione della seconda lingua o di altre ufficiali da parte dello Stato di esecuzione è percepito come un problema dovuto soprattutto alla difficoltà a reperire traduttori ufficiali e ai ritardi nelle procedure di traduzione.

Tutti gli Stati membri che hanno risposto di aver notificato solo la lingua ufficiale nazionale per l’EIO, dichiarano comunque che si tratta di un ostacolo superabile in caso di urgenza in quanto tutti ammettono una traduzione in inglese dell’EIO.

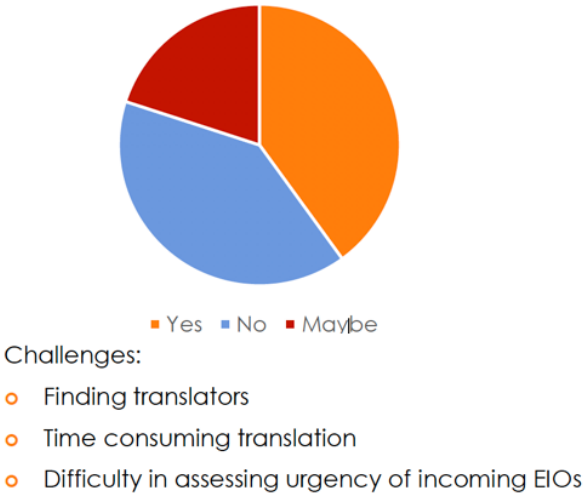

Figura 3.35: Q2, notificazione della sola lingua nazionale dello Stato di esecuzione

Per quanto riguarda la specifica sezione B8 le barriere che sono emerse dalle risposte alle domande sono le seguenti:

– mancanza di una lingua pivot esistente che consenta uno scambio e una comprensione rapidi delle richieste;

- mancanza di traduttori ufficiali pronti a tradurre la richiesta in modo rapido;
- mancanza di fiducia, accettazione e utilizzo di strumenti automatici per la traduzione.

Queste barriere possono essere superate da un'azione di ciascuno degli Stati membri a livello nazionale in collaborazione con le azioni progettuali della Commissione al fine di:

- individuare come obbligatoria una seconda lingua comune da utilizzare in tutti gli Stati membri;
- individuare e formare un elenco di traduttori ufficiali a livello nazionale anche mediante la rete di traduttori legali che lavorano a livello europeo (come quelli di OPOCE[8] o Eur-Lex[9]);
- creare strumenti automatizzati affidabili e mirati per la traduzione di EIO anche riutilizzando risorse già esistenti come lo strumento automatico Eur-Lex per la traduzione della legislazione nazionale.

3.2.9 Analisi della sezione D del questionario: il training per le autorità giudiziarie competenti in materia di EIO

Un'accurata e specifica formazione professionale non può che rappresentare una delle migliori garanzie per gli addetti alla giustizia, in grado di assicurare, da un lato, un'adeguata tutela dei diritti dei soggetti coinvolti e, dall'altro, anche una corretta applicazione della normativa europea.

Non solo: per gli stessi addetti (magistrati, giudici e pubblici ministeri) una formazione professionale mirata e "su misura" rappresenta una delle migliori garanzie in grado di assicurarne una forma d'autonomia fondamentale: ovvero l'indipendenza dall'ignoranza.

Il possesso di una buona cultura giuridica e, prima ancora, di una buona cultura generale possono costituire un requisito essenziale ed indispensabile perché chi è istituzionalmente chiamato ad avere un ruolo fondamentale nel

[8]Si tratta dell'ufficio pubblicazioni dell'Unione europea, che si occupa di pubblicare multilingue una serie di documenti ufficiali. Si veda https://op.europa.eu/en/web/general-publications/publications.

[9]Eur-Lex è un sito web dell'Unione europea che offre la consultazione online gratuita di tutti i testi di legge dell'UE, ed inoltre pubblica la Gazzetta Ufficiale. Si veda https://eur-lex.europa.eu/.

settore giudiziario possa svolgere correttamente ed in maniera credibile la propria missione.

L’Europa, attraverso le sue iniziative e azioni, ha mostrato grande interesse per il tema della formazione professionale, e in particolare per la formazione nel settore giudiziario. La formazione giudiziaria è fondamentale per rafforzare la fiducia reciproca e migliorare la cooperazione tra autorità e operatori giudiziari nei vari Stati membri e deve essere considerata un elemento essenziale nella promozione di un’autentica cultura giudiziaria europea.

Il Trattato di Amsterdam, che all’art. 1 pone quale obiettivo fondamentale dell’Unione europea quello di creare uno «spazio di libertà, sicurezza e giustizia», ha individuato all’art. K2 la formazione professionale nel settore della giustizia come azione comune da intraprendere per migliorare la cooperazione tra autorità giudiziarie dei diversi Stati membri e per garantire un’applicazione corretta del diritto dell’UE.

In altre parole, la formazione professionale dovrebbe rappresentare per magistrati, giudici e pubblici ministeri un elemento di primaria importanza al fine di migliorare la propria competenza nello sviluppo del quadro legislativo europeo comune e per garantire che la legislazione UE sia applicata correttamente e uniformemente nell’ambito dei vari Stati membri.

A tale proposito, nel settembre 2011 la Commissione europea ha pubblicato la comunicazione *Costruire la fiducia nella giustizia in tutta l’UE, una nuova dimensione della formazione giudiziaria europea.* L’obiettivo della comunicazione è stato quello di dare una nuova e unitaria dimensione europea alla formazione giudiziaria, in modo tale da consentire a un numero crescente di magistrati, giudici e pubblici ministeri di accedere a una formazione uniforme e di alta qualità sulla legislazione dell’Unione.

Ciò dovrebbe condurre a raggiungere tre obiettivi determinanti per la costruzione di una cultura giudiziaria europea comune:

- una più ampia fiducia reciproca tra magistrati, giudici e pubblici ministeri dei diversi Stati membri;
- favorire lo scambio di informazioni in ambito giudiziario in modo corretto e conforme alla normativa in vigore;
- agevolare la tutela dei diritti e delle libertà dei cittadini dell’Unione.

In linea con gli obiettivi delineati dalla Comunicazione, molte organizzazioni transnazionali e networks europei stanno cercando di dare nuovi impulsi alla formazione professionale in ambito giudiziario.

Una menzione particolare dovrebbe essere data all'attività della European Judicial Training Network (EJTN). La rete svolge un ruolo cruciale nell'attuazione di politiche comuni, collegando le istituzioni nazionali e quelle europee per definire linee e azioni comuni in materia di formazione giudiziaria; anche attraverso il coordinamento delle diverse "Scuole di magistratura" nazionali.

Fine ultimo di EJTN, in linea con gli obiettivi della Comunicazione del 2011, dovrebbe essere proprio la promozione della conoscenza della normativa dell'Unione europea per migliorarne la comprensione, nonché per incentivare e sviluppare una maggior fiducia e cooperazione tra magistrati, giudici e pubblici ministeri dei diversi Stati membri.

Le attività, ma soprattutto i risultati ottenuti da EJTN in relazione alla formazione professionale, sono stati oggetto di una valutazione molto positiva ad opera del Consiglio dell'Unione europea. Nelle Conclusioni "Training on legal practitioners: an essential tool to consolidate the EU acquis" (2014/C443/04), il Consiglio ha affermato che, a livello dell'UE, EJTN "è nella posizione migliore per coordinare, attraverso i suoi membri, le attività di formazione nazionali e per sviluppare un'adeguata offerta di formazione per giudici e pubblici ministeri dei vari Stati membri".

In particolare, nel giugno 2016, EJTN ha adottato nove principi in materia di formazione giudiziaria con un duplice obiettivo:

a) costruire i "building blocks" sui quali le Scuole di formazione giudiziaria dell'Unione Europea devono organizzare e sviluppare l'offerta formativa;
b) creare i "building blocks" ai quali coloro che si occupano di fornire formazione in campo giudiziario devono ispirarsi per pianificare e fornire una formazione su misura e uniforme per lo specifico settore.

I principi sottolineano l'importanza di:

- una formazione specifica prima dell'assunzione delle funzioni e nel corso di tutta la vita professionale di giudici e pubblici ministeri;
- una formazione professionale che non si limiti all'aggiornamento delle competenze legali ma costruisca capacità e valori professionali;
- una formazione professionale effettiva dei magistrati e a tale proposito, evidenzia il ruolo fondamentale degli Stati membri ai quali è deputata la responsabilità di provvedervi;
- sostenere le più alte autorità giudiziarie nelle attività di formazione giudiziaria: gli Stati membri devono non solo garantire di rendere ef-

fettiva la formazione di giudici e magistrati ma anche renderla possibile attraverso finanziamenti.

Un altro passo importante verso la creazione di standard comuni in materia di formazione giudiziaria è la *Declaration of the International Organization for Judicial Training (IOJT)*, adottata l'8 novembre 2017.

L'IOJT è un'organizzazione non profit, istituita nel 2002, la cui missione si realizza attraverso conferenze internazionali e regionali, sedi che offrono opportunità per i giudici, magistrati e per coloro che si occupano di formazione giudiziaria, per discutere le strategie per la creazione e lo sviluppo di specifici centri di formazione, per delineare curricula di studio comuni, infine per migliorare le metodologie di insegnamento.

Più specificamente, sia i principi adottati dalla EJTN che la Dichiarazione IOJT rafforzano l'importanza delle ICT nello sviluppo e nel potenziamento dei programmi di formazione.

Il principio EJTN n. 7 si concentra proprio sul primato delle tecniche educative che coinvolgano direttamente i discenti e l'utilizzo di tecniche di formazione moderne.

A questo proposito, EJTN ha investito negli ultimi anni molte risorse per lo sviluppo di strumenti in grado di ampliare la portata delle opportunità di formazione giudiziaria. Per permettere il maggior numero di partecipanti a corsi e offerte formative sono state sviluppate e implementate varie piattaforme on line, corsi e-learning su varie materie disciplinate dalla legislazione UE.

Analoghe considerazioni sul principio n. 10 della *Declaration IOJT*, che ha affermato che la formazione giudiziaria dovrebbe riflettere le migliori e moderne pratiche nella progettazione di programmi di formazione professionale. Tali programmi dovrebbero avere un "taglio pratico" e dovrebbero ricorrere all'utilizzo di una vasta gamma di metodologie moderne di insegnamento.

In questo contesto si inserisce la sezione D del questionario che ha lo scopo specifico di avere un quadro completo dello "status quo" della formazione in materia di EIO esistente negli Stati membri per le autorità competenti per l'emissione e l'esecuzione e se vi sia un'ulteriore richiesta di formazione specifica sull'EIO.

Q1. Come è organizzata la formazione delle autorità di emissione e di esecuzione dell'EIO nel suo Stato?

La prima domanda (Q1) mira a capire se la formazione per le autorità giudiziarie competenti ai sensi della Direttiva 2014/41/UE venga svolta nei diversi Stati membri e chi sia l'istituzione nazionale responsabile in mate-

ria. Nella maggior parte degli Stati membri le autorità di formazione sono istituzionali (Figura 3.36).

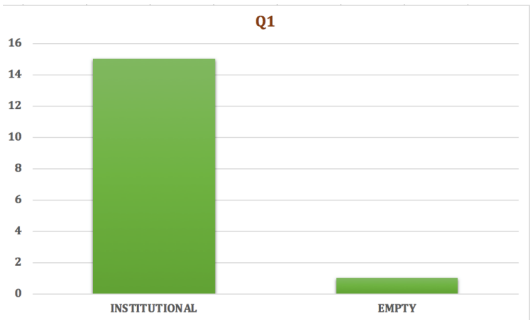

Figura 3.36: Q1, autorità nazionali di formazione

In generale la formazione in materia di EIO viene svolta dalle Scuole di magistratura nazionali e dalla rete EJTN.

La seconda domanda (Q2) era la seguente:

Q2. Sai chi sono i "trainers" che si occupano della formazione? A quale categoria di soggetti appartengono?

Le risposte a questa domanda hanno dimostrato che, in generale, i soggetti incaricati di effettuare formazione per coloro che si occupano di EIO sono per lo più gli stessi pubblici ministeri e giudici (Figura 3.37).

In alcuni paesi come Belgio, Lussemburgo, Grecia, Austria, Italia e Spagna sono coinvolti anche esperti della materia che sono avvocati. Tra gli Stati membri oggetto della presente ricerca solo la Repubblica Ceca ha dichiarato che tra i formatori sono inclusi anche rappresentanti del personale amministrativo.

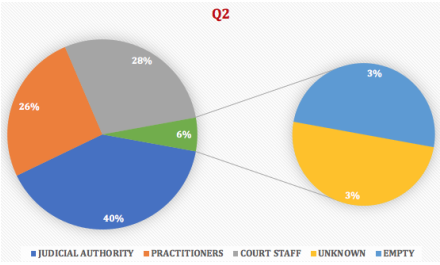

Figura 3.37: Q2, trainers in materia di EIO

Per quanto riguarda l’organizzazione dei corsi di formazione, agli Stati membri è stata chiesta la domanda che segue:

Q3. I corsi di formazione sono organizzati solo per il personale giudiziario? In caso contrario, chi sono gli altri soggetti coinvolti? (ad esempio, il personale amministrativo dell’autorità di emissione/esecuzione dell’EIO)

Più in dettaglio, la domanda (Q3) mostra (Figura 3.38) che le sessioni sono rivolte principalmente al personale giudiziario, vale a dire pubblici ministeri e giudici. In Belgio, Italia, Bulgaria, Spagna e Portogallo vengono organizzati anche corsi di formazione per il personale amministrativo delle cancellerie, e anche per gli avvocati che si occupano del tema.

La domanda (Q4) si occupa in particolare dell’oggetto/contenuto della offerta formativa.

Q4. In base alla sua esperienza, su quali aspetti pensa che i corsi di formazione in materia dovrebbero concentrarsi?

Le risposte fornite, hanno dimostrato che tra gli Stati membri emerge la necessità di avere corsi di formazione che coprano totalmente gli aspetti legati all’EIO: da quelli tecnici, legati ad esempio all’uso dell’e-Evidence Portal della Commissione[10], a quelli più giuridici, fino ad aspetti più specificatamente amministrativi.

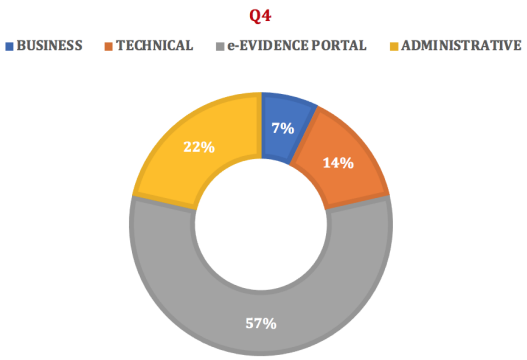

Figura 3.38: Q4, contenuto dell’offerta formativa sull’EIO

L’ultima domanda della sezione, infine, mira ad avere informazioni circa il livello di conoscenza dei singoli Stati membri sulle iniziative di training in materia, portate avanti dalla Commissione.

[10]Per maggiori dettagli si veda il Capitolo 4 del presente lavoro.

Q5. È a conoscenza delle iniziative della Commissione in materia di training sull'EIO?

Come hanno dimostrato le risposte alla domanda cinque (Q5) (Figura 3.39), la maggior parte degli Stati membri non è a conoscenza del fatto che la Commissione europea stia portando avanti iniziative in materia e stia preparando anche materiali informativi sugli aspetti fondamentali dell'emissione/esecuzione dell'EIO e dello scambio delle eventuali prove digitali. Solo quegli Stati membri che sono coinvolti direttamente in alcune iniziative progettuali europee sull'argomento hanno dichiarato di essere ben consapevoli e in attesa di questi materiali di formazione (si tratta nello specifico di Olanda, Spagna, Germania, Austria e Francia).

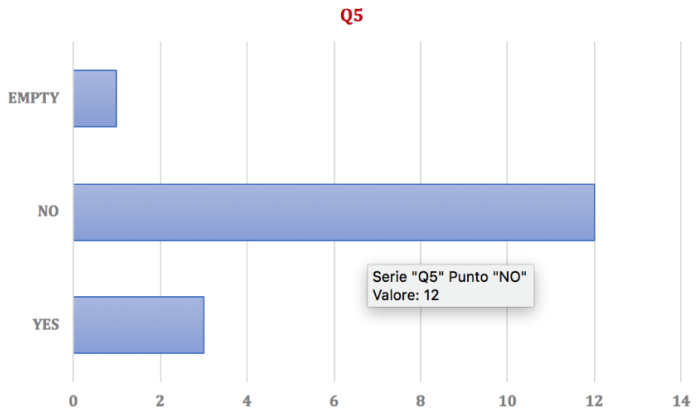

Figura 3.39: Q5, conoscenza delle iniziative europee per la formazione sull'EIO

Per quanto riguarda la specifica sezione D), le barriere che sono state delineate dai risultati del questionario sono le seguenti:

- mancanza di formazione standardizzata poiché i corsi di formazione esistenti sono sviluppati a livello nazionale senza uniformità generale o accordo tra i vari Stati membri sui programmi dell'offerta formativa;
- mancanza di visione globale dei soggetti cui dovrebbero essere indirizzati i corsi di formazione, poiché questi ultimi sono organizzati principalmente per il personale giudiziario e non sempre anche per quello amministrativo e tecnico delle cancellerie;

– gli argomenti insegnati durante i corsi di formazione non riguardano tutti gli aspetti dell'EIO, ma sono limitati solo ad alcuni di essi (ad esempio sono organizzati corsi che riguardano gli aspetti giuridici della procedura ma che non toccano quelli che sono gli aspetti tecnici).

Queste barriere possono essere superate da un'azione di diversi Stati membri a livello nazionale supportati dalle azioni progettuali finanziate dalla Commissione al fine di:

– creare a livello europeo corsi e elaborare materiali di formazione standardizzati e uniformi da rendere nelle diverse lingue degli Stati membri;
– coinvolgere tutte le categorie di soggetti coinvolti nella procedura EIO, autorità giudiziarie, personale amministrativo e tecnico delle cancellerie e avvocati. Obiettivo dovrà essere quello di creare corsi e materiali che tengano in considerazione lo specifico ruolo svolto da ciascun target group in relazione all'EIO;
– sviluppare corsi di formazione con una copertura completa sugli aspetti rilevanti per l'EIO.

Capitolo 4

Gli aspetti tecnologici e l'implementazione dell'EIO, analisi dei risultati del questionario on-line

Il Capitolo, dopo una prima parte dedicata allo stato dell'arte delle iniziative e degli strumenti tecnici esistenti a livello europeo per garantire uno scambio sicuro delle prove digitali, analizza i risultati della sezione del questionario on-line relativa ad aspetti tecnici delle procedure di EIO e MLA. In particolare, le domande della sezione sono state incentrate sullo "status quo" dei sistemi di informazione nazionali, sulla consapevolezza dei partecipanti all'indagine circa l'esistenza dei progetti sul tema e dei risultati da questi ottenuti in materia di scambio transnazionale delle prove digitali, infine su come ciascuno Stato membro affronti i problemi più comuni che si possono manifestare concretamente e tecnicamente nella realizzazione dello scambio[1].

[1]Il Capitolo 4 del presente lavoro è il frutto della mia partecipazione alle attività di studio e ricerca condotte nell'ambito dei progetti europei Evidence2e-Codex ed EXEC, nel corso del triennio di dottorato. In particolare, l'analisi condotta e i risultati descritti nel presente Capitolo sono stati presentati ai seguenti seminari/meetings: 1. *Meeting the Technical Community: Validation of the Evidence* (L'Aja, 26-27 marzo 2019) organizzato nell'ambito dei progetti europei Evidence2e-CODEX ed EXEC; 2. *e-Evidence co-funded project coordination Meeting* (Bruxelles, Commissione europea, 23 luglio 2019).

4.1 Lo stato dell'arte degli strumenti per lo scambio sicuro delle prove digitali

Nel giugno 2016, i ministri del Consiglio dell'Unione europea[2] hanno raccomandato di semplificare le procedure di cooperazione giudiziaria in materia penale, in particolare al fine di scambiare in maniera più efficace le prove digitali potenzialmente connesse ai processi. Come sottolineato nel paragrafo 2.2 del presente lavoro, le opzioni disponibili sono state quelle di sviluppare un approccio decentralizzato o centralizzato per l'infrastruttura da realizzare per lo scambio:

- un portale a livello centralizzato dell'UE, quale strumento per l'assistenza giudiziaria reciproca e le richieste di EIO, con una struttura di archiviazione centrale per le prove digitali raccolte e da scambiare; oppure
- un'infrastruttura decentralizzata comune e uniforme per tutti gli Stati membri, per lo scambio delle prove digitali nei processi penali transfrontalieri, che dovrà essere installata individualmente da ciascuno degli Stati.

Ancora oggi il dibattito sulle modalità e caratteristiche del portale non si è arrestato.

La Commissione sta cercando di rendere disponibile una piattaforma sicura per lo scambio, attraverso l'EIO e gli strumenti di MLA, delle prove digitali tra autorità giudiziarie dei diversi Stati membri.

Per quanto riguarda più nel dettaglio la struttura della piattaforma, il sistema di scambio digitale "e-Evidence Exchange System – eEDES" che la Commissione sta realizzando, sarà un sistema decentralizzato di scambio sicuro tra le autorità competenti degli Stati membri, che dovrebbe consentire loro di comunicare rapidamente, efficacemente ed in modo sicuro nel contesto dell'EIO e delle MLA nel campo del diritto penale.

Ciò, in linea con le politiche europee sulla sicurezza e al fine di combattere efficacemente il crimine informatico: il sistema dovrebbe mirare a migliorare le possibilità per le autorità giudiziarie di diversi Stati membri di scambiare prove digitali tra loro nell'ambito dei processi penali. In altre parole, tale piattaforma dovrebbe facilitare e accelerare la cooperazione giudiziaria anche

[2] Consiglio europeo, *Conclusioni del Consiglio sul miglioramento della giustizia penale*, 9 giugno 2016, in https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf.

in casi particolarmente complicati, legati ad esempio al terrorismo e alla criminalità organizzata, situazioni nelle quali la rapidità delle indagini potrebbe rappresentare un elemento fondamentale per la risoluzione del caso.

Per quanto riguarda lo sviluppo delle caratteristiche tecniche della piattaforma, è stato concordato nelle varie consultazioni con gli Stati membri che la piattaforma dovrà essere decentralizzata, utilizzando il sistema e-CODEX come strumento per la trasmissione sicura dei dati. Le specifiche funzionali della piattaforma sono state adottate a febbraio 2018 e sono in corso lavori sull'implementazione della piattaforma stessa. Il sistema dovrebbe entrare in funzione verso la fine del 2019.

Inoltre, come già sottolineato nel paragrafo 2.2 del presente lavoro, sono state senza dubbio rilevanti nel contesto esaminato con il presente lavoro, le iniziative ed anche i risultati di due progetti europei, che potrebbero aiutare a realizzare concretamente la piattaforma per lo scambio: l'iniziativa e-CODEX e il progetto Evidence[3]. Il primo potrebbe fornire l'infrastruttura necessaria per lo scambio di richieste e prove attendibile e sicuro, mentre il secondo potrebbe fornire la metodologia e il linguaggio formale per consentire lo scambio in modo uniforme e sicuro.

Di queste potenzialità senza dubbio la Commissione europea è stata consapevole, finanziando il progetto europeo Evidence2e-CODEX con l'intento, nello specifico contesto delle procedure MLA e dell'EIO, di sviluppare un "case study" per lo scambio sicuro ed affidabile delle prove digitali in Europa mettendo insieme l'infrastruttura veloce, sicura e affidabile realizzata dal progetto e-CODEX con quanto proposto dal progetto Evidence sull'adozione di un linguaggio formale di scambio.

L'efficacia delle procedure di EIO (ma anche di quelle di MLA in generale) si basano proprio sull'attuazione di un sistema sicuro e affidabile per lo scambio di prove digitali tra le autorità competenti e i risultati raggiunti dalle varie iniziative progettuali potrebbero rappresentare uno degli elementi fondamentali per la costruzione di una piattaforma sicura ed affidabile per tale scambio.

Ed in questo senso si stanno muovendo le molte iniziative di collaborazione tra i team di ricerca del progetto e-EDES della Commissione e di Evidence2e-CODEX.

In questo contesto si inserisce l'analisi delle domande più specificatamente tecniche del questionario.

[3]Si veda il paragrafo 2.2 del presente lavoro.

4.2 Analisi della sezione "C" del questionario: gli aspetti tecnici nella procedura di EIO

La sezione tecnica/operativa pone l'accento sulle questioni tecniche relative alla gestione dell'EIO e delle procedure di MLA. In particolare, la sezione contiene domande sullo "status quo" dei sistemi di informazione nazionali, sulla consapevolezza dell'esistenza dei progetti sul tema e dei risultati da questi ottenuti in materia di scambio transnazionale delle prove digitali, infine su come ciascuno Stato membro affronti i problemi tecnici più comuni che si possono manifestare concretamente.

La prima domanda (Q1) mira a conoscere quali siano le procedure tecniche in atto in ciascuno Stato membro partecipante all'indagine, nel caso di ricevimento di un EIO o in caso di richiesta di MLA.

Q1. Nel caso in cui riceve una richiesta di EIO o MLA da un altro paese, quali sono le procedure in atto nel suo Paese per gestirla?

Le possibili risposte guidate suggerite nel questionario sono state le seguenti:

- il sistema informatico nazionale può gestire gran parte della procedura in modo digitale, in modo decentralizzato (esistono quindi, molti punti a livello locale nel proprio paese);
- il sistema informatico nazionale può gestire gran parte della procedura in modo digitale, in modo centralizzato (un unico punto nazionale nel paese);
- le procedure sono gestite manualmente in modo tradizionale mediante sistema cartaceo o e-mail;
- non gestiamo questi casi al momento;
- altro (si prega di specificare).

Le risposte hanno rivelato, come mostrato nella Figura 4.1, che la maggior parte dei paesi (circa 61% dei partecipanti all'indagine) gestisce manualmente l'EIO/MLA, solo alcuni paesi (circa 28%) hanno un sistema nazionale centralizzato per gestire questi tipi di richieste, mentre sono ancora meno quei paesi (circa 11%) dotati di un sistema decentralizzato per la gestione delle richieste di EIO o di MLA.

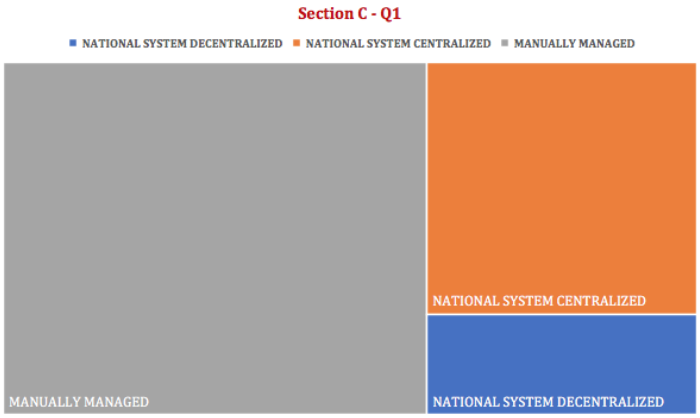

Figura 4.1: Q1, sistema nazionale per la gestione delle richieste di EIO/MLA

Per quanto riguarda gli Stati membri che sono stati più specificatamente analizzati nel presente lavoro, le risposte sono state le seguenti:

- Austria gestisce le procedure EIO/MLA basandosi su un sistema nazionale decentralizzato;
- Repubblica Ceca, Spagna, Lituania e Croazia trattano manualmente le richieste di EIO/MLA;
- Lussemburgo si basa su un sistema nazionale centralizzato.

La seconda domanda (Q2) intende indagare sulla volontà dei vari Stati membri partecipanti all’indagine di aderire alle iniziative portate avanti da alcuni progetti europei, che mirano a fornire un servizio per la gestione di EIO e MLA in modo digitale e sicuro basato sull’infrastruttura e-CODEX.

La domanda originale era la seguente:

Q2. Il progetto e-Evidence della Commissione, insieme ad altri progetti europei, fornirà un servizio per la gestione di EIO e MLA in modo digitale e sicuro basato sull’infrastruttura e-CODEX come canale di trasmissione. Il suo paese ha intenzione di aderire a questa iniziativa/progetto?

Le possibili risposte che sono state suggerite nel questionario sono state le seguenti:

- abbiamo già aderito all’iniziativa;
- abbiamo partecipato alle riunioni e-CODEX e stiamo decidendo di aderire all’iniziativa;
- abbiamo partecipato alle riunioni e-CODEX ma non abbiamo ancora deciso di aderire;

– abbiamo partecipato alla riunione e-CODEX ma non aderiremo all'iniziativa a causa della carenza di risorse (umane e/o finanziarie);
– non conosciamo il progetto e-CODEX;
– altro (si prega di specificare).

Sulla base delle risposte fornite (Figura 4.2), è stato possibile trarre la conclusione che tra gli Stati membri esiste un ampio accordo (circa 94% dei partecipanti all'indagine) volto all'adesione alle iniziative citate e solo una percentuale molto bassa (6%) ha dichiarato di non aver ancora deciso.

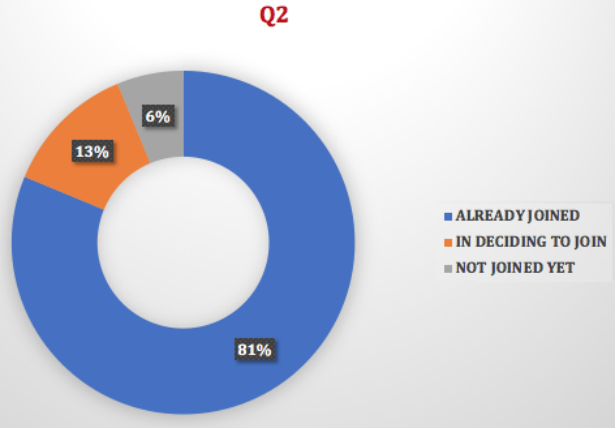

Figura 4.2: Q2, paesi aderenti a iniziative e-Evidence

Per quanto riguarda gli Stati membri oggetto del presente lavoro, hanno tutti risposto di aver aderito alle iniziative progettuali della Commissione.

La domanda (Q3) ha inteso esaminare in che modo ogni Stato membro tratti praticamente una procedura EIO/MLA.

Il testo originale era:

Q3. Nell'ambito delle procedure EIO e/o MLA come si scambiano le prove digitali rilevanti per un caso oggetto di indagine in un altro paese?

Le risposte guidate fornite nel questionario sono state le seguenti:

– abbiamo sequestrato le prove digitali potenziali e le abbiamo conservate fino a quando una persona autorizzata dallo Stato di emissione delle richiesta di EIO o di MLA non è arrivata;
– se richiesto, creiamo una copia forense della fonte sequestrata delle prove (disco rigido, smartphone, ecc.), successivamente arriva una persona autorizzata dallo Stato di emissione;

- se la dimensione della prova non è troppo grande, la inviamo all'autorità richiedente via e-mail, cloud sicuro con chiave di crittografia o password;
- non è mai successo finora;
- altro (si prega di specificare).

Le risposte fornite dai partecipanti all'indagine (Figura 4.3) evidenziano che lo scambio di prove, tra le autorità giudiziarie, è principalmente basato su modalità tradizionali, quindi nella maggior parte dei casi viene scambiata la copia forense della fonte di prova originale o la fonte originale sequestrata utilizzando persone appositamente incaricate. In altre parole, un'autorità giudiziaria di uno Stato membro dell'UE (Stato di emissione) richiede a un altro Stato membro UE (Stato di esecuzione) a seguito della raccolta di prove digitali, di generare una copia forense o di procedere a sequestrare la fonte di prova originale per poi consegnare tutto allo Stato richiedente. Successivamente, lo scambio della copia forense, o dell'originale sequestrato, nella maggioranza dei casi sarà realizzato su base umana. Una bassa percentuale (circa 26%) di paesi, infine, dichiara di fare affidamento su alcuni servizi cloud.

Per quanto riguarda gli Stati membri oggetto della presente ricerca, le risposte sono state le seguenti:

- l'Austria scambia le prove con consegna a mano dell'originale o crea una copia forense e consegna poi a mano la copia forense;
- la Croazia dichiara di utilizzare la consegna a mano o uno qualsiasi dei metodi indicati nella domanda, come e-mail/cloud, seguito comunque dalla consegna a mano della copia forense o dell'originale sequestrato;
- la Repubblica Ceca dichiara di utilizzare una delle soluzioni indicate nelle prime tre risposte del questionario;
- la Lituania scambia le prove con consegna a mano o utilizza uno qualsiasi dei metodi suggeriti nella domanda, come e-mail/cloud;
- il Lussemburgo crea una copia forense e quindi la scambia a mano;
- la Spagna crea una copia forense e quindi la scambia a mano o con uno qualsiasi dei metodi come e-mail/cloud.

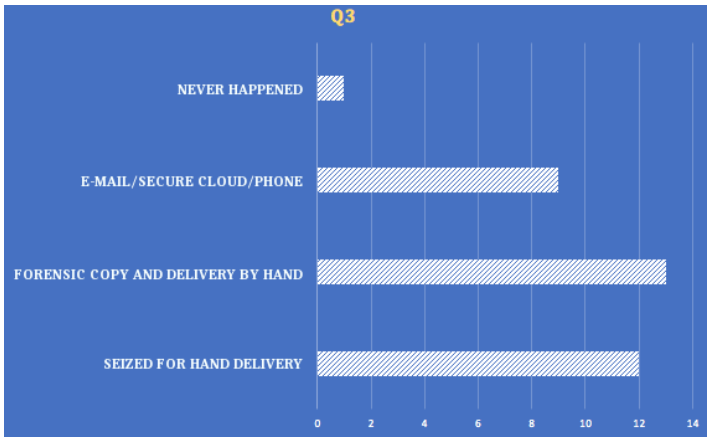

Figura 4.3: Q3, modalità utilizzata per scambio prove digitali

La domanda (Q4) mira ad individuare come ciascuno Stato membro affronti i casi in cui devono essere scambiati i file di larghe dimensioni.

La domanda originale era la seguente:

Q4. Nell'ambito delle procedure EIO e/o MLA come si scambiano file di grandi dimensioni (ad esempio un'acquisizione da uno smartphone da 16 GB) di prove digitali con un altro paese?

Le possibili risposte guidate fornite nel questionario sono state le seguenti:

- gli scambi di file di grandi dimensioni si basano su metodi tradizionali (corriere sicuro, a mano con una persona designata/autorizzata del paese richiedente, ecc.);
- utilizziamo un archivio cloud privato sicuro;
- usiamo una tecnologia per dividere il file in piccole parti (torrent, ecc.);
- non è mai successo finora;
- altro (si prega di specificare).

Le risposte rivelano, come mostrato nella Figura 4.4, che lo scambio di file di grandi dimensioni è principalmente basato sull'uomo. La maggior parte dei paesi infatti (circa 87% dei partecipanti all'indagine) usa il metodo tradizionale per trasferire un file di grandi dimensioni contenente prove.

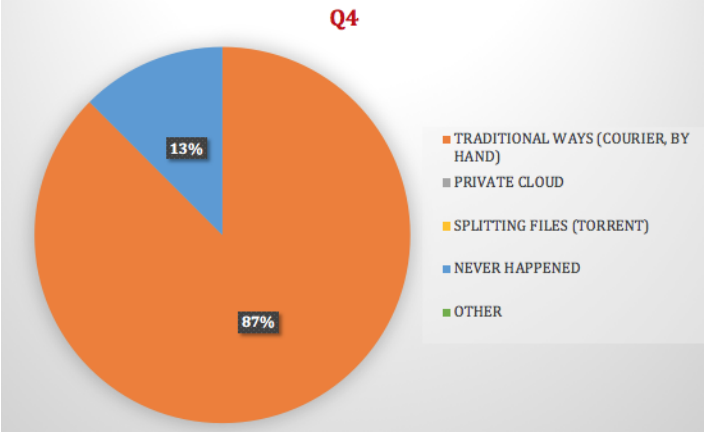

Figura 4.4: Q4, modalità scambio large file

Per quanto riguarda gli Stati membri oggetto specifico del presente lavoro, le risposte sono state le seguenti:

- Austria, Croazia, Spagna, Lituania e Lussemburgo dichiarano di utilizzare mezzi tradizionali per trasferire file di grandi dimensioni contenenti prove;
- la Repubblica Ceca dichiara di non aver mai scambiato fino ad ora file di grandi dimensioni.

La domanda (Q5) mira a indagare su questioni relative all’ammissibilità delle prove dinanzi a un tribunale.

La domanda originale era la seguente:

Q5. Esistono vincoli legali per la ricevibilità/ammissibilità di tali prove in tribunale?

Le risposte rivelano, come mostrato nella Figura 4.5, che nella maggior parte dei casi (56% dei partecipanti all’indagine) non vi sono particolari vincoli sull’ammissibilità di tali prove dinanzi a un tribunale, ma esiste anche una percentuale rilevante di casi (38%) in cui il giudice o l’avvocato della difesa può contestare l’ammissibilità di una prova di questo tipo (senza tuttavia indicazione circa le possibili motivazioni).

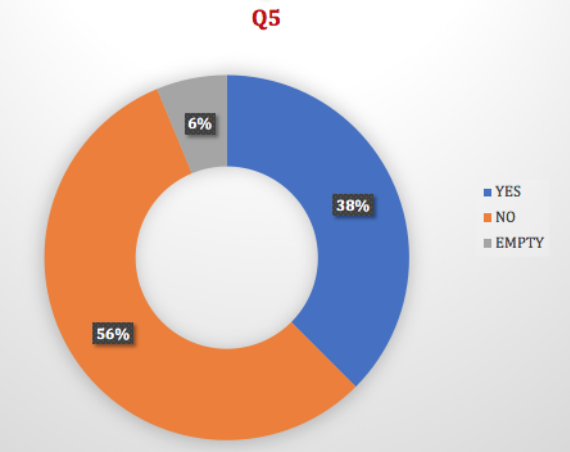

Figura 4.5: Q5, vincoli di ammissibilità delle prove digitali

Per quanto riguarda gli Stati membri oggetto specifico del presente lavoro, le risposte sono state le seguenti:

- Austria, Spagna e Lussemburgo sostengono che una prova digitale anche se ammessa nel processo, possa poi essere contestata dinanzi a un tribunale;
- Croazia e Lituania dichiarano che le prove digitali ottenute legalmente non sono messe in discussione davanti a un tribunale;
- la Repubblica Ceca ha lasciato la risposta vuota.

La domanda (Q6) mira a esaminare, in maniera più specifica rispetto alla domanda Q2, se gli Stati membri avranno intenzione di far uso di piattaforme digitali per gestire le procedure EIO o MLA, ed anche quindi lo scambio delle prove.

La domanda originale era la seguente:

Q6. Il suo paese utilizzerà una piattaforma digitale per la gestione delle procedure EIO e MLA?

Le possibili risposte guidate fornite nel questionario sono state le seguenti:

- utilizzeremo e-CODEX;
- utilizzeremo la nostra piattaforma nazionale;
- utilizzeremo il portale di riferimento creato dalla Commissione europea (e-EDES portal).

Le risposte mostrano, come illustrato nella Figura 4.6, che la maggior parte degli Stati membri (36% dei partecipanti all'indagine) ha dichiarato

che sono in atto iniziative nazionali volte a permettere l'utilizzo della piattaforma e-CODEX, una percentuale significativa (32%) ha dichiarato che utilizzerà le piattaforme nazionali, un'altra percentuale rilevante (24%) utilizzerà il portale di riferimento fornito dalla CE (e-EDES Portal) e solo una percentuale bassa (8%) non ha fornito una risposta.

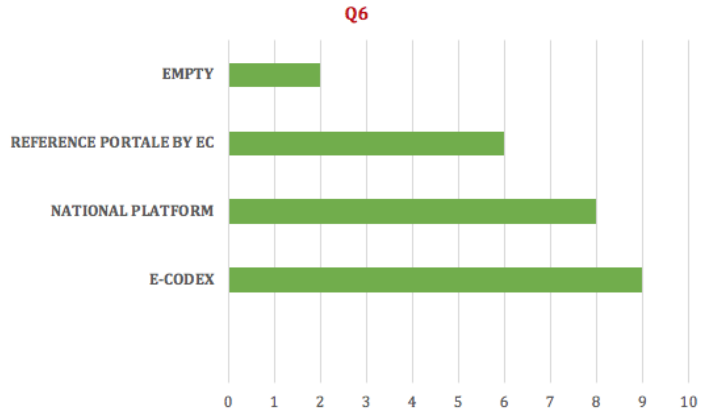

Figura 4.6: Q6, utilizzo di piattaforma digitale per gestione EIO/MLA

Per quanto riguarda gli Stati membri oggetto del presente lavoro, le risposte sono state le seguenti:

- Austria utilizza e-CODEX e i sistemi nazionali e, in futuro, il portale di riferimento della Commissione;
- Croazia e Lituania utilizzeranno e-CODEX e il portale di riferimento della Commissione;
- Repubblica Ceca utilizza il sistema nazionale, pur dichiarando di aver aderito alle iniziative e-CODEX;
- Lussemburgo non ha fornito una risposta;
- Spagna utilizza e-CODEX e i sistemi nazionali.

La domanda (Q7) riguarda la comprensione della qualità della connettività in ciascuno Stato membro, al fine di proporre soluzioni ragionevoli per il trasferimento di informazioni e in particolare per lo scambio di file di prove di grandi dimensioni.

La domanda originale era la seguente:

Q7. Qual è la velocità disponibile nel tuo ufficio/sistema?

Le possibili risposte guidate fornite nel questionario sono state le seguenti:

- 1 giga bit al secondo;
- tra 500 e 800 mega bit al secondo;
- tra 200 e 500 mega bit al secondo;
- tra 100 e 200 mega bit al secondo;
- tra 50 e 100 mega bit al secondo;
- meno di 50 mega bit al secondo;
- non lo so.

Le risposte delineano, come illustrato nella Figura 4.7, che molti paesi (6) non sono stati in grado di fornire una risposta, alcuni paesi (3) hanno una connettività eccellente, tra 500 e 800 Mbits/sec e altri paesi hanno una bassa connettività (3).

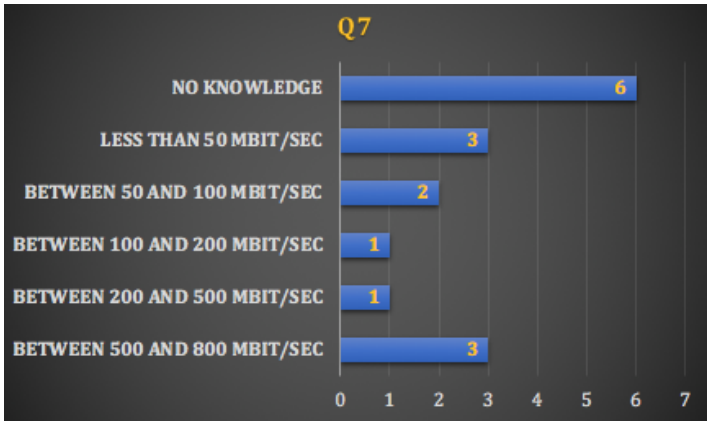

Figura 4.7: Q7, connettività delle piattaforme

Per quanto riguarda gli Stati membri oggetto del presente lavoro, le risposte sono state le seguenti:

- Austria e Croazia hanno una connettività inferiore a 50 Mbits/sec (piuttosto bassa);
- Repubblica Ceca e Lussemburgo hanno una connettività eccellente (tra 500 e 800 Mbits/sec);
- Lituania ha un'ottima connettività (tra 200 e 500 Mbits/sec);
- Spagna non è a conoscenza della sua connettività (è possibile che la risposta sia stata fornita da qualcuno senza un background tecnico).

La domanda (Q8) riguarda i metodi di crittografia in atto negli Stati membri.

La domanda originale era la seguente:

Q8. Che tipo di metodi di crittografia usa nel suo sistema nazionale per proteggere la trasmissione di dati sensibili?

Le possibili risposte guidate fornite nel questionario sono state le seguenti:

– crittografia basata su chiavi asimmetriche;
– crittografia basata su chiavi simmetriche;
– crittografia basata su chiavi asimmetriche e simmetriche;
– non lo so.

Le risposte spiegano, come mostrato nella Figura 4.8, che la maggior parte dei paesi (11) non è stata in grado di fornire una risposta, alcuni paesi (3) usano le chiavi asimmetriche come metodo di crittografia e solo due paesi usano entrambe le chiavi, simmetriche e asimmetriche, per il loro sistema di crittografia.

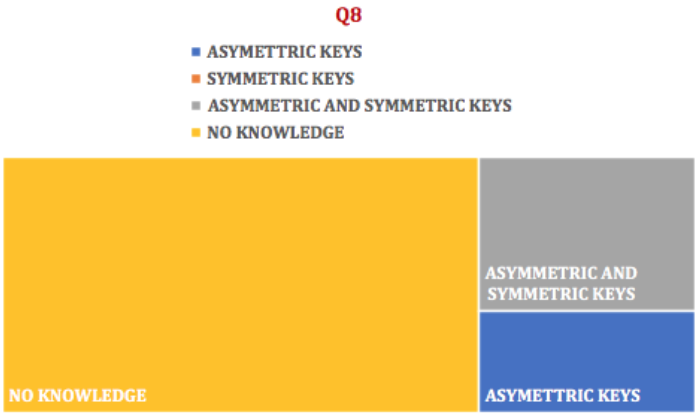

Figura 4.8: Q8, crittografia

Per quanto riguarda gli Stati membri oggetto del presente lavoro, le risposte sono state le seguenti:

– Austria e Spagna utilizzano chiavi asimmetriche per la crittografia dei dati;
– Repubblica Ceca, Lussemburgo e Croazia non hanno fornito alcuna risposta per mancanza di conoscenza.

La domanda (Q9) ha riguardato i metodi di autenticazione in atto negli Stati membri, per proteggere l’accesso ai dati sensibili.

La domanda originale era la seguente:

Q9. Che tipo di metodi di autenticazione usa nel suo sistema nazionale per proteggere l'accesso a dati sensibili o aree protette?

Le possibili risposte guidate fornite nel questionario sono state le seguenti:

- fornire utente e password su canale sicuro;
- metodi a due fattori basati su token online o offline;
- metodi a due fattori basati sul sistema biometrico;
- non lo so.

Le risposte delineano, come illustrato nella Figura 4.9, che la maggior parte dei paesi (10) utilizza un utente/password su un canale sicuro come metodo di autenticazione, solo alcuni paesi (3) utilizzano un metodo a due fattori basato sul token come metodo di autenticazione, e alcuni paesi (4) non sono stati in grado di fornire una risposta a causa della mancanza di conoscenza del sistema in atto nel proprio paese.

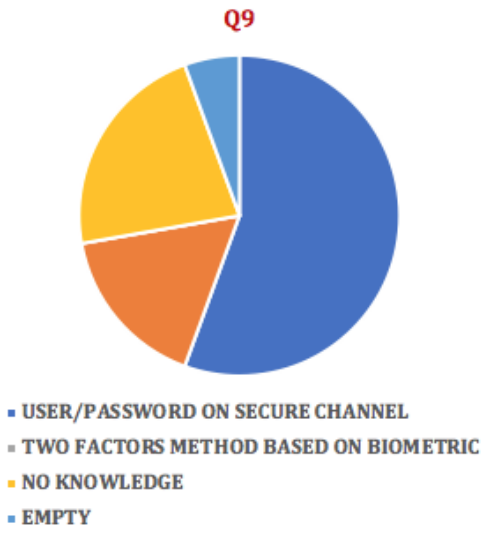

Figura 4.9: Q9, modalità autenticazione

Per quanto riguarda gli Stati membri oggetto del presente lavoro, le risposte sono state le seguenti:

- Austria utilizza l'Utente/Password su "Secure Channel" e i due fattori basati su metodi di autenticazione token;
- la Repubblica Ceca non è a conoscenza del proprio sistema nazionale di autenticazione;

– Spagna, Lituania e Croazia utilizzano l’utente/password sul canale protetto;
– Lussemburgo utilizza i due fattori basati sul token come metodo di autenticazione.

La domanda (Q10) riguarda l’uso della firma elettronica in atto negli Stati membri.

La domanda originale era la seguente:

Q10. Usa la firma elettronica?

Le risposte delineano, come illustrato nella Figura 4.10, che la maggior parte dei paesi (11) utilizza una firma elettronica, solo alcuni paesi (4) non hanno un sistema per convalidare/autenticare i documenti attraverso un metodo di firma elettronica e un paese non ha fornito una risposta.

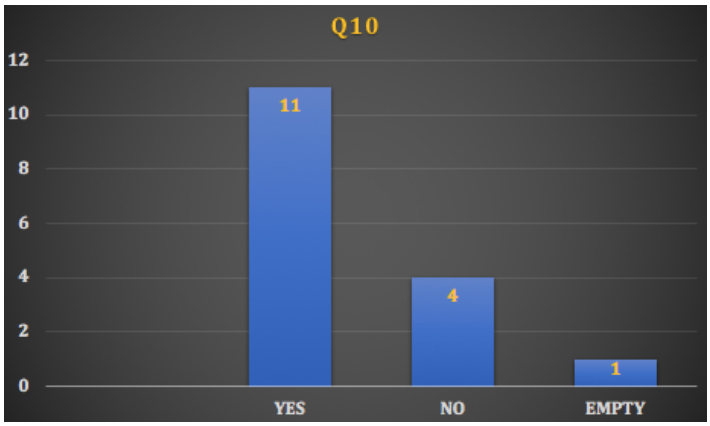

Figura 4.10: Q10, firma elettronica

Per quanto riguarda gli Stati membri oggetto del presente lavoro, le risposte sono state le seguenti:

– Austria, Repubblica Ceca, Spagna e Lituania dispongono di un sistema di firma elettronica;
– Croazia e Lussemburgo non dispongono di un sistema di firma elettronica.

La domanda (Q11) è stata formulata per capire se la trasmissione di prove sia accettato o meno in uno Stato membro se ricevuta da un paese che non ha una firma elettronica in atto.

La domanda originale era la seguente:

Q11. Se un Paese non ha in atto una procedura di firma elettronica, il suo Paese può accettare lo scambio elettronico per accelerare la procedura e quindi successivamente dare seguito a procedure in formato cartaceo (sì, no, commento)?

Le risposte delineano, come illustrato nella Figura 4.11, che la maggior parte dei paesi (13) accetta le prove ricevute in tal modo, solo pochi paesi (2) non accetterebbero tali prove e un paese non ha fornito una risposta.

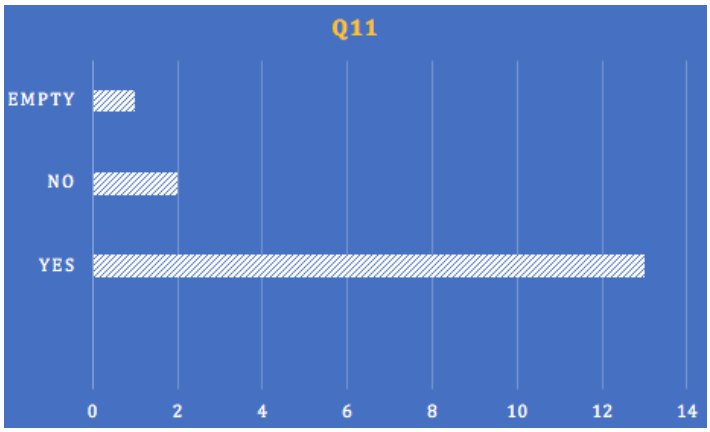

Figura 4.11: Q11, accettazione scambio senza firma digitale

Per quanto riguarda gli Stati membri oggetto del presente lavoro, le risposte sono state le seguenti: Austria, Repubblica Ceca, Spagna, Lituania, Lussemburgo e Croazia hanno tutti dichiarato di accettare una prova trasmessa da un altro paese anche senza firma elettronica, soprattutto in caso di urgenza e se comunque viene dato seguito ad una procedura tradizionale, cartacea.

Per quanto riguarda la specifica sezione tecnico/operativa C, gli ostacoli indicati dai risultati del questionario sono stati i seguenti:

- troppi paesi gestiscono ancora le procedure EIO/MLA in modo manuale, senza fare affidamento su nuove tecnologie per accelerare le procedure stesse e la speditezza delle indagini. I metodi tradizionali ancora in atto rendono le operazioni di scambio sicuramente più lente e probabilmente più soggette a errori;
- lo scambio di prove digitali, nell'ambito degli strumenti giuridici EIO/MLA, tra diversi Stati membri è ancora prevalentemente basa-

to sull'uomo. Lo standard di fatto consiste nella consegna a mano o della fonte di prova originale (che è stata sequestrata) o della copia forense della fonte di prova originale. Questo metodo rende lo scambio molto lento e al tempo stesso anche costoso;
– lo scambio di prove in file di grandi dimensioni è ancora principalmente basato sull'uomo. Per risolvere questo problema, è fondamentale disporre di una connettività valida e stabile per realizzare il trasferimento dallo Stato di esecuzione allo Stato di emissione.

Queste barriere possono essere superate da un'azione di diversi Stati membri a livello nazionale in collaborazione con la Commissione europea e soprattutto con le iniziative progettuali da questa finanziate (progetto e-Evidence, progetto Evidence2e-Codex e progetto EXEC) al fine di:

– promuovere e adottare il sistema di scambio e-Evidence quando sarà pronto per essere utilizzato (entro la fine del 2019) e organizzare una formazione efficace sul suo uso, sui benefici e vantaggi che potrebbe portare la sua adozione (breve termine);
– favorire l'adozione dello standard per la rappresentazione di metadati e dati di una prova. Attualmente lo standard sta diventando diffuso e popolare ma alcuni importanti stakeholder, come le Forensic Tools Companies, devono essere convinte di adattare i loro strumenti allo standard (medio termine);
– il rafforzamento della connettività implica investimenti a lungo termine che possono essere ottenuti basandosi solo sulle politiche del governo di ciascuno Stato membro (medio/lungo termine).

Capitolo 5

Gli ostacoli individuati attraverso l'indagine e le possibili azioni da intraprendere a livello europeo

Il Capitolo, dopo l'analisi dei risultati dei questionari fatti circolare tra i rappresentanti del CCBE, tra magistrati e pubblici ministeri che hanno aderito alle iniziative formative di EJTN sul tema oggetto del presente lavoro, infine tra i rappresentanti delle Istituzioni europee (EUROPOL, EUROJUST, OLAF e EJN), è dedicato alla presentazione di una proposta di azioni comuni da adottare per un'efficace e uniforme realizzazione dello scambio transnazionale delle prove digitali nei processi penali. La proposta di azioni comuni per far fronte alle barriere ed ostacoli individuati nelle risposte ai questionari, è stata elaborata tenendo in considerazione la totalità dei feedback ricevuti dai vari "targets groups" dell'indagine.[1]

[1]Il Capitolo 5 del presente lavoro è il frutto della mia partecipazione alle attività di studio e ricerca condotte nell'ambito dei progetti europei Evidence2e-Codex ed EXEC, nel corso del triennio di dottorato. In particolare, l'analisi condotta e i risultati descritti nel presente Capitolo sono stati presentati ai seguenti seminari/meetings: 1. *Meeting the Technical Community: Validation of the Evidence* (L'Aja, 26-27 marzo 2019) organizzato nell'ambito dei progetti europei Evidence2e-CODEX ed EXEC; 2. *e-Evidence co-funded project coordination Meeting* (Bruxelles, Commissione europea, 23 luglio 2019). I risultati del par. 5.2 sono stati analizzati ed elaborati a seguito del seminario "Evidence in the cloud: new challenges in collecting evidence on cyberspace in the European Union", organizzato da EJTN il 27-28 settembre 2018 presso la sede della Scuola di Magistratura in Firenze

5.1 Analisi della prospettiva degli avvocati del CCBE

Per una panoramica completa sulle modalità di scambio delle informazioni, sulla raccolta delle prove digitali e sulle procedure per richiedere ulteriori indagini nel contesto dell'EIO, è stato della massima importanza per il presente lavoro il contributo fornito dai membri del CCBE, che rappresenta l'associazione di più di un milione di avvocati europei. Alcuni rappresentanti del CCBE (circa 80-90) hanno compilato una versione ridotta del questionario, con solo le domande attinenti alle procedure di EIO che riguardano le specifiche funzioni da essi esercitate nell'ambito del processo penale. Pertanto, il punto di vista offerto dalle risposte si concentra solo su questioni specifiche e mirate, idonee a esprimere la prospettiva degli avvocati sullo scenario attualmente in corso nel contesto dell'EIO.

La categoria degli avvocati rappresenta uno dei soggetti competenti, ai sensi della Direttiva 2014/41/UE, a richiedere l'emanazione di un EIO. Infatti, l'art. 1 par. 3 della Direttiva espressamente stabilisce che: "Il rilascio di un EIO può essere richiesto da un indagato o imputato, o da un avvocato per suo conto, nell'ambito dei diritti di difesa applicabili in conformità con la procedura penale nazionale".

Va notato che nell'era digitale gli avvocati sono sempre più coinvolti nelle procedure transfrontaliere volte a fronteggiare il crimine: pertanto, un'analisi approfondita delle modalità e procedure da essi adottate e attuate potrebbe essere un utile punto di partenza allo scopo di identificare eventuali problemi ravvisati da tali soggetti nel contesto dell'EIO. E al tempo stesso un utile punto di partenza per identificare potenziali azioni per migliorare e rendere maggiormente efficaci le procedure di EIO e la collaborazione con l'autorità giudiziaria.

Il questionario, redatto in lingua inglese, è stato distribuito tra i rappresentanti dei seguenti paesi: Repubblica Ceca, Estonia, Finlandia, Francia,

nell'ambito delle iniziative di formazione sul tema dello scambio transnazionale delle prove digitali per magistrati e pubblici ministeri europei. I risultati del par. 5.3 sono stati analizzati ed elaborati a seguito del seminario organizzato dal Consiglio Nazionale delle Ricerche in collaborazione con i progetti europei Evidence2e-CODEX ed EXEC nell'ambito delle iniziative di collaborazione con i team di esperti in materia di scambio transnazionale delle prove, appartenenti alle diverse Istituzioni europee (Europol, Eurojust, Olaf), tenutosi a L'Aja 20-21 Novembre 2018.

Grecia, Irlanda; Liechtenstein, Spagna, Svezia e Olanda. Tutti questi paesi hanno risposto al questionario, ad eccezione dell'Irlanda (che non ha recepito la direttiva EIO) e del Liechtenstein (che al momento in cui il questionario è stato distribuito non aveva ancora attuato la direttiva).

Il sondaggio si è concentrato principalmente sulle domande riportate di seguito.

Q1. Nel suo paese, come può essere richiesto il rilascio di un EIO per conto di un indagato o imputato?

I risultati dell'indagine hanno dimostrato che, in generale, tale richiesta è considerata come qualsiasi altra richiesta di raccolta di prove o di ulteriori indagini nei procedimenti penali nazionali.

Non esistono formalità specifiche, ma alcuni dei partecipanti all'indagine hanno sottolineato l'importanza di una richiesta scritta contenente i motivi e ciò che si cerca di ottenere. In altre parole, la richiesta di condurre (ulteriori) indagini deve essere puntualmente e specificatamente motivata.

Q2. Esistono nel suo Stato condizioni preliminari da soddisfare per richiedere l'emissione di un EIO?

I risultati generali hanno mostrato che tutti gli avvocati che hanno partecipato all'indagine hanno confermato che l'EIO può essere richiesto allo stesso modo di qualsiasi altra richiesta di raccolta di prove e che non devono essere soddisfatte condizioni preliminari speciali.

Più in dettaglio, la richiesta deve essere solo "ragionevole" e "comprovata": se le prove da raccogliere attraverso l'EIO possono essere potenzialmente rilevanti per il caso specifico, allora lo strumento processuale dovrebbe essere rilasciato.

Q3. Esistono nel suo Stato particolari termini relativi al trattamento delle richieste di rilascio di un EIO (ad esempio, le autorità giudiziarie sono tenute a rispondere a una richiesta entro un determinato periodo di tempo)?

I risultati della domanda sono praticamente tutti uniformi: gli avvocati che hanno partecipato all'indagine hanno dichiarato che non sono previsti, nei rispettivi ordinamenti, termini per la risposta alla richiesta di rilascio di un EIO.

In generale, esistono intese comuni, buone prassi nel settore giudiziario: la richiesta di un EIO dovrebbe essere trattata e gestita tenendo conto delle regole e principi e con la stessa rapidità in cui viene gestito un atto procedurale interno, e le scadenze dovrebbero essere quelle previste dal codice di procedura penale.

Più in dettaglio, tutti i partecipanti all'indagine hanno semplicemente dichiarato che la richiesta di un EIO deve essere gestita "il più rapidamente possibile" (anche per non vanificare la fase investigativa del procedimento) e, comunque, senza indebito ritardo.

Q4. Che tipo di dati può coprire la richiesta di rilascio di una EIO? Dati degli abbonati, dati di contenuto, metadati?

I risultati mostrano che le risposte fornite dagli avvocati che hanno partecipato all'indagine sono molto equilibrate, poiché i tre tipi di dati proposti sono quasi sempre richiesti insieme.

Q5. Esiste nel suo ordinamento giuridico una definizione di dato dell'abbonato, metadato e dato di contenuto? Se sì, si prega di specificare.

In generale, non è stata data una risposta precisa e puntuale alla domanda, ciò perché nei vari ordinamenti nazionali degli avvocati che hanno partecipato all'indagine non sembra esistere una definizione normativa delle varie tipologie di dati.

I partecipanti si sono limitati genericamente a rispondere che possono essere oggetto di richiesta tutti i dati necessari per la definizione del caso concreto. Senza pertanto distinguere tra dati degli abbonati, dati di contenuto e metadati.

Solo l'avvocato proveniente dalla Svezia ha dichiarato che la definizione di metadati è stata accolta in alcuni documenti ufficiali (in particolare in alcuni rapporti governativi) quali informazioni generate dai fornitori di servizi allo scopo di fornire un servizio di comunicazione ad esempio per scopi di fatturazione ecc.

Q6. In che modo le autorità giudiziarie competenti nel suo paese trasferiscono i dati ottenuti tramite un EIO agli avvocati?

E in quale formato?

Per quanto riguarda le procedure adottate dalle autorità giudiziarie per il trasferimento di dati e informazioni agli avvocati, i risultati dell'indagine hanno dimostrato che negli Stati membri di appartenenza dei vari avvocati che hanno partecipato all'indagine i sistemi elettronici di trasmissione rappresentano il principale strumento di trasferimento.

Più in dettaglio:

Tab. 5.1: Modalità trasferimento dati agli avvocati

Rep. Ceca	I dati ottenuti tramite un EIO vengono trasferiti direttamente all'avvocato attraverso la casella di posta personale certificata presso il rispettivo ordine forense. In alternativa viene utilizzato il servizio postale.
Estonia	I dati ottenuti tramite EIO vengono trasferiti elettronicamente (attraverso E-File system).
Finlandia	I dati ottenuti tramite un EIO al momento vengono trasferiti sia in formato cartaceo sia in formato elettronico (CD-ROM/DVD).
Francia	I dati ottenuti tramite EIO vengono trasferiti tramite i soliti canali di comunicazione alle parti previsti dalle disposizioni di diritto interno relative ai procedimenti penali e all'accesso al fascicolo. In altre parole, secondo le procedure di cui agli articoli 114, 390 e 390-2 del Codice di procedura penale.
Spagna	Non sono indicate esperienze in materia
Svezia	Non viene data una risposta specifica: i dati e le informazioni vengono trasferite secondo modalità diverse a seconda del caso concreto.
Olanda	I dati saranno trasferiti elettronicamente tramite il giudice istruttore attraverso gli strumenti del processo penale telematico.

L'analisi dei risultati non ha mostrato particolari difficoltà o problemi percepiti dagli avvocati europei nel contesto delle procedure di EIO. Tuttavia, l'esame della prospettiva di tale categoria di soggetti è stata determinante per avere un quadro completo in materia, che riguardi non soltanto il lato dell'autorità giudiziaria (giudici, magistrati, pubblici ministeri, personale amministrativo e tecnico delle Corti) ma anche quello di professionisti del diritto coinvolti nella procedura di EIO.

5.2 I risultati del seminario organizzato da EJTN

Il seminario organizzato da EJTN per giudici e pubblici ministeri degli Stati membri dell'UE, dal titolo "Evidence in the cloud: new challenges in collecting evidence on cyberspace in the European Union", si è svolto a Firenze lo scorso 27 e 28 settembre 2018. In totale, al seminario hanno partecipato 35 tra giudici e pubblici ministeri, rappresentanti delle autorità giudiziarie dei seguenti Stati: Belgio, Bulgaria, Repubblica Ceca, Croazia, Danimarca, Francia, Germania, Grecia, Italia, Lettonia, Olanda, Polonia, Portogallo, Romania, Slovacchia, Spagna, Svezia e Ucraina.

Il seminario, come specificato anche in precedenza, è stato organizzato nell'ambito delle attività ed eventi formativi organizzati da EJTN sul tema specifico dello scambio delle prove digitali nel contesto dell'EIO. Le domande poste ai partecipanti sono state in parte estratte dal questionario on-line sopra analizzato, in parte sono state elaborate nell'ambito delle attività dei progetti europei che si sono occupati, e si occupano, di scambio transnazionale delle prove digitali nei processi penali (Evidence, Evidence2e-CODEX ed EXEC) e sono state riproposte durante il meeting.

Le domande, e la relativa analisi, vengono riportate di seguito.

Q1. Sa cosa è una prova digitale?

Q2. Conosce cosa sia il ciclo di vita di una prova digitale?

Q3. Ha familiarità con il linguaggio e la terminologia legati alla "digital forensics"? (ad es. acquisizione forense, copia forense, analisi forense, ecc. . .)

Q4. Le è mai capitato di trattare e/o scambiare prove digitali nella sua attività lavorativa quotidiana?

In generale, i risultati delle risposte alle prime domande (Figura 5.1), hanno dimostrato ampia consapevolezza dei partecipanti circa le nozioni giuridiche di base in tema di prove digitali. Tuttavia, dalla discussione in aula, è emerso che laddove si tratti in particolare della conoscenza del ciclo di vita della prova digitale, la consapevolezza diminuisce e ciò si riflette anche nella conoscenza del gergo più propriamente digital forensics. Sebbene una buona percentuale di giudici e pubblici ministeri che hanno partecipato all'evento abbiano dichiarato di occuparsi quotidianamente di questo tipo di prove durante le loro attività lavorative.

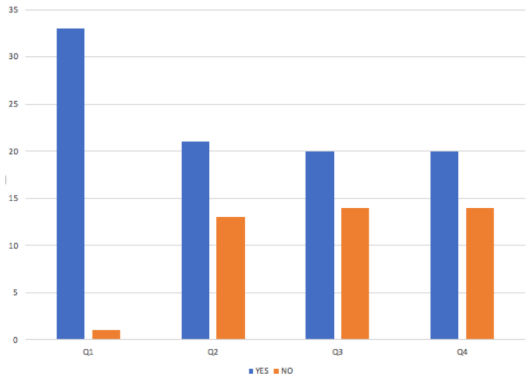

Figura 5.1: Q1-Q4 seminario EJTN, conoscenza nozioni generali

La domanda successiva, mirava ad indagare le problematiche e difficoltà che giudici e pubblici ministeri incontrano laddove nel processo venga in rilievo una prova digitale.

Q5. Quali problemi ha incontrato nei casi in cui nel processo penale sono venute in rilievo e sono state presentate prove digitali? (problemi di ammissibilità, autenticità, integrità, scarsa familiarità, mancato rispetto della catena di custodia, scarsa formazione professionale, ecc.)

In particolare, dalle risposte alla domanda, ciò che emerge è la particolare preoccupazione di giudici e pubblici ministeri circa le garanzie di ammissibilità, autenticità e integrità della prova che potrebbero essere compromesse in caso di natura digitale della stessa.

La Figura 5.2 dimostra, infatti, che le principali difficoltà riscontrate tra i partecipanti al seminario riguardavano proprio l'ammissibilità della prova digitale, la sua autenticità e integrità.

Anche la mancanza di familiarità con il trattamento di questi tipi di prove rappresenta un possibile ostacolo individuato da giudici e pubblici ministeri per un corretto e uniforme scambio delle prove stesse.

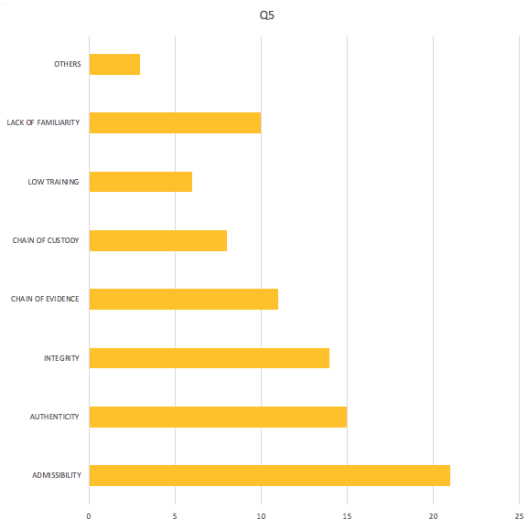

Figura 5.2: Q5 seminario EJTN, difficoltà trattamento prove digitali

La successiva serie di domande, estrapolate direttamente dal questionario on-line, mirava a indagare le modalità e procedure in atto nei singoli Stati

membri in caso di scambio di prove digitali in un contesto transfrontaliero. In particolare, le domande proposte ai partecipanti al seminario sono state le seguenti. Q6. Le è mai capitato di scambiare prove digitali con un Paese UE o con altro Paese straniero?

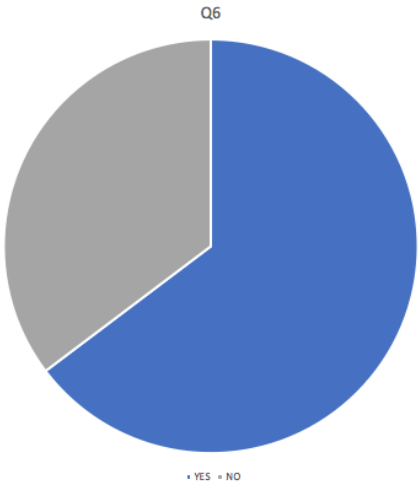

Figura 5.3: Q6 seminario EJTN, scambio delle prove digitali con altri Stati

I risultati (Figura 5.3) dimostrano che nella maggioranza dei casi i partecipanti all'indagine hanno dichiarato di essere stati coinvolti in procedure di scambio di prove digitali sia con paese UE sia con Stati terzi.

Q7. Quali strumenti giuridici utilizza nel caso?

Le risposte alla domanda Q7 (Figura 5.4) hanno evidenziato che gli strumenti utilizzati nella maggioranza dei casi sono l'EIO e le procedure di MLA. Tuttavia, gli Stati membri hanno dichiarato che il primo strumento processuale viene utilizzato nel rapporto tra Stati membri, mentre le procedure di MLA sono utilizzate solo laddove sia richiesta cooperazione giudiziaria in materia penale verso Stati membri che non applicano la procedura EIO, ovvero con Stati terzi non UE.

Q8. In che modo concretamente viene scambiata la prova digitale?

I risultati di questo seminario hanno confermano che i mezzi tradizionali sono quelli prevalenti per lo scambio delle prove digitali in un contesto transnazionale. Nella maggior parte dei casi lo scambio avviene su base umana o tramite corriere sicuro (Figura 5.5).

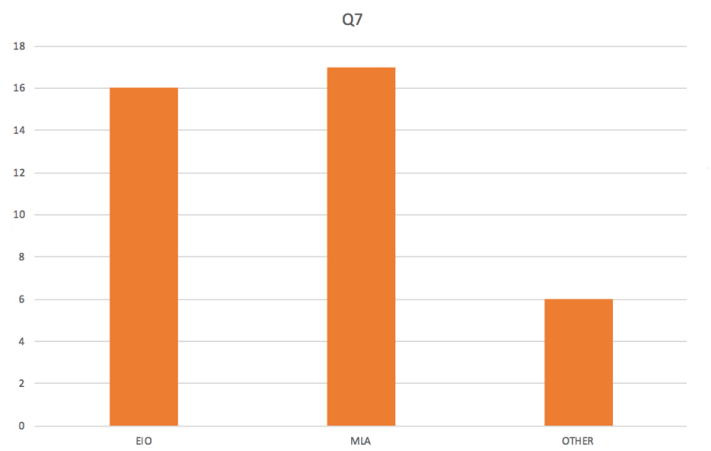

Figura 5.4: Q7 seminario EJTN, strumenti giuridici per lo scambio delle prove digitali

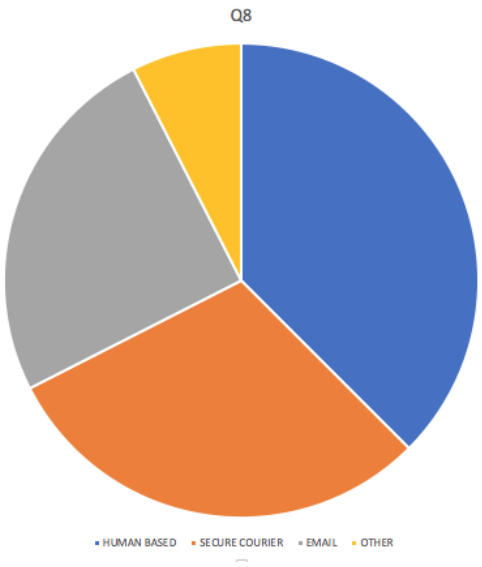

Figura 5.5: Q8 seminario EJTN, modalità di scambio della prova digitale

Q9. Nell'ambito delle procedure EIO e/o MLA quali sono le difficoltà che ostacolano maggiormente lo scambio di prove digitali con un altro paese?

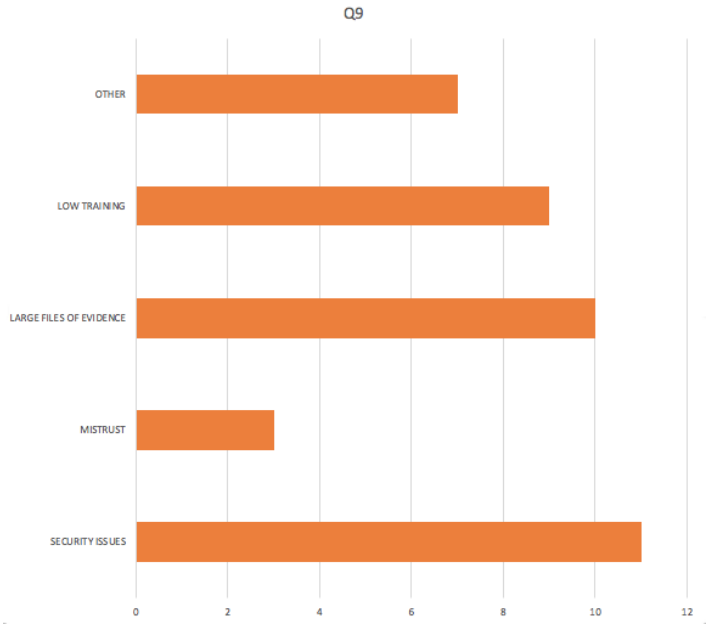

Figura 5.6: Q9 seminario EJTN, difficoltà nello scambio delle prove digitali

Per quanto riguarda l'identificazione delle principali barriere che ostacolano lo scambio delle prove digitali, i risultati hanno confermato che la trasmissione di file di grandi dimensioni e la sicurezza degli scambi rappresentano gli ostacoli maggiormente in gioco insieme alla scarsa formazione sulle procedure EIO e MLA negli Stati membri (Figura 5.6).

Al seminario è stata, poi, prestata particolare attenzione al rapporto con gli ISPs, quando l'acquisizione di prove digitali coinvolge questo particolare detentore di dati e informazioni (si pensi ai dati relativi alle comunicazioni telefoniche). Sono state poste le seguenti domande:

Q10. Le è mai capitato di cooperare attivamente con gli ISPs per l'acquisizione di una prova digitale?

Q11. Se si, che tipo di dati sono stati richiesti?

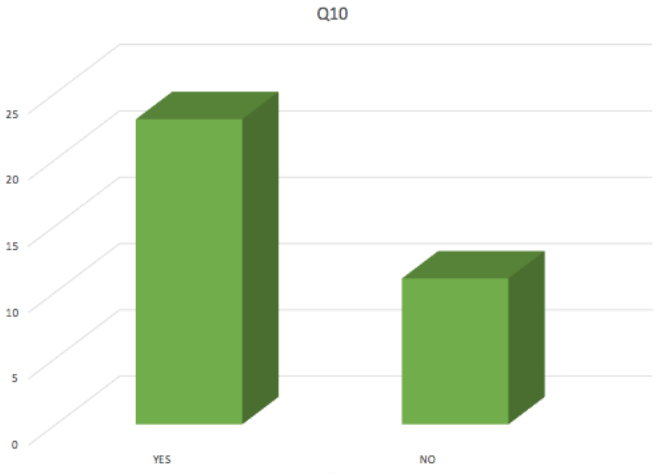

Figura 5.7: Q10 seminario EJTN, collaborazione con ISP

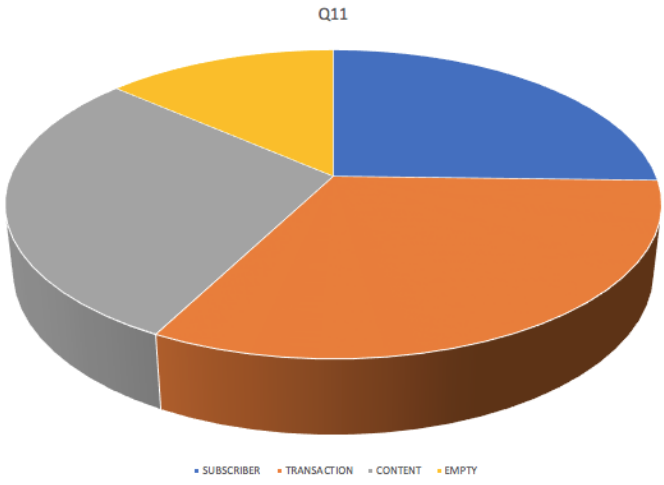

Figura 5.8: Q11 seminario EJTN, tipologia di dati richiesti agli ISPs

Le risposte alle domande hanno confermato che la maggior parte degli Stati membri rappresentati al seminario ha relazioni e attua forme di collaborazione con gli ISPs (Figura 5.7) e che in generale le richieste dirette ai fornitori di servizi di comunicazione sono ampie, in quanto coprono tre tipologie di dati: dati degli abbonati, dati dei contenuti e metadati (Figura 5.8).

Q12. Nel caso vi sia stata cooperazione, quali sono i possibili miglioramenti che riterrebbe opportuni nel rapporto tra autorità giudiziaria e ISP?

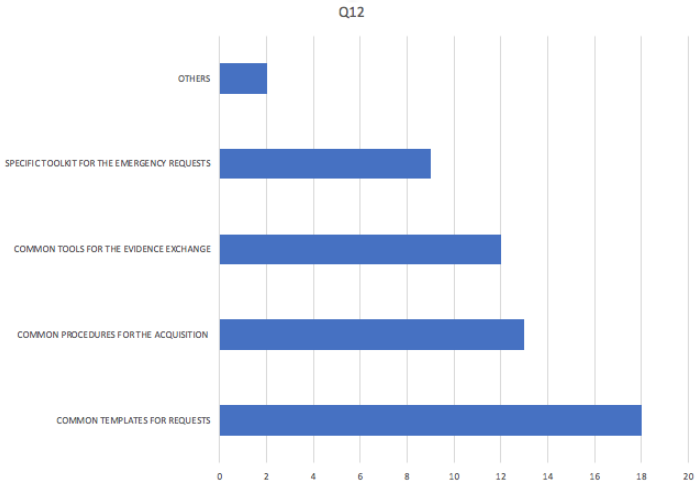

Figura 5.9: Q12 seminario EJTN, miglioramenti rapporto con ISP

Ai partecipanti al seminario è stato chiesto di proporre miglioramenti che secondo la loro opinione potessero contribuire a implementare le relazioni tra autorità giudiziarie e ISPs, per facilitare e rendere più veloce lo scambio dei dati richiesti. La Figura 5.9 mostra che le proposte avanzate sono dirette principalmente a:

- creare modelli comuni per la richiesta di dati agli ISPs;
- concordare procedure comuni per l'acquisizione di dati;
- implementare strumenti comuni per il confezionamento delle prove prima dello scambio;
- implementare strumenti specifici per l'acquisizione di prove in caso di urgenze.

Quasi tutti i partecipanti sono stati concordi nel ritenere di fondamentale importanza avere "template" e "form" comuni nei vari Stati membri per le richieste all'ISP.

Le successive domande miravano ad indagare le modalità e i formati in cui i dati sono trasferiti dall'ISP.

Q13. In che modalità i dati sono trasferiti dagli ISPs?

Q14. In quale formato gli ISPs usano trasferire i dati oggetto della richiesta? (email, PDF, DOC, XLS)

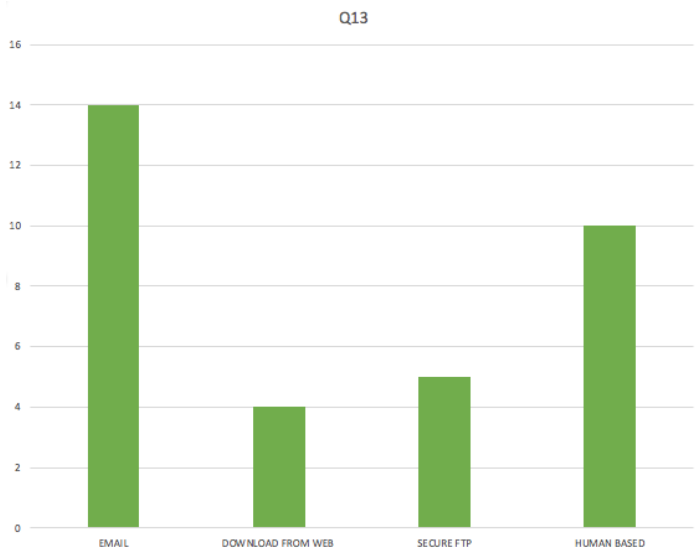

Figura 5.10: Q13 seminario EJTN, modalità di trasferimento dati da parte di ISP

Per quanto riguarda le domande specifiche sulle metodologie utilizzate dagli ISPs per il trasferimento dei dati, i partecipanti al seminario hanno fornito il seguente feedback (Figura 5.10): sono generalmente utilizzati diversi mezzi di trasmissione dei dati da parte degli ISPs alle autorità giudiziarie (posta, mezzi tradizionali, servizio di download dal web su canali sicuri) e sono utilizzati diversi formati dei dati comunicati (PDF, Word, Excel) come mostrato nella figura 5.11.

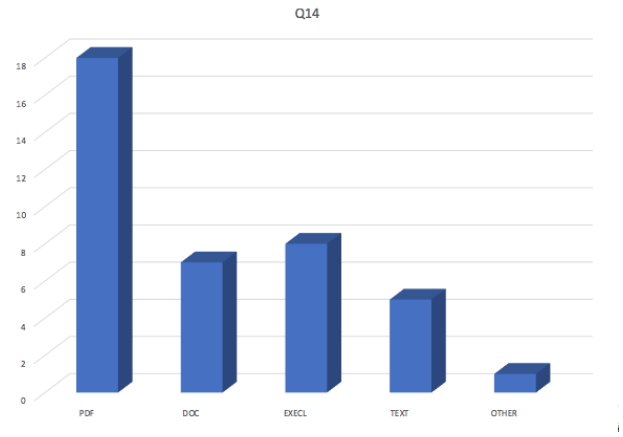

Figura 5.11: Q14 seminario EJTN, formati trasferimento dati ISP

In merito alle attività di formazione in materia di EIO svolte dagli Stati membri coinvolti nel seminario, la domanda Q15 mirava a chiedere un feedback sulle sessioni di formazione esistenti in ciascuno degli Stati rappresentati.

Q15. Nel suo Stato vengono organizzati corsi di formazione in materia di EIO e scambio transnazionale delle prove digitali?

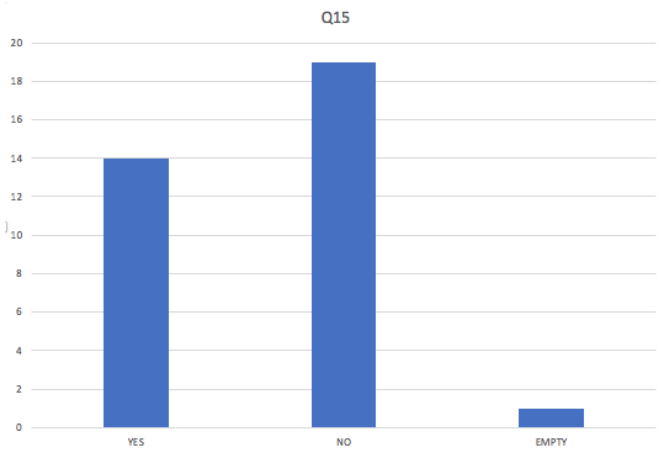

Figura 5.12: Q15 seminario EJTN, corsi di formazione professionale

Nella maggior parte dei casi gli Stati membri hanno dichiarato che i corsi di formazione sull'argomento specifico sopra citato non sono in atto nel proprio paese, mentre solo il 40% dei partecipanti ha dichiarato che ci sono alcune iniziative in corso nei rispettivi paesi.

Per quanto riguarda nello specifico l'organizzazione dei corsi le due successive domande Q16 e Q17 miravano ad indagare le tipologie di soggetti a cui è dedicata l'offerta formativa ed anche gli argomenti trattati nei corsi.

Q16. Nel suo Stato per quali categorie di soggetti vengono organizzati corsi di formazione in materia di EIO e scambio transnazionale delle prove digitali?

Q17. Nel suo Stato quali tipi di argomenti vengono affrontati nei corsi di formazione in materia di EIO e scambio transnazionale delle prove digitali?

I partecipanti al seminario hanno confermato che, laddove organizzati, i corsi di formazione sono diretti principalmente al personale giudiziario e non anche al personale tecnico e amministrativo delle Corti, come mostrato nella figura seguente (Figura 5.13).

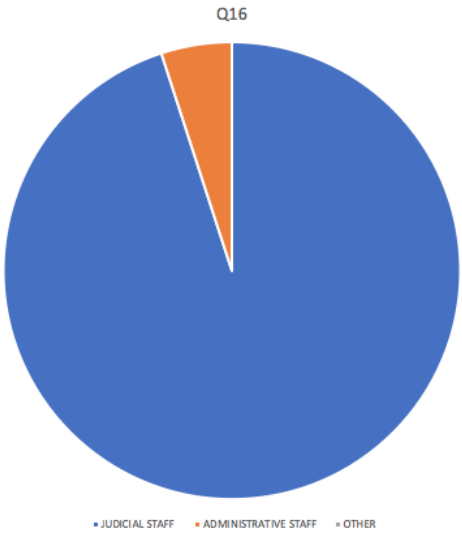

Figura 5.13: Q16, soggetti partecipanti ai corsi di formazione

Più in dettaglio, i risultati del questionario proposto al seminario per la parte relativa alla formazione, hanno confermato che, come risulta anche dal

questionario on-line (Sezione D), la domanda di formazione in materia di EIO è per una ampia e completa copertura di tutte le categorie di soggetti che a vario titolo possono essere coinvolti nelle procedure di EIO. Non soltanto quindi corsi organizzati per giudici e pubblici ministeri, ma anche per il personale tecnico e amministrativo delle cancellerie. Inoltre, per quanto riguarda gli argomenti da trattare nei corsi, le risposte alla domanda hanno confermato il bisogno di formazione non solo sugli aspetti giuridici della procedura ma anche su aspetti tecnici e sullo specifico uso del portale che la Commissione sta realizzando (e-EDES Portal) (Figura 5.14).

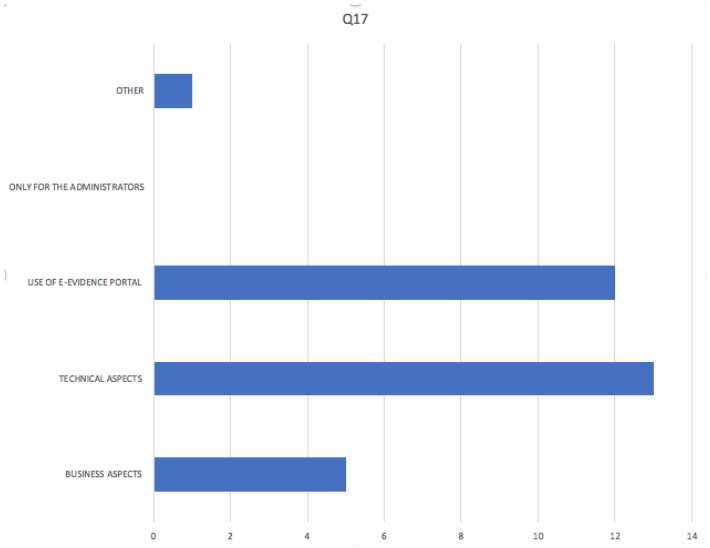

Figura 5.14: Q17 seminario EJTN, argomenti dei corsi di formazione

L'analisi dei risultati delle risposte del seminario organizzato da EJTN confermano i risultati del questionario on-line. Molte delle barriere e ostacoli individuate dalle autorità giudiziarie che hanno partecipato all'indagine on-line sono state ugualmente sollevate dai giudici e pubblici ministeri che hanno aderito all'iniziativa di EJTN.

5.3 I risultati del seminario tecnico organizzato dal CNR in collaborazione con i progetti Evidence2e-CODEX ed EXEC

Il seminario organizzato dal CNR in collaborazione con i progetti europei Evidence2-eCODEX ed EXEC si è tenuto a L'Aia il 20-21 novembre 2018: si è trattato di un meeting dedicato principalmente agli aspetti tecnici delle procedure di EIO e in generale di MLA.

I partecipanti (circa 30 persone) rappresentavano alcune Istituzioni europee che si occupano di cooperazione transfrontaliera: in particolare, erano presenti al seminario membri dell'OLAF, di Europol, di Eurojust ed anche alcuni rappresentanti della Commissione europea che si occupano dell'implementazione dell'e-EDES Portal. In generale, le domande del questionario sono state estrapolate da quello on-line e i risultati sono stati comunicati immediatamente al fine di sollecitare un dibattito costruttivo sulle possibili difficoltà riscontrate.

Le domande che sono state preparate per stimolare il dibattito in aula, sono state le seguenti.

Q1. Quali sono le principali difficoltà da lei incontrate nel trattare prove digitali nell'ambito del processo?

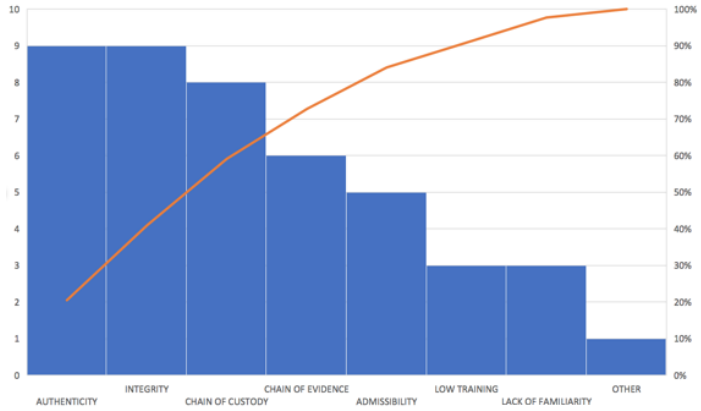

Figura 5.15: Q1 seminario tecnico, possibili difficoltà nel trattamento delle prove digitali

Le risposte della prima domanda Q1 (Figura 5.15), rivelano uniformità con quelle date al seminario EJTN su analoga domanda. Anche in questo caso, l'autenticità e l'integrità delle prove sono i requisiti che maggiormente preoccupano coloro che hanno partecipato al meeting.

Il risultato della seconda domanda (Q2) è riportato nella figura 5.16: la domanda mirava ad indagare quali fossero le principali difficoltà incontrate nello scambio delle prove digitali.

Q2. Nell'ambito delle procedure di EIO o in generale nelle procedure di MLA quali sono state le principali questioni che possono ostacolare lo scambio delle prove digitali con altri Stati?

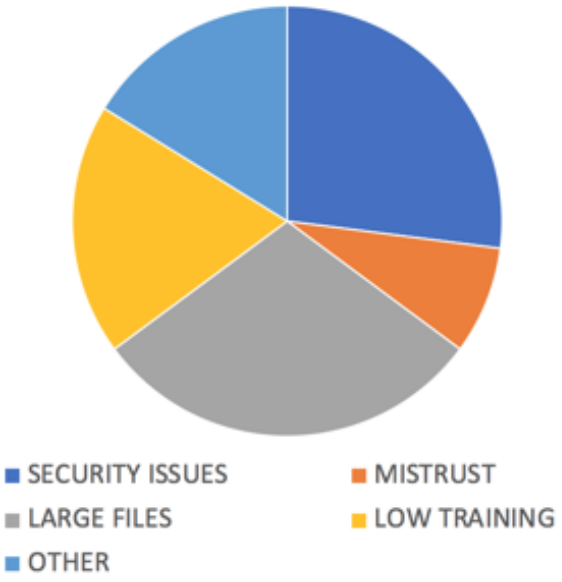

Figura 5.16: Q2 seminario tecnico, difficoltà nello scambio delle prove digitali

Anche in questo caso, le risposte date confermano quelle del seminario EJTN sul tema specifico: le principali difficoltà riscontrate nello scambio delle prove digitali riguardano principalmente lo scambio dei file di grandi dimensioni e la sicurezza dello scambio stesso.

Q3. Quali sono le tipologie principali di tracce digitali che vengono analizzate nel contesto delle procedure di EIO?

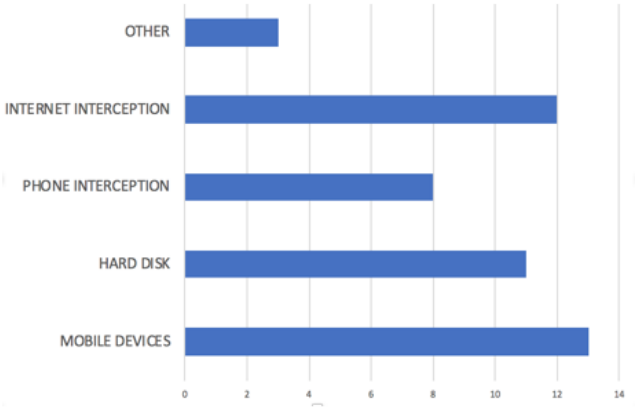

Figura 5.17: Q3 seminario tecnico, principali tracce digitali

Le risposte alla domanda Q3 (Figura 5.17) dimostrano che, principalmente, le tracce digitali sono rilasciate dai dispositivi di telefonia mobile e da Internet (intercettazioni in Internet).

Q4. Nel futuro prossimo, quali secondo lei potrebbero essere le maggiori difficoltà che potranno essere riscontrate da un punto di vista investigativo?

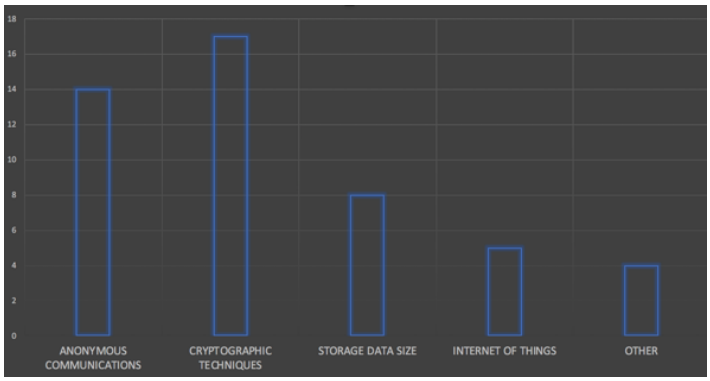

Figura 5.18: Q4, seminario tecnico, future difficoltà tecniche

La domanda forniva le seguenti risposte guidate:
– comunicazioni anonime in Internet
– utilizzo di tecniche avanzate di crittografia
– dimensioni dello spazio di archiviazione dei dati

– "Internet of things"
– altro (si prega di specificare)

Le risposte dei partecipanti al meeting hanno evidenziato che i problemi che dovranno essere affrontati nella fase investigativa riguardano principalmente l'utilizzo da parte della criminalità di tecniche di crittografia avanzate e della comunicazione anonima in Internet.

L'ultima domanda posta ai partecipanti al meeting riguardava i possibili problemi di ammissibilità in giudizio di una prova in ragione della sua natura digitale e degli strumenti informatici utilizzati per la raccolta e trattamento della stessa.

Q5. C'è una crescente necessità di garantire l'affidabilità degli strumenti informatici utilizzati per la raccolta, trattamento e conservazione delle prove digitali potenzialmente connesse ad un reato. Quali regole vengono seguite al fine di garantire che le potenziali prove estratte siano ammissibili dinanzi a un tribunale?

I risultati della domanda Q5 (Figura 5.19) mostrano che nella comunità degli esperti che hanno partecipato al seminario il metodo più utilizzato per garantire la precisione e l'accuratezza dei dati raccolti sia rappresentato da una doppia validazione degli stessi. In altre parole, i dati raccolti vengono analizzati con due diversi "forensics tools" per confermare la validità dei risultati ottenuti.

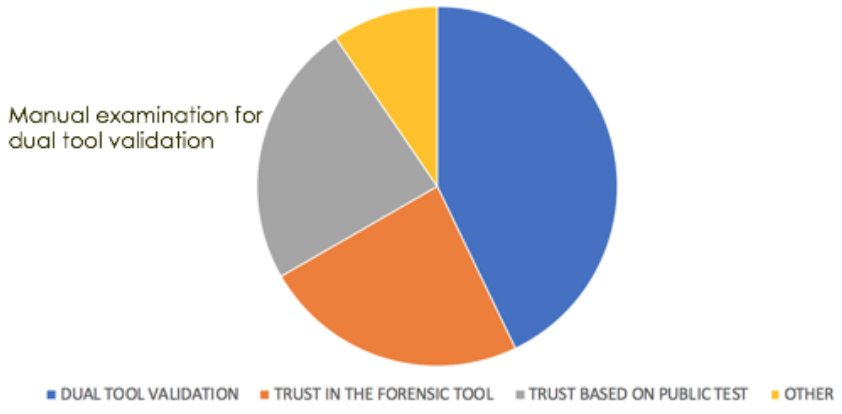

Figura 5.19: Q5, seminario tecnico, metodologie di validazione dei dati raccolti

Anche il quadro delineato nel seminario tecnico sembra confermare i risultati precedentemente riportati, a conferma che nella comunità che si occupa di scambio transnazionale delle prove digitali in contesti penali sono avvertite le stesse difficoltà nelle procedure e sono individuati i medesimi ostacoli per un efficace, veloce e uniforme sistema di scambio in Europa.

La uniformità dei risultati del questionario on line, delle risposte della comunità degli avvocati, dei risultati del seminario EJTN e di quello tecnico, hanno consentito di individuare una serie di potenziali barriere alla creazione di un sistema di scambio uniforme ed efficiente delle prove digitali, barriere alle quali si è cercato di rispondere individuando azioni comuni da attuare a livello nazionale o a livello dell'Unione, che ne consentissero il superamento.

5.4 La proposta per una piena, efficace e uniforme realizzazione dello scambio transnazionale delle prove digitali in ambito penale: strategie e azioni per un quadro comune europeo

Questo paragrafo è dedicato alla presentazione di una proposta di azioni comuni da realizzare a livello nazionale o sovranazionale, volte a superare le barriere e ostacoli individuati dalle risposte ai 4 questionari analizzati nei capitoli e paragrafi precedenti.

Più nello specifico, nella tabella che segue, le barriere emerse dall'indagine svolta sono evidenziate insieme alle possibili azioni da intraprendere e all'attore che dovrebbe essere incaricato di mettere in atto le misure necessarie per superare gli ostacoli che attualmente rallentano la piena, uniforme e completa attuazione dell'EIO. Tali azioni devono essere considerate come suggerimenti per gli Stati membri, la Commissione europea e altri attori coinvolti nelle procedure dell'EIO. Insieme alle possibili azioni da intraprendere è stata indicata nella tabella anche una tempistica per l'attuazione delle misure/strategie indicate.

In particolare, sono state indicate misure a breve termine (che potrebbero essere avviate entro la fine del 2019) e misure a medio termine (che dovranno essere avviate più avanti nel tempo).

Tutti gli elementi individuati (barriere, azioni, attori e tempistiche) sono riportati nel presente lavoro, quale punto di partenza da portare all'attenzione delle Istituzioni europee ed in particolare della Commissione, ma anche degli Stati membri, per essere ulteriormente discussi e concordati al fine di contribuire a realizzare un sistema sicuro ed efficace per lo scambio transnazionale delle prove digitali nei processi penali.

Tabella 5.1: Proposta di azioni comuni

Sezione	Barriera	Azione/i	Attore/i	Tempi realizz.ne
A - Generale	Frammentazione nella normativa nazionale che implementa l'EIO.	Consolidare in un unico atto nazionale delle numerose leggi di recepimento di ciascuno Stato.	Stati membri a livello nazionale	Breve termine
	Mancanza di una versione inglese della legge di implementazione.	Prevedere traduzione ufficiale di legge di implementazione nazionale.	Stati membri a livello nazionale	Breve termine
B1 - EIO & MLA	In caso di parziale sostituzione non sempre è chiaro come le due procedure operano.	Chiarire istituzionalmente quando le procedure di MLA devono essere preferite all'EIO attraverso linee guida per gli operatori del diritto.	Stati membri a livello nazionale	Breve termine
	Gli strumenti di trasmissione delle richieste sono quelli tradizionali (Posta e fax).	Adottare strumenti elettronici quali e-mail per una trasmissione più rapida oppure utilizzare la piattaforma sicura resa disponibile da e-CODEX.	Stati membri a livello nazionale	Breve termine
	Diverse tipologie di form o template per EIO e MLA/Difficoltà di comprensione del contenuto delle richieste per mancanza di modelli uniformi.	Concordare modelli uniformi e comuni per le richieste di MLA anche quando si tratta di richieste verso gli ISPs.	Commissione europea attraverso l'azione di nuovi progetti europei	Breve termine

Continua sulla prossima pagina

Tabella 5.1 – *Continua dalla pagina precedente*

Sezione	Barriera	Azione/i	Attore/i	Tempi realizz.ne
B2 - Procedure emissione/trasmissione EIO	Mancanza di un obbligo generale per l'autorità giudiziaria di inviare report statistici su EIO ad un'autorità centrale nazionale.	Prevedere un obbligo di inviare report all'autorità centrale, definendo modalità uniformi e scadenze specifiche (es. alla fine di ogni anno giudiziario) per tutti gli Stati membri e prevedere la conservazione dei report in un database nazionale.	Stati membri a livello nazionale attraverso il supporto delle iniziative progettuali finanziate dalla Commissione (es. progetto EXEC, Evidence2e-CODEX)	Breve termine
B3 - Autorità competente ad emanare l'EIO	Scarsa chiarezza circa competenze in capo ad autorità amministrative che intervengono nella procedura di EIO come autorità di emissione.	Prevedere azione a livello nazionale per realizzare linee guida e pagine informative sul ruolo delle autorità amministrative nazionali in materia di EIO.	Stati membri a livello nazionale	Breve termine
B4 - Autorità competente ad eseguire l'EIO	Difficoltà di individuazione autorità di esecuzione.	Prevedere best practices affinché ciascuno Stato comunichi regolarmente aggiornamenti su data base istituzionali (ATLAS; EUROJUST) circa le autorità di esecuzione nazionali.	Stati membri a livello nazionale	Medio termine

Continua sulla prossima pagina

Tabella 5.1 – *Continua dalla pagina precedente*

Sezione	Barriera	Azione/i	Attore/i	Tempi realizz.ne
B4 - Autorità competente ad eseguire l'EIO	Obsolescenza e mancanza di granularità delle informazioni disponibili nei sistemi sovranazionali per l'identificazione delle autorità di esecuzione in ciascuno Stato membro (ad esempio indicazione dei punti di contatto nazionali in EJN-Atlas in maniera generica senza indicazione della specifica corte competente o ufficio).	Prevedere best practices per comunicare regolarmente agli organismi che gestiscono e aggiornano i sistemi disponibili in uso (punti di contatto nazionali EJN-Atlas) informazioni sull'autorità di esecuzione competente a livello nazionale (informazioni specifiche e capillari anche sui singoli uffici competenti).	Stati membri a livello nazionale	Breve termine
B5 - Modalità di trasmissione dell'EIO	Modalità di trasmissione prevalentemente tradizionale (posta e fax), con possibili conseguenze negative in caso di trasmissione di file di larghe dimensioni.	Adottare strumenti elettronici quali la posta elettronica laddove la trasmissione sia solo via posta tradizionale o via fax, oppure implementare in ciascuno Stato membro l'uso della piattaforma sicura e affidabile e-CODEX.	Stati membri a livello nazionale con il supporto della Commissione europea per stimolare l'adesione alle iniziative e-CODEX.	Breve termine
	Mancanza di reti di collaborazione stabile, ufficiale e strutturata tra le autorità competenti durante l'esecuzione degli EIO.	Migliorare il dialogo tra le autorità durante l'esecuzione dell'EIO anche laddove questo dialogo esista ma non sia strutturato stabilmente e in maniera uniforme.	Stati membri a livello nazionale attraverso tavoli di lavoro che definiscano linee guida per una stabile e uniforme collaborazione durante l'esecuzione dell'EIO	Breve termine

Continua sulla prossima pagina

Tabella 5.1 – *Continua dalla pagina precedente*

Sezione	Barriera	Azione/i	Attore/i	Tempi realizz.ne
	Mancanza di relazioni istituzionalizzate e regolari tra Stati membri e ISPs.	Creare un framework comune e standardizzato di collaborazione tra autorità competenti degli Stati membri e gli ISPs, al fine di facilitare il flusso di richieste e la consegna dei dati detenuti dagli stessi ISPs.	Commissione europea attraverso l'azione di nuovi progetti europei volti alla creazione di modelli di relazioni strutturate e uniformi tra Autorità giudiziarie nazionali e ISPs.	Medio termine
B6 - Cooperazione con ISP	Utilizzo frammentato di diversi strumenti giuridici per la richiesta di informazioni agli ISPs anche a causa della mancanza di un quadro giuridico comune dell'UE (richieste a testo libero direttamente all'ISP, EIO)	Elaborare linee guida uniformi sugli strumenti giuridici da utilizzare per richiedere dati agli ISPs da parte degli Stati membri dell'UE.	Commissione europea attraverso l'azione di nuovi progetti europei volti alla creazione di modelli di relazioni strutturate e uniformi tra Autorità giudiziarie nazionali e ISPs.	Medio termine
	Diversità di modelli e moduli utilizzati per la richiesta di dati dal momento che manca un "template" comune.	Creare un modello comune e uniforme per la richiesta di dati che gli Stati membri devono utilizzare per ottenere informazioni dall'ISP.	Commissione europea attraverso l'azione di nuovi progetti europei volti alla creazione di modelli di relazioni strutturate e uniformi tra Autorità giudiziarie nazionali e ISPs.	Medio termine
	Utilizzo di diversi mezzi di trasmissione delle richieste e diversi formati dei dati comunicati.	Adottare uno standard formale comune da utilizzare per il confezionamento dei dati e la loro trasmissione elettronica.	Commissione europea attraverso l'azione di nuovi progetti europei volti alla creazione di modelli di relazioni strutturate e uniformi tra Autorità giudiziarie nazionali e ISPs.	Medio termine

Continua sulla prossima pagina

Tabella 5.1 – *Continua dalla pagina precedente*

Sezione	Barriera	Azione/i	Attore/i	Tempi realizz.ne
B7 - EIO e strumenti internazionali di lotta alla criminalità informatica	Nessuna difficoltà o barriera individuata. La Convenzione di Budapest è uno strumento in vigore da molti anni.	Nessuna azione da intraprendere	Nessun attore individuato	Nessuna tempistica indicata
B8 - La lingua dell'EIO	Mancanza di una lingua pivot esistente che consenta uno scambio e una comprensione rapidi delle richieste.	Individuare come obbligatoria una seconda lingua comune da utilizzare in tutti gli Stati membri (ad esempio lingua inglese).	Stati membri a livello nazionale supportati dalla Commissione europea per la creazione di un quadro comune ed uniforme anche per quanto riguarda il linguaggio dell'EIO	Breve termine
	Mancanza di traduttori ufficiali pronti a tradurre la richiesta in modo rapido.	Individuare un elenco di traduttori ufficiali a livello nazionale e formarli in materia di EIO, anche attraverso la collaborazione con la rete di traduttori legali che lavorano già a livello europeo (come quelli di OPOCE o Eur-Lex).	Stati membri a livello nazionale con il supporto della Commissione europea, per la creazione di forme stabili di collaborazione con la rete di traduttori legali ufficiali già esistente (es. quelli dell'OPOCE, di Eur-Lex).	Breve termine
	Mancanza di fiducia, accettazione e utilizzo di strumenti automatici per la traduzione.	Creare strumenti automatizzati affidabili e mirati per la traduzione di EIO anche riutilizzando risorse già esistenti come lo strumento automatico Eur-Lex per la traduzione multilingue della legislazione nazionale.	Commissione europea	Breve termine

Continua sulla prossima pagina

Tabella 5.1 – *Continua dalla pagina precedente*

Sezione	Barriera	Azione/i	Attore/i	Tempi realizz.ne
	Gestione manuale delle procedure EIO/MLA, senza fare affidamento su nuove tecnologie per accelerare le procedure stesse e la speditezza delle indagini.	Promuovere e adottare il sistema di scambio e-Evidence della Commissione e organizzare una formazione efficace sul suo uso, sui benefici e vantaggi che potrebbe portare la sua adozione.	Commissione europea con il supporto degli Stati membri	Breve termine
C - Gli aspetti tecnologici dell'EIO	Scambio di prove digitali, nell'ambito degli strumenti giuridici EIO/MLA, tra diversi Stati membri, ancora prevalentemente basato sull'uomo (corrieri, personale giudiziario autorizzato).	Promuovere e adottare il sistema di scambio e-Evidence della Commissione e organizzare una formazione efficace sul suo uso, sui benefici e vantaggi che potrebbe portare la sua adozione.	Commissione europea con il supporto degli Stati membri	Medio termine
	Scambio di prove in file di grandi dimensioni ancora principalmente basato sull'uomo (corrieri, personale giudiziario autorizzato).	Rafforzare la connettività dei sistemi nazionali per favorire lo scambio anche di file di grandi dimensioni	Commissione europea e Stati membri a livello nazionale	Medio termine
D - Il training in materia di EIO	Mancanza di formazione standardizzata poiché i corsi di formazione esistenti sono sviluppati a livello nazionale senza uniformità generale o accordo tra i vari Stati membri sui programmi dell'offerta formativa.	Creare a livello europeo corsi e elaborare materiali di formazione standardizzati e uniformi da rendere nelle diverse lingue degli Stati membri.	Commissione europea attraverso l'azione di nuovi progetti europei sul training in materia di EIO	Medio termine

Continua sulla prossima pagina

Tabella 5.1 – *Continua dalla pagina precedente*

Sezione	Barriera	Azione/i	Attore/i	Tempi realizz.ne
D - Il training in materia di EIO	Mancanza di visione globale dei soggetti cui dovrebbero essere indirizzati i corsi di formazione, poiché questi ultimi sono organizzati principalmente per il personale giudiziario e non sempre anche per quello amministrativo delle cancellerie.	Coinvolgere tutte le categorie di soggetti che hanno un ruolo nella procedura EIO: autorità giudiziarie, personale amministrativo e tecnico delle cancellerie e avvocati.	Commissione europea attraverso l'azione di nuovi progetti europei sul training in materia di EIO.	Medio termine
	Gli argomenti insegnati durante i corsi di formazione non riguardano tutti gli aspetti dell'EIO, ma sono limitati solo ad alcuni di essi (ad esempio sono organizzati corsi che riguardano gli aspetti giuridici della procedura ma che non toccano quelli che sono gli aspetti tecnici).	Sviluppare corsi di formazione con una copertura completa sugli aspetti rilevanti per l'EIO.	Commissione europea attraverso l'azione di nuovi progetti europei sul training in materia di EIO	Medio termine

Capitolo 6

Profili di "data protection" nello scambio transnazionale delle prove digitali. Analisi dei risultati della sezione E del questionario on-line

Il Capitolo, dopo un'introduzione sulla nuova normativa europea in materia di protezione dei dati personali (Regolamento n. 2016/679/UE e Direttiva n. 2016/680/UE), definisce il rispettivo campo di applicazione dei due atti citati. In particolare, vengono esaminate le norme del Regolamento che si riferiscono espressamente all'attività di trattamento dei dati personali da parte dell'autorità giudiziaria. Successivamente, vengono individuati alcuni concetti chiave presenti in entrambi i provvedimenti, concetti che rappresentano dei punti fondamentali per garantire e sviluppare un adeguato livello di protezione dei dati personali. Ciò a dimostrazione dell'intenzione del legislatore europeo di creare un livello uniforme di tutela nell'ambito dei diversi Stati membri, attraverso l'individuazione di una base comune ed omogenea non solo di regole, ma anche di definizioni in materia di trattamento dei dati personali. Il Capitolo prosegue poi con l'analisi delle disposizioni della Direttiva, specificatamente applicabile nel contesto della "prevenzione, indagine, accertamento e perse-

guimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica", e viene quindi esaminato il rapporto con le procedure di EIO. Infine, vengono analizzate le risposte della sezione E del questionario on-line espressamente dedicata ad indagare la conoscenza della normativa citata da parte dei vari "target groups" coinvolti nelle procedure di EIO [1]

6.1 La legislazione in materia di "data protection": Reg. 2016/679/UE vs. Direttiva 2016/680/UE

Negli ultimi anni, si è assistito nel settore giudiziario ad un forte interessamento verso il tema della protezione dei dati personali. Se da un lato l'uso delle tecnologie della società dell'informazione rappresenta un elemento fondamentale per il miglioramento dell'amministrazione della giustizia, dall'altro esso apre nuovi scenari e questioni delicate per la tutela effettiva dei dati personali. L'utilizzo di strumenti informatici è essenziale per garantire un efficiente funzionamento dell'attività giurisdizionale: ciò si ripercuote in un effettivo accesso alla giustizia per i cittadini, in procedure più snelle e semplici in caso di violazione della legge e infine in una più stretta ed efficace cooperazione delle autorità giudiziarie nazionali tra di loro e tra i diversi paesi dell'Unione europea.

La disponibilità di strumenti che utilizzano web services e sistemi di archiviazione elettronica, la possibilità di scambiare elettronicamente documenti e atti giuridici, nonché l'avvio dei processi telematici mirano sicuramente a supportare coloro che operano nel settore della giustizia, incrementando

[1] Il Capitolo 6 del presente lavoro è il frutto della mia partecipazione alle attività di studio e ricerca condotte nell'ambito dei progetti europei Evidence2e-Codex ed EXEC, nel corso del triennio di dottorato. In particolare, l'analisi condotta e i risultati descritti nel presente Capitolo sono stati presentati ai seguenti seminari/meetings: 1. *Meeting the Technical Community: Validation of the Evidence* (L'Aja, 26-27 marzo 2019) organizzato nell'ambito dei progetti europei Evidence2e-CODEX ed EXEC; 2. *e-Evidence co-funded project coordination Meeting* (Bruxelles, Commissione europea, 23 luglio 2019). Il paragrafo 6.1 del presente lavoro è stato pubblicato in Ginevra Peruginelli, Sara Conti, "L'impatto del Regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale" in Ciberspazio e Diritto, 1-2/2018, Mucchi, pp. 123-139.

l'offerta di adeguati servizi per il cittadino e per un'efficiente e trasparente amministrazione della giustizia. Tuttavia, in tale contesto vengono raccolti, trattati e conservati grandi quantità di dati personali, creando situazioni di estrema ambiguità. Il settore della giustizia dei diversi Stati membri si è trovato fino ad oggi di fronte ad un frammentato panorama normativo in materia di protezione dei dati personali, caratterizzato da differenti approcci nazionali, nonché da diverse procedure relative alla raccolta, gestione e conservazione dei dati personali che comportano, ad esempio, attività autorizzate in uno Stato membro e non permesse in un altro. Il primo tentativo di regolamentare la protezione dei dati personali è stata la Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Questo atto legislativo stabiliva le norme minime sulla protezione dei dati personali in Europa per raggiungere un livello equivalente ed uniforme di protezione in tutti gli Stati membri. L'obiettivo era quello di eliminare le divergenze tra le legislazioni nazionali degli Stati membri in modo da garantire una regolamentazione coerente e comune del flusso di dati personali. Nonostante l'ambizioso proposito, a livello pratico la Direttiva non ha impedito la frammentazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione che le operazioni *online*, in particolare, comportassero rischi per la protezione delle persone fisiche. Trattandosi, com'è noto, di un atto comunitario non direttamente applicabile negli Stati membri, ma suscettibile di trovare attuazione attraverso l'adozione di apposite misure nazionali, le divergenze tra i vari Stati membri nell'attuazione e nell'applicazione della Direttiva hanno contribuito a creare diversi livelli di protezione. Tali criticità in riferimento soprattutto all'effettività della tutela giuridica offerta dalla Direttiva hanno portato il legislatore europeo ad affidare la disciplina di un settore così articolato come quello del trattamento dei dati personali ad un differente strumento normativo, vale a dire il regolamento.

Nel dicembre 2015 è stato completato il processo per concordare una nuova serie di norme volte a riformare il quadro giuridico per garantire il diritto alla protezione dei dati personali dei cittadini dell'UE.

Questo processo ha portato all'emanazione del Regolamento (UE) 2016/679[2] (da ora Regolamento), entrato in vigore il 24 maggio 2016, volto a

[2]Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati): https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA.

rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini dell'Unione europea, sia all'interno sia all'esterno dei confini dell'Unione.

Dal 24 maggio 2018 la Direttiva sulla protezione dei dati del 1995 viene sostituita dal Regolamento che costituisce un atto comunitario dotato, rispetto alla Direttiva, di una maggiore carica di incisività, caratterizzato dall'obbligatorietà di tutti i suoi elementi e dalla diretta applicabilità delle sue disposizioni in tutti gli Stati membri. Il Legislatore europeo delinea così un nuovo quadro normativo che dovrebbe portare maggiore uniformità e, soprattutto, dovrebbe essere più adatto alla rivoluzione portata dalle tecnologie digitali. La diffusione degli ambienti *social*, dell'*Internet of things*, dei *big data* e dei trattamenti automatizzati con finalità di profilazione degli utenti, rappresenta infatti una delle tante nuove sfide che la tutela dei dati personali si trova a dover fronteggiare. L'autorità giurisdizionale, per allinearsi alle nuove regole, deve attivarsi in modo coerente per costruire un vero e proprio processo strutturato di trattamento dei dati che prevede nuovi ruoli, responsabili e responsabilità.

Il Regolamento si definisce come atto di portata generale e quindi non specificamente dedicato all'attività giurisdizionale. In quest'ultimo ambito il Regolamento trova applicazione solo qualora non vi siano provvedimenti nazionali o emanati dall'Unione europea specificatamente dedicati al settore giudiziario. In tale contesto la Direttiva (UE) 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati (da ora Direttiva)[3], si colloca specificatamente nell'ambito della prevenzione e perseguimento dei crimini. Entrambi i provvedimenti si inseriscono all'interno di quello che è stato definito il "Pacchetto europeo protezione dati" che definisce un quadro comune in materia di tutela dei dati personali per tutti gli Stati membri dell'Unione europea.

In altre parole, il Regolamento rappresenta la *lex generalis* in materia di trattamento dei dati personali, mentre la Direttiva (che abroga la decisio-

[3]Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ITA. La Direttiva viene esaminata nel paragrafo 6.2 del presente Capitolo.

ne quadro 2008/977/GAI del Consiglio, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale), si pone come *lex specialis* nell'area della prevenzione e perseguimento dei crimini.

Il Regolamento affianca a norme di carattere generale disposizioni che riguardano anche l'attività giurisdizionale. In particolare, per il primo gruppo il riferimento è alle definizioni di cui all'art. 4, comma 1, nn. 1, 2 e all'art. 5, rispettivamente dato personale, trattamento e principi applicabili al trattamento dei dati.

La nozione di dato personale nel Regolamento, così come quella di trattamento, rappresentano dei concetti chiave che l'autorità giurisdizionale nell'esercizio delle proprie funzioni deve fare propri per comprendere se le operazioni effettuate quotidianamente sui dati personali rientrano o meno nel campo di applicazione della nuova normativa europea. Per quanto riguarda i principi applicabili al trattamento di dati personali, il Regolamento introduce la responsabilizzazione del titolare del trattamento. Qualsiasi titolare, quindi anche l'autorità giurisdizionale, quando compie operazioni sui dati personali deve raccogliere tali dati per finalità determinate, esplicite e legittime e trattare i dati in modo lecito, corretto e trasparente nei confronti dell'interessato, così da garantirne la minimizzazione[4] e l'esattezza rispetto allo scopo per i quali sono raccolti. Il titolare, al tal fine, deve adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti.

Solo attraverso una profonda conoscenza di cosa sono i dati personali e quali sono le operazioni che possono essere effettuate lecitamente[5], l'autorità giurisdizionale è in grado di assicurare il reale rispetto della normativa in materia di protezione dei dati.

Attraverso una semplice analisi testuale del Regolamento sono state individuate alcune disposizioni del Regolamento stesso appartenenti al secondo

[4]I dati personali devono sempre essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (art. 5, co. 1, lettera c, Regolamento). Ogni ulteriore dato richiesto all'interessato oppure ogni ulteriore utilizzo che verrà fatto del dato così ottenuto determinerà una violazione del Regolamento perché eccedente rispetto a quanto strettamente necessario per il raggiungimento di quella finalità come predeterminata e comunicata all'interessato.

[5]Il Regolamento, nell'elencare le operazioni di trattamento all'art. 4, comma 1, n. 2 non pretende di indicare in modo tassativo tutte le operazioni che possono essere compiute sui dati personali.

gruppo di norme, ossia quelle specificatamente dedicate al contesto giudiziario. La ricognizione sembra opportuna poiché l'impostazione del Regolamento non è di facile lettura e le disposizioni sono articolate in affermazioni di principio e numerose specifiche eccezioni.

In particolare, l'analisi è partita dalla ricerca della terminologia che in qualche modo può caratterizzare il contesto in esame, come ad esempio "attività giurisdizionale", "attività giudiziaria", "accertare, esercitare o difendere un diritto", "indagine", "prevenzione", "reati".

La ricerca non ha fornito risultati molto incoraggianti: soltanto 13 disposizioni, su un totale di 173 Considerando e 99 Articoli, sono dedicate esplicitamente a disciplinare il trattamento dei dati personali in ambito giudiziario. Ciò a conferma del fatto che il Regolamento si pone come normativa di carattere generale e come tale si applica ai trattamenti di dati personali effettuati nell'ambito dell'attività giurisdizionale solo qualora non vi siano provvedimenti nazionali o emanati dall'Unione europea specificatamente dedicati al settore giudiziario.

In questa direzione, il Considerando 19 espressamente stabilisce che «la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati sono oggetto di uno specifico atto dell'Unione. Il presente Regolamento non dovrebbe pertanto applicarsi ai trattamenti effettuati per tali finalità. I dati personali trattati dalle autorità pubbliche in forza del presente regolamento, quando utilizzati per tali finalità, dovrebbero invece essere disciplinati da un più specifico atto dell'Unione, segnatamente la Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio».

L'art. 2 comma 2 lettera d) continua ribadendo che «il presente Regolamento non si applica ai trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse».

Il Considerando 20, pur riconoscendo che la normativa introdotta dal Regolamento si applica anche alle attività delle autorità giurisdizionali, lascia al diritto interno degli Stati membri un margine di possibilità per specificare alcune operazioni di trattamento sui dati personali, qualora effettuate da tali soggetti. Il Considerando continua, sottolineando la peculiarità e speci-

ficità dell'autorità giurisdizionale in relazione alle operazioni e procedure di trattamento sui dati personali, ribadendo che «non è opportuno che rientri nella competenza delle autorità di controllo il trattamento di dati personali effettuato dalle autorità giurisdizionali nell'adempimento delle loro funzioni giurisdizionali, al fine di salvaguardare l'indipendenza della magistratura nell'adempimento dei suoi compiti giurisdizionali, compreso il processo decisionale. Si dovrebbe poter affidare il controllo su tali trattamenti di dati ad organismi specifici all'interno del sistema giudiziario dello Stato membro».

La disposizione salvaguarda dunque l'indipendenza dell'autorità giurisdizionale nell'esercizio delle sue funzioni giurisdizionali, escludendo la necessità di sottoporne la supervisione ad un'autorità di controllo salvo che non sia interna allo stesso sistema giudiziario[6]. L'indipendenza, la competenza e l'autonomia sono ancora elementi che sottendono alla esclusione della nomina del Responsabile della protezione dei dati (da ora RPD) prevista dal Considerando 97 e dall'art. 37 per le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali. Dato che il RPD è «... una persona che ha una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento", il Considerando in esame esplicitamente esclude l'assistenza di questo soggetto qualora le operazioni di trattamento siano effettuate da un'autorità giurisdizionale.

Un altro gruppo di disposizioni prevede poi la possibilità di limitare l'esercizio di alcuni dei diritti dei soggetti interessati riconosciuti dal Regolamento, nel caso in cui il trattamento sia effettuato da un'autorità giurisdizionale. Il Considerando 73 stabilisce infatti che «il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e ai diritti di informazione, accesso, rettifica e cancellazione di dati, al diritto alla portabilità dei dati, al diritto di opporsi, alle decisioni basate sulla profilazione, nonché alla comunicazione di una violazione di dati personali all'interessato e ad alcuni obblighi connessi in capo ai titolari del trattamento, ove ciò sia necessario e proporzionato in una società democratica per la salvaguardia della sicurezza pubblica, ivi comprese la tutela della vita umana, in particolare in risposta a catastrofi di origine naturale o umana, le attività di prevenzione, indagine e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica».

[6]In Italia ad esempio il Consiglio Superiore della Magistratura potrebbe svolgere il ruolo di autorità di controllo.

In particolare, con riferimento al diritto del soggetto interessato alla rettifica dei dati personali ed al diritto all'oblio laddove la conservazione di tali dati violi il Regolamento, il Considerando 65 e l'art. 17 comma 3, lettera e) specificano che un'ulteriore conservazione di tali dati dovrebbe essere considerata lecita se necessaria per accertare, esercitare o difendere un diritto in sede giudiziaria.

E ancora l'art. 21 comma 1, n. 1 in materia di opposizione del soggetto interessato al trattamento dei suoi dati personali conferma la liceità della continuazione del trattamento qualora vi sia la necessità di accertare, esercitare o difendere un diritto in sede giudiziaria. Quest'ultimo profilo rileva anche in relazione alla deroga alle disposizioni in materia di trasferimento dei dati verso paesi terzi o organizzazioni internazionali di cui agli artt. 44-50 del Regolamento. L'art. 49 comma 1, lettera e) stabilisce, infatti, che è ammesso il trasferimento di dati personali qualora ciò sia necessario proprio per l'azione in giudizio.

L'art. 23 comma 1, lettera d) e f) rappresenta una disposizione cruciale poiché incide sulla limitazione dei diritti degli interessati previsti dagli Artt. 12-22 del Regolamento. La lettera d) prevede infatti la possibilità di limitare, mediante misure legislative, la portata dei diritti sopra indicati per salvaguardare «la prevenzione, l'indagine e il perseguimento di reati o l'esecuzione di sanzioni, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica». Alla lettera f) è prevista la stessa limitazione con lo scopo di garantire l'indipendenza e autonomia dell'autorità giurisdizionale e dei procedimenti giudiziari in relazione al trattamento dei dati personali. In tale ottica, risulta comprensibile e lecita ad esempio una eventuale limitazione della trasparenza del trattamento dei dati personali al fine di salvaguardare l'attività investigativa.

Infine, l'art. 9 comma 1, lettera f) e il Considerando 52 introducono una deroga al divieto di trattare particolari categorie di dati[7] se «il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali».

[7]Si tratta dei cd. dati sensibili che, ai sensi dell'art. 9 comma 1, possono «rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

Ciò può verificarsi ad esempio nell'ipotesi in cui il trattamento di dati sensibili potrebbe essere reso necessario per l'ammissibilità di prove nel processo.

Dall'analisi testuale effettuata sul testo del Regolamento emergono due elementi fondamentali che sembrano caratterizzare la volontà del legislatore europeo: la salvaguardia dell'indipendenza e autonomia dell'autorità giurisdizionale nell'esercizio delle proprie funzioni e la possibilità di deroghe ad alcune disposizioni del Regolamento e di limitazioni ai diritti riconosciuti agli interessati, al fine di garantire le indagini, la prevenzione e il perseguimento dei crimini.

Nonostante non siano numerose le norme dedicate all'attività di trattamento sui dati personali da parte delle autorità giurisdizionali, tuttavia la necessità di un bilanciamento tra esigenze di trasparenza e quelle di segretezza risulta ben evidenziata. Il diritto alla protezione dei dati personali è un diritto fondamentale dell'Unione europea: le parti del processo hanno diritto a che i loro dati siano debitamente tutelati nel corso delle indagini. Tuttavia esigenze di efficienza ed efficacia della giustizia impongono deroghe e limiti alle disposizioni a tutela del trattamento dei dati personali. Spetta all'autorità giurisdizionale realizzare tale delicato bilanciamento assicurando una corretta applicazione delle disposizioni del nuovo Regolamento.

Tale compito è in linea con gli obiettivi del Regolamento che prevede «la realizzazione di uno spazio di libertà, sicurezza e giustizia» e l'armonizzazione della «tutela dei diritti e delle libertà fondamentali delle persone fisiche»[8], tra i quali è incluso il diritto alla protezione dei dati personali. La consapevolezza dell'importanza di garantire un adeguato livello di protezione dei diritti e delle libertà delle persone fisiche, con particolare riferimento al diritto alla protezione dei dati personali, è infatti considerato elemento fondamentale dell'attività quotidiana delle autorità giurisdizionali.

Inoltre una corretta applicazione delle disposizioni del nuovo Regolamento da parte dell'autorità giurisdizionale implica anche un miglioramento nella libera circolazione dei dati personali tra Stati membri. L'instaurazione e il funzionamento del mercato interno, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, richiedono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano allo stesso tempo tutelati i diritti fondamentali della persona, tra i quali proprio il diritto alla protezione dei dati personali. La

[8]Considerando 2 del Regolamento (UE) 2016/679.

globalizzazione e l'avvento delle nuove tecnologie informatiche hanno condotto a un considerevole incremento dei flussi transnazionali di dati personali. L'importanza di creare un clima di fiducia che coinvolga cittadini, imprese e soggetti pubblici nel trattamento e scambio dei dati personali rappresenta un elemento fondamentale per la realizzazione di una moderna economia digitale. Il Regolamento mira proprio a stabilire regole uniformi per il trattamento dei dati personali, garantendo un elevato livello di protezione e assicurando una libera circolazione nell'ambito dell'Unione europea.

E la Direttiva persegue lo stesso obiettivo nel contesto della prevenzione e perseguimento dei reati.

Ciò che rileva ai fini della definizione dell'ambito di applicazione delle due disposizioni dell'Unione europea è proprio la finalità perseguita dall'autorità giurisdizionale. La Direttiva trova applicazione qualora l'autorità competente agisca a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica. Dove per "autorità competenti", si definiscono soggetti quali la polizia, i pubblici ministeri e i giudici, nell'esercizio di funzioni giurisdizionali legate al perseguimento dei crimini.

Ad esempio, nel caso in cui un'autorità competente effettua il trattamento di dati di lavoratori della stessa per finalità retributive e previdenziali, il Regolamento trova applicazione dal momento che tali attività di trattamento non sono strettamente legate a finalità investigative o di perseguimento di crimini.

Di seguito per chiarezza espositiva vengono individuati alcuni concetti chiave presenti in entrambi i provvedimenti che rappresentano dei punti fondamentali per garantire e sviluppare un adeguato livello di protezione dei dati personali.

La tabella riportata sotto mostra l'intenzione del legislatore europeo di creare un livello uniforme di tutela in materia di trattamento dei dati personali nell'ambito dei diversi Stati membri, tramite l'individuazione di una base comune e omogenea non solo di regole, ma anche di definizioni. Così, l'autorità giurisdizionale del singolo paese può beneficiare di due strumenti di protezione dei dati che si basano su un comune quadro definitorio.

Tabella 6.1: Confronto tra Direttiva (UE) 2016/680 e Regolamento (UE) 2016/679

Direttiva (UE) 2016/680	Regolamento (UE) 2016/679
art. 3, n. 1: Dati personali - «Qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica».	*art. 4, n. 1: Dato personale* - «Qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».
art. 3, n. 2: Trattamento - «Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».	*art. 4, n. 2: Trattamento* - «Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».
art. 10: Trattamento di categorie particolari di dati personali - «Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e solo se si verificano determinate condizioni».	*art. 9 comma 1: Trattamento di categorie particolari di dati personali* - «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il comma 1 non si applica qualora si verifichino determinate condizioni».

6.2 Le disposizioni della Direttiva 2016/680/Ue e la Direttiva sull'EIO

La Direttiva (UE) 2016/680 rappresenta lo strumento introdotto dal Legislatore europeo per la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

Pertanto, rappresenta la normativa di riferimento per il trattamento dei dati personali nel corso delle procedure di EIO.

La Direttiva sull'EIO pone particolare attenzione all'esigenza di assicurare la tutela dei dati personali dei soggetti coinvolti nelle procedure di EIO. In particolare, ai sensi del Recital 40, «la protezione delle persone fisiche in relazione al trattamento dei dati personali è un diritto fondamentale», quindi ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano qualsiasi sia la situazione in cui il trattamento degli stessi venga in rilievo.

A tal fine, il Recital 41 espressamente stabilisce che «gli Stati membri dovrebbero prevedere, nell'applicazione della presente direttiva, politiche trasparenti riguardo al trattamento dei dati personali e all'esercizio del diritto dell'interessato di ricorrere ai mezzi d'impugnazione per la protezione dei propri dati personali».

Infine, il Recital 42 continua affermando che «i dati personali acquisiti ai sensi della presente direttiva dovrebbero essere trattati solamente laddove necessario e in modo proporzionato a fini compatibili con la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali e l'esercizio del diritto di difesa».

Per quanto riguarda le modalità di trattamento dei dati personali nel corso delle procedura di EIO, l'art. 20 della Direttiva 2014/41/UE pone in capo agli Stati membri un obbligo di assicurare che «i dati personali siano protetti e possano essere trattati solo in conformità della decisione quadro 2008/977/GAI del Consiglio»[9]. Decisione che è stata abrogata dalla Diret-

[9]Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale. Si veda https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32008F0977.

tiva 2016/680/UE, che quindi rappresenta la base giuridica del trattamento dei dati personali nel corso dell'emanazione ed esecuzione di un EIO.

Attraverso la regolamentazione del trattamento dei dati personali in ambito penale, la Direttiva 2016/680 si propone di incentivare e al tempo stesso tutelare il libero flusso di dati personali tra le autorità competenti contribuendo a favorire «la costruzione di un quadro comune e uniforme di norme per la protezione dei dati personali nell'Unione»[10].

Al tempo stesso, una corretta regolamentazione della protezione dei dati rappresenta sicuramente un fattore fondamentale «per garantire un'efficace cooperazione giudiziaria in materia penale e in materia di cooperazione di polizia»[11].

Proprio allo scopo di rafforzare la cooperazione giudiziaria in materia penale e per favorire la prevenzione e repressione del crimine, il Recital 44 della Direttiva 2016/680/UE afferma che «gli Stati membri dovrebbero poter adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato o a limitare, in tutto o in parte, l'accesso di questi ai suoi dati personali nella misura e per la durata in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata, per non compromettere indagini, inchieste

[10]Recital 4 della Direttiva: «La libera circolazione dei dati personali tra le autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, inclusi la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, all'interno dell'Unione e il trasferimento di tali dati personali verso paesi terzi e organizzazioni internazionali, dovrebbe essere agevolata garantendo al tempo stesso un elevato livello di protezione dei dati personali. Ciò richiede la costruzione di un quadro giuridico solido e più coerente in materia di protezione dei dati personali nell'Unione, affiancato da efficaci misure di attuazione».

[11]Recital 7 della Direttiva: «Assicurare un livello uniforme ed elevato di protezione dei dati personali delle persone fisiche e facilitare lo scambio di dati personali tra le autorità competenti degli Stati membri è essenziale al fine di garantire un'efficace cooperazione giudiziaria in materia penale e di polizia. Per questo sarebbe auspicabile un livello di tutela equivalente in tutti gli Stati membri dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento dei diritti degli interessati e degli obblighi di tutti coloro che trattano dati personali, nonché poteri equivalenti per controllare e garantire il rispetto delle norme di protezione dei dati personali negli Stati membri».

o procedimenti ufficiali o giudiziari, per non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, per proteggere la sicurezza pubblica o la sicurezza nazionale o per tutelare i diritti e le libertà altrui. È opportuno che il titolare del trattamento valuti, mediante un esame concreto e individuale di ciascun caso, se si debba applicare una limitazione parziale o totale del diritto di accesso».

L'art. 15 conferma le limitazioni del diritto di accesso ai dati sopra indicate: il testo della Direttiva pone quindi limiti che di fatto contribuiscono ad un efficace svolgimento delle indagini e nel caso di EIO, ad un corretto svolgimento delle procedure.

6.3 Analisi della sezione E del questionario: "data protection" e procedure di EIO

Nel contesto sopra descritto si inserisce l'indagine sul livello di conoscenza della normativa europea in materia di protezione dei dati da parte dei partecipanti al questionario on-line.

In particolare, la sezione E di quest'ultimo aveva lo scopo specifico di comprendere in che modo gli Stati membri gestiscono il rapporto tra le richieste EIO e le esigenze di protezione dei dati personali che possono venire in rilievo nel corso delle procedure di scambio delle prove digitali. Dall'analisi delle domande risulta chiara la difficoltà della quasi totalità dei paesi che hanno partecipato all'indagine a rispondere anche alle più semplici delle richieste. Nella maggior parte dei casi, tutta questa sezione E è stata lasciata senza alcuna risposta. I problemi derivano soprattutto dalla mancanza di familiarità con il nuovo regolamento generale sulla protezione dei dati e sulla nuova direttiva.

Nei casi in cui una qualche risposta è stata fornita, tuttavia si trattava di risposte generiche: ad esempio alcuni dei partecipanti hanno semplicemente confermato che le procedure di EIO nel proprio paese si svolgono in un ambiente protetto e sicuro, quindi anche i dati personali che possono venire in rilievo beneficiano di un elevato livello di tutela.

Questa sezione era composta da 17 domande distinte.

Q1. Le prove, e tra queste anche quelle digitali, raccolte mediante un EIO possono contenere dati personali, come nel caso delle informazioni sui conti bancari (considerando 24 della Direttiva EIO), informazioni sulle operazioni

bancarie (considerando 24) e monitoraggio delle operazioni bancarie (articolo 28) o potrebbero riguardare la comunicazione di dati personali (come nel caso di videoconferenze o conferenze telefoniche, del considerando 24). Sapete se vengono condotte verifica periodiche alla luce dei principi di protezione dei dati in relazione alla trasmissione di tali prove?

Q2. In caso affermativo, può fornire una descrizione delle procedure di verifica periodica?

La maggior parte dei paesi ha lasciato queste prime due domande senza risposta, o ha dichiarato di non essere a conoscenza del fatto che la verifica periodica abbia luogo o meno.

Inoltre, in alcuni casi gli Stati membri partecipanti all'indagine hanno sottolineato il fatto che le procedure di scambio delle prove tramite EIO avvengono principalmente "human based", ovvero con l'intervento di corrieri o incaricati dall'autorità giudiziaria appositamente autorizzati al trasferimento di tali prove. Questo secondo le risposte dovrebbe comportare meno rischi per la protezione dei dati personali.

Q3. Ha riscontrato difficoltà/problemi sia nella trasmissione di richieste di EIO che nello scambio di prove in relazione alla protezione dei dati personali in esse contenuti?

Q4. In caso affermativo, può spiegare quali difficoltà ha riscontrato? (Ad esempio, un diverso livello di protezione dei dati nei vari Stati membri).

Nessuno dei partecipanti ha purtroppo dato risposta alle due precedenti domande. Ciò potrebbe essere dovuto da un lato, al fatto che effettivamente le procedure di EIO vengono attuate tenendo in considerazione la disciplina introdotta dalla Direttiva 2016/680/UE. Pertanto, non sorgono particolari difficoltà nella trasmissione di EIO e nello scambio di prove digitali ottenute con tale strumento processuale e vengono rispettate anche le garanzie di tutela dei dati personali. Dall'altro lato, la mancanza di risposta potrebbe anche essere dovuto ad una scarsa conoscenza della normativa in materia di "data protection".

Q5. Esistono garanzie in merito al rispetto dei diritti fondamentali diversi dal diritto alla protezione dei dati personali, direttamente o implicitamente rilevanti nell'EIO?

Anche questa domanda non ha avuto risposta nella maggior parte dei casi.

Soltanto in un caso è stata indicata una possibile salvaguardia a tutela dei diritti fondamentali delle persone, nel contesto dell'EIO.

La garanzia, indicata da un solo partecipante, riguardava il fatto che non sono utilizzati strumenti automatici (o automatizzati) per procedere al controllo delle prove digitali trasmesse, ma è necessario un controllo manuale davanti al giudice. Pertanto l'elemento umano funziona, anche in questo caso, quale garanzia del rispetto dei diritti degli interessati.

Una seconda garanzia menzionata è la disponibilità nel processo di rimedi e strumenti per gli indagati/imputati a tutela dei loro diritti fondamentali.

Q6. Il vostro Stato ha già implementato la direttiva 2016/680/EU (sulla protezione delle persone fisiche per quanto riguarda il trattamento dei dati personali da parte di autorità competenti ai fini della prevenzione, dell'indagine, dell'individuazione o del perseguimento di reati penali o l'esecuzione di sanzioni penali, e sulla libera circolazione di tali dati, e l'abrogazione della decisione quadro del Consiglio 2008/977/JHA)?

Q7. In caso affermativo, può fornire riferimenti relativi (numero e data di pubblicazione) e informare a partire dalla data applicabile alle autorità giudiziarie?

Q8. In caso affermativo, il suo Stato ha una versione ufficiale inglese della legge di attuazione nazionale?

Q9. È disponibile una traduzione non ufficiale in inglese della legge di implementazione?

Le risposte alle serie di 4 domande sopra indicate hanno dimostrato che ormai la maggior parte dei paesi ha attuato la direttiva 2016/680/EU. I partecipanti hanno semplicemente risposto che i rispettivi ordinamenti giuridici hanno adottato leggi di recepimento della stessa, senza specificare poi il provvedimento e se vi sia una versione ufficiale o non ufficiale in inglese dello stesso.

Solo due Stati membri hanno precisato che:

- in Italia la Direttiva è stata attuata con l'emanazione del decreto legislativo numero 51 del 18 maggio 2018[12].
- in Austria la Direttiva è stata attuata con l'adozione del Data Protection Adjustment Act 2018.

[12] Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. Si veda www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018-05-18;51!vig=.

La successiva serie di domande poste ai partecipanti al questionario online mirava ad indagare il livello di conoscenza dei partecipanti sugli aspetti e modalità di operatività della Direttiva.

Purtroppo le varie domande sono state lasciate vuote, a dimostrazione della scarsa conoscenza nei partecipanti all'indagine, della materia e del suo rapporto con le procedure di EIO.

Q10. Il vostro Stato fornisce garanzie più elevate al trattamento dei dati personali da parte delle autorità competenti definite all'art. 3, lett. f, della Direttiva 2016/680/UE, rispetto a quelle stabilite dalla direttiva stessa?

Q11. Quali misure tecniche o organizzative appropriate secondo il disposto dell'art. 4, lett. f, Direttiva 2016/680/UE, sono poste in essere nel suo Stato al fine di garantire un trattamento sicuro dei dati personali?

Q12. Quale limite di tempo prevede la normativa di recepimento del suo Stato per la cancellazione dei dati personali ai sensi dell'articolo 5 della Direttiva 2016/680/UE?

Q13. È a conoscenza di ulteriori misure legislative adottate dal suo Stato secondo l'art. 13 della Direttiva 2016/680/UE? (L'art. 13 stabilisce che gli Stati membri possono adottare misure legislative che possono limitare la comunicazione di informazioni all'interessato laddove ciò sia necessario per le indagini)

Q14. Il suo Stato ha adottato misure legislative che limitano, interamente o in parte, il diritto di accesso ai dati personali che viene ai sensi dell'articolo 15? (Limitazioni al diritto di accesso dell'interessato)

Q15. Si prega di fornire il sito web dell'autorità nazionale per la protezione dei dati.

Q16. Il suo Stato ha altre leggi in materia di protezione dei dati personali, che includano norme per il trattamento dei dati personali in materia di polizia?

Q17. Siete a conoscenza di eventuali decisioni giudiziarie o amministrative sull'attuazione della direttiva 2016/680/EU nel vostro paese? In caso affermativo, si prega di fornire una copia o il riferimento ad un link in cui reperire la risorsa.

L'analisi dei risultati della sezione E del questionario ha senza dubbio rilevato la necessità di organizzare a livello europeo con il supporto degli Stati membri percorsi formativi per giudici e pubblici ministeri che si occupano di EIO, sul tema della protezione dei dati personali.

Capitolo 7

Conclusioni e sviluppi futuri

Il presente lavoro di ricerca si è incentrato sull'analisi delle modalità di raccolta, uso e scambio transnazionale delle prove digitali attraverso l'EIO nei diversi Stati membri.

Nell'intento del Legislatore comunitario l'EIO dovrebbe facilitare la cooperazione giudiziaria in materia penale tra Stati membri, introducendo per la prima volta il principio della disponibilità di misure investigative. La disciplina legislativa introdotta con l'EIO prevede, quindi, la possibilità in capo all'autorità giudiziaria di un Paese di richiedere all'autorità di un altro Paese, che venga effettuata una vera e propria indagine, con eventuale acquisizione di elementi di prova.

In altre parole, si tratta di uno strumento processuale per la ricerca della prova, anche digitale, e per la circolazione probatoria oltre i confini giurisdizionali di ciascuno Stato membro dell'Unione Europea.

Tuttavia, il recepimento dell'EIO negli Stati membri è un processo ancora in divenire, che presuppone l'integrazione di questo nuovo strumento nel diritto nazionale penale di ciascun paese. In particolare, l'EIO deve essere recepito nel diritto processuale penale di ciascuno Stato, che quindi dovrà essere adattato e modificato. Questo processo di adattamento, nonostante l'obiettivo dell'introduzione dell'EIO sia stato quello di incentivare la cooperazione giudiziaria tra Stati, potrebbe comportare nelle procedure nazionali dei vari paesi lievi divergenze. Divergenze che potrebbero ostacolare lo scambio di prove, anche di natura digitale, acquisite attraverso l'EIO.

Le autorità di polizia e quelle giudiziarie si trovano a operare in un quadro normativo incerto: non esiste un quadro giuridico omogeneo fra i vari Stati membri dell'Unione europea, riguardante la raccolta, l'uso e lo scam-

bio di prove digitali. Di volta in volta, si manifesta la necessità di adottare soluzioni che possono anche risultare incoerenti o confuse, sia dal punto di vista giuridico, sia dal punto di vista delle soluzioni tecnologiche.

La prospettiva abbracciata dalla presente ricerca muove proprio da un'analisi delle modalità di implementazione dell'EIO nei vari Stati membri al fine di individuare possibili barriere o ostacoli per la realizzazione di un efficace ed efficiente sistema di scambio delle prove digitali in contesti penali.

Sono state quindi identificate una serie di criticità nel "trattamento" della prova digitale, ad ognuna delle quali è stata data risposta nel presente lavoro, attraverso l'elaborazione di una proposta (una "roadmap"), che contiene strategie ed azioni comuni per superare gli ostacoli individuati.

L'obiettivo, con questo lavoro, è stato proprio quello di individuare e di predisporre una serie di azioni comuni per le autorità giudiziarie degli Stati membri (da realizzare nel medio e lungo termine), che si qualifichino come strumento da percorrere per realizzare una sistematica e uniforme raccolta, ma anche uso e scambio transnazionale delle prove digitali nei processi penali. Al tempo stesso, le strategie elaborate e le azioni individuate nell'ambito di questo lavoro dovrebbero porre le basi per migliorare l'efficienza delle indagini e, in generale, dei procedimenti giudiziari penali, mantenendo le adeguate garanzie a tutela dei diritti fondamentali della persona e rispettando chiari standard operativi di condotta.

L'idea alla base del presente lavoro è stata quella di procedere concretamente (attraverso l'elaborazione di un questionario) a raccogliere da "target groups" specifici, informazioni sulle procedure di EIO nei vari Stati membri. Informazioni che provenivano direttamente da coloro che si trovano quotidianamente ad affrontare questioni connesse all'EIO e allo scambio transnazionale delle prove digitali eventualmente ottenute attraverso questo strumento processuale.

Le risposte provenienti da "target groups" diversi ha permesso di avere un'analisi completa dello "status quo" delle procedure e modalità di attuazione dell'EIO nei vari Stati membri, ricevendo feedback dal lato non solo dei rappresentanti dell'autorità giudiziaria coinvolti nelle procedure di EIO, ma anche rappresentanti dell'Ordine degli Avvocati europei che si occupano della materia, rappresentanti di Istituzioni europee che si occupano di cooperazione transfrontaliera, infine esperti di digital forensics.

Le barriere emerse dall'indagine svolta, come sopra specificato, sono state evidenziate insieme alle possibili azioni da intraprendere e all'attore che

dovrebbe essere incaricato di mettere in atto le misure necessarie per superare gli ostacoli che attualmente rallentano la piena, uniforme e completa attuazione dell'EIO. Gli Stati membri sono i primi attori della realizzazione concreta delle azioni e misure comuni proposte, anche se la Commissione riveste un ruolo fondamentale. In alcuni casi è stata individuata quale promotrice di iniziative volte al superamento di alcuni degli ostacoli individuati, mentre altre volte la sua azione è stata indicata a supporto di quella degli Stati membri.

Insieme alle possibili azioni da intraprendere è stata indicata anche una tempistica per l'attuazione delle misure/strategie indicate.

In particolare, sono state indicate misure a breve termine (che potrebbero essere avviate entro la fine del 2019) e misure a medio termine (che dovranno essere avviate più avanti nel tempo).

La proposta di azioni comuni deve essere considerata come suggerimento per gli Stati membri, la Commissione europea e gli altri attori coinvolti nelle procedure dell'EIO.

Tutti gli elementi individuati (barriere, azioni, attori e tempistiche) sono riportati nel presente lavoro, quale punto di partenza da portare all'attenzione delle Istituzioni europee ed in particolare della Commissione, ma anche degli Stati membri, per essere ulteriormente discussi e concordati al fine di contribuire a realizzare un sistema sicuro ed efficace per lo scambio transnazionale delle prove digitali nei processi penali.

Appendice A

Pubblicazioni

L'attività di ricerca ha prodotto diverse pubblicazioni che sono indicate di seguito:

1. **Sara Conti**. "La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia", in *Informatica e diritto*, 2016, n. 1-2.
2. **Sara Conti**, Sveva Avveduto, Daniela Luzi, Lucio Pisacane. "The conceptual representation of the Electronic Evidence", in M.A. Biasiotti, J.P. Mifsud Bonnici, J. Cannataci, F. Turchi (eds.), *Handling and exchanging electronic evidence across Europe*, Springer International Publisher, 2018.
3. **Sara Conti**, Maria Angela Biasiotti, Fabrizio Turchi. "Electronic Evidence Semantic Structure: Exchanging Evidence across Europe in a coherent and consistent way", in *Proc. of The 16th International Conference on Artificial Intelligence and Law (ICAIL 2017)*, London (United Kingdom), 2018. **(Best paper award)**.
4. **Sara Conti**, Maria Angela Biasiotti, Fabrizio Turchi. "La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno standard", in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime*, Utet giuridica, 2018.
5. **Sara Conti**, Ginevra Peruginelli. "L'impatto del Regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale", in *Ciberspazio e Diritto*, 2018, n. 1-2.
6. **Sara Conti**, Ginevra Peruginelli, "La tutela dei dati personali nel settore giudiziario: l'importanza dei modelli e-learning", in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e Algoritmi. Diritto e diritti nella società digitale*, Il Mulino (in corso di pubblicazione).

Appendice B

Questionario on-line

Nell'Appendice viene riportata la versione integrale del Questionario on-line in lingua inglese, che è stato fatto circolare tra i rappresentanti di 16 Stati membri dell'Unione europea (giudici, pubblici ministeri, personale amministrativo e tecnico delle Corti, esperti di digital forensics). Le domande dei questionari fatti circolare tra gli avvocati del CCBE e nell'ambito di dei due seminari che si sono svolti rispettivamente a Firenze e L'Aja, sono estrapolazioni delle domande della versione integrale del Questionario qui di seguito presentata.

A) GENERAL SECTION

Implementation of the Directive 2014/41/EU
1) Has your State already implemented the EIO Directive? In such case, can you give the pertinent references (number and date of publication) and information on the date from it is applicable to your judicial authorities?
2) Has your State an official English version of the national implementation law? If yes kindly add link or a copy to this questionnaire.

B) LEGAL SECTION

EIO & MUTUAL LEGAL ASSISTANCE INSTRUMENTS (MLA)
Since 22 May 2017, the European Investigation Order has become the single instrument to gather and transfer all types of evidence, including e-evidence, within the EU. Has your State already substituted the MLA instruments with EIO?
Is it a full substitution or a partial substitution?
In case of partial substitution, how are MLA instruments and EIO combined in your national system?
How are MLA requests transmitted? Are electronic means of transmission accepted? Is a legal framework for the use of an online platform required? Are the MLA workflows similar to the EIO ones? Can the same forms of EIO instruments be also used for MLA? If not what else will be used? Please, attach the template used for MLA here
Are there in your State proposal to give consistency to such combined instruments? For examples proposal to adopt the EIO request/sending form in case of MLA request/responding?

Information on EIOs issued and transmitted
Is there a domestic obligation for local authorities to report to a central national authority the number of EIOs issued and received?
If so, do you have the possibility to have statistic reports on the amount of EIOs already issued or received? Can you share these numbers for the purposes of this questionnaire?
If there is not this obligation, is there any other system in place that allows for the gathering of information on the amount of EIOs issued or executed by your local authorities?
Is there any centralized national database or are there local databases for gathering and storing EIOs? In such last case which is the level of de-centralisation (e.g. single databases for each Courts of Appeals, regional databases, etc.)

Information on the Issuing authority
In your State who is the person in charge of requesting the issuing of an EIO (*as for the Directive "the issuing of an EIO may be requested by a suspected or accused person, or by a lawyer on his behalf, within the framework of applicable defence rights in conformity with national criminal procedure*")
In your State which is the authority that is able to issue an EIO (*as for the Directive "issuing authority means: (i) a judge, a court, an investigating judge or a public prosecutor competent in the case concerned; or (ii) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law*). Can you identify who are they?
In case (ii) above mentioned, the issuing authority could be also identified by your State with a competent authority that in the specific case is acting in its capacity as "*an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law".* Can you identify who is such issuing authority in accordance with your domestic law? (e.g. administrative authorities, police officers, etc.)
In this last case before it is transmitted to the executing authority the EIO shall be validated, after examination of its conformity with the conditions for issuing an EIO under this Directive.

Is there any validation procedure by a judicial authority? If yes, is this a judge, court, investigating judge or a public prosecutor?
Is there in your State any procedure by which the issuing authority can find address and routes of the competent authority for the execution of EIO? (e.g. the use of EJN Atlas, Court database, etc.)

Information on the Executing authority
In your State which is the authority having competence to recognize an EIO and ensure its execution? Can you identify who are they?
Is there in your State administrative authority or police officers or other authorities which can issue EIOs?
When executing an EIO, are there any procedures applicable in a similar domestic case which may require a court authorization where provided by your national law?

Transmission of EIOs
How are the EIOs transmitted? Via post? By e-mail? Any other channel of communication?
Do you use any aligned forms for transmitting EIO?
Do you use any automated tool for translations of EIO? If not, can you describe the translation method?
Did you face any difficulties either in the transmission of EIOs or in receiving/sending pieces of execution/e-evidences?
Did you find any difficult in case of large file transmission?

Are you aware of contacts between national/local authorities during the execution of an EIO?
If yes, do you have any information on possible difficulties in establishing these contacts?

Cooperation with Internet service providers and EIO
Do you have any cooperation procedure with ISP in case of EIOs?
If yes, which kind of data does the request of EIO cover? Subscriber data ☐ Metadata (including traffic data, location data and access logs) ☐ Content data? ☐
If you need to acquire data from ISP: Do you send your request directly to ISP? Do you use EIO?
Do you have a standard form for such request or a standard template? Yes, please attach the template Not, free text
Do you have a quick response from the ISP? If not, does the ISP give a motivation for the delay? How ISP transfer you the requested data? In which format? Word, excel pdf other

EIO and Budapest Convention
Is the Budapest Convention implemented in your State?
Article 29 of the Budapest Convention regulates the "expedited preservation of stored computer data". Art. 32 of the EIO regulates the preservation of electronic evidence. How do you apply these two instruments alongside each other in practice?
Art. 34 par. 3 of the EIO Directive specifically establishes that *"in addition to this Directive, Member States may conclude or continue to apply bilateral or multilateral agreements or arrangements with other Member States after 22 May 2017 only insofar as these make it possible to further strengthen the aims of this Directive and contribute to simplifying or further facilitating the procedures for gathering evidence and provided that the level of safeguards set out in this Directive is respected*". Moreover article 34 par. 4 of the EIO Directive establishes that "*Member States shall notify to the Commission by 22 May 2017 the existing agreements and arrangements referred to in paragraph 3 which they wish to continue to apply*". Did your MS notify the use of the Budapest Convention to the Commission (under article 34, para 3 and 4, of the EIO Directive)

Language of EIO
Arr. 5, par. 2 of the EIO Directive: "Each Member State shall indicate the language(s) which, among the official languages of the institutions of the Union and in addition to the official language(s) of the Member State concerned, may be used for completing or translating the EIO when the Member State concerned is the executing State". Has your State notified a second language for the EIO? If your State has indicated only to use its national language, could this represent an obstacle in urgent cases?

C) TECHNICAL/OPERATIONAL SECTION

In case you receive an EIO or a MLA request from another country, how to you deal with it? • [ ] the national IT system can manage much part of the procedure in a digital way in a decentralized way (many national points over the country) • [ ] the national IT system can manage much part of the procedure in a digital way in a centralized way (a single national point over the country)

- [ ] the procedures are manually managed in a traditional way using paper o email system
- [ ] we don't manage these cases at the moment
- [ ] other (please specify)

e-Evidence project, together with other European projects, is going to provide a service for handling EIO and MLA in a digital and secure way over e-CODEX infrastructure as a transmission channel. Does your country have the intention to join this initiative/project?

- [ ] We have already joined the initiative
- [ ] We have participated to e-CODEX meetings and we are deciding about joining the initiative
- [ ] We have participated to e-CODEX meetings but we don't have decided to join yet
- [ ] We have participated to e-CODEX meeting but we won't join the initiative due to shortage of resources (human and/or financial)
- [ ] We do not know the e-CODEX project
- [ ] Other (please specify)

Within the EIO and/or MLA procedures how do you exchange digital evidence relevant for a case under investigation with another country?

[ ] we seized the potential evidence and preserve it until some authorized person from the Issuing State comes and bring it to their national forensic laboratories.
[ ] if requested we create a forensic copy of the seized source of evidence (hard disk, smartphone, etc.) and then some authorized person from the Issuing State comes and bring it to their national forensic laboratories.
[ ] if the size of the evidence is not too large we send it to the requesting authority by email, secure cloud with encryption key or password transmitted through different channels (email, phone, etc.)
[ ] it has never happened so far
[ ] other (please specify)

Within the EIO and/or MLA procedures how do you exchange large-sized file (i.e. an acquisition from a smartphone of 16GB) of digital evidence with another country?

[ ] the large-sized are exchanged relying on traditional ways (secure courier, by hand with an appointed/authorized person of the requesting country, etc.)
[ ] we use a secure private cloud storage
[ ] we use a technology for splitting the file in little parts (torrent, etc.)
[ ] it has never happened so far[ ]
[ ] other (please specify)

Can you provide some metrics ?
[ ] Number of cases requiring transfer of electronic evidence?
[ ] Average size of a file;
[ ] Max size;
[ ] Max Number of attachments files allowed
[ ] Allowed formats for attached files

Is there any legal constraints for non-repudiation in Court?
[ ]Yes
[ ]No

If yes, please specify the procedure
Does your country use a digital platform for handling EIO and MLA procedures? [ ] We will use e-CODEX [ ] We will use our national platform [ ] we will use the reference portal built by the European Commission
Connectivity Which is the available speed connection available in your office/system? [ ] 1 giga bits per second [ ] between 500 and 800 mega bits per seconds [ ] between 200 and 500 mega bits per seconds [ ] between 100 and 200 mega bits per seconds [ ] between 50 and 100 mega bits per seconds [ ] less than 50 mega bits per seconds [ ] I do not know
Encryption Which kind of encryption methods do you use in your national system for protecting the transmission of sensible data? [ ] encryption based on asymmetric keys [ ] encryption based on symmetric keys [ ] encryption based on asymmetric and symmetric keys [ ] I do not know What is encrypted? How? How is it managed?
Authentication Which kind of authentication methods do you use in your national system for protecting the access to sensible data or protected areas? [ ] providing user and password on secure channel (TLS) [ ] a two factors methods based on token online or offline [ ] a two factors methods based on biometrics system [ ] I do not know
Electronic Signature Do you use electronic signature? What is the minimal requirement in your country? What is used in your country: ink, e-sign, other? In case your country can not accept or verify the electronic signature in place in another country, can you accept electronic exchange to speed up the procedure and then follow up with paper procedures (yes, no, comment)?

D) ADMINISTRATIVE SECTION

Training sessions on EIO
How is the training of issuing/executing authorities on the EIOs organized in your State?
Do you know who are the trainers? Which category/target group they belong to?
Are the training sessions organized only for judicial staff? If not, who are the other categories/target groups involved? (for example, administrative staff of the issuing/executing authority)
From your experience, do you think that trainings should focus on: [ ] business aspects [ ] technical aspects [ ] use of the e-Evidence portal [ ] training only for the Admin of the users Any other suggestion
Are you aware that in your country the EC will prepare training materials on the topic to the attention of MS?

E) DATA PROTECTION ISSUE AND EIO

Evidence and e-evidence collected by way of an EIO may contain personal data, as in the case of information on bank accounts (Recital 24), information on banking transactions (Recital 24) and monitoring of banking transactions (Article 28) or could cover the communication of personal data (as in the case of video or telephone conference, set out in Recital 24). Do you know if periodical verification in light of the data protection principles are conducted related to transmission of those evidences? If yes, can you give a description of the procedures of periodical verification?
Did you face any difficulties/problems either in the transmission of EIOs or in receiving/sending pieces of execution/e-evidences concerning data protection issues?

If yes, can you please explain which difficulties you dealt with? (For example a different level of data protection in another Member State)

Are there any safeguards regarding to other fundamental rights directly or implicitly referred to in the EIO?

Did your State already implement Directive 2016/680/EU (on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA)?

If yes, can you please give pertaining references (number and date of publication) and inform from which date is it applicable to your judicial authorities?

If so, has your State an official English version of the national implementation law? If yes, kindly add link or a copy to this questionnaire.
Is there an unofficial English translation of the implementation law available?

If yes:

- Does your State provide higher safeguards to the processing of personal data by competent authorities according to Article 1 Paragraph 3, than those established in this Directive?
- Which appropriate technical or organizational measures according to Article 4 Paragraph 1 lit. f, does your state provide for ensuring a secure processing of personal data?
- Which time limit does your state schedule for the erasure of personal data according to Article 5?
- Are you aware of any further legislative measures based on Article 13 Abstract 3 and 4?
- Did your state adopt any legislative measures restricting, wholly or partly, the data subject's right of access to the personal data that is being processed according to Article 15?
- Please provide the website of the data protection authority.

If no:

Does your State have any other data protection legislation that includes regulations for the processing of personal data in Police Matters?

Are you aware of any court or administrative decisions on the implementation of Directive 2016/680/EU in your country? If yes, please provide a copy or a link.

Bibliografia

1. Allegrezza S., "Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality", in Ruggeri S. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Springer, 2014
2. Amalfitano C., "Codice di cooperazione giudiziaria penale dell'Unione europea", Giappichelli, 2017
3. Asaro C., "Sul cammino tracciato da Evidence", in *Informatica e diritto*, 2016, n. 2
4. Aulitano S., "E-evidence in the European Union", in De Zan T.-Aulitano S., *EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace*, Documenti IAI, 16/17 novembre 2016
5. Belfiore R., "Critical Remarks on the Proposal for a European Investigation order and Some Considerations on the Issue of Mutual Admissibility of Evidence", in Ruggeri S. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Springer, 2014
6. Belfiore R., "Su alcuni aspetti del decreto di attuazione dell'ordine europeo di indagine penale", in *Cassazione penale*, 2018, n. 1
7. Bene T., Luparia L., Marafioti L., "L'ordine europeo di indagine penale. Criticità e prospettive", Giappichelli, 2017
8. Bergonzi Perrone M., "Il mancato rispetto delle disposizioni della Legge n. 48 del 2008 in tema di acquisizione probatoria informatica: per una ipotesi sanzionatoria non prevista esplicitamente dal dato normativo", in *Ciberspazio e diritto*, 2013, n. 1

9. Biasiotti M.A., Conti S., Turchi F., "Electronic Evidence Semantic Structure: Exchanging Evidence across Europe in a coherent and consistent way", in *Proc. of The 16th International Conference on Artificial Intelligence and Law (ICAIL 2017)*, London, 2018. (Best paper award).
10. Biasiotti M.A., Mifsud Bonnici J.P., Cannataci J., Turchi F., "Handling and Exchanging Electronic Evidence Across Europe", Law, Governance and Technology Series, Vol. 39, Springer, 2018
11. Biasiotti M.A., Conti S., "The New Regulation on Data protection. The Italian case (Italien)", in Forgò, Helfrich, Schneider (eds.), *Betrieblicher datenschutz*, third ed., Beck, 2019
12. Biasiotti M.A., "Presente e futuro dello scambio della prova digitale in Europa", in Biasiotti M.A., Epifani M., Turchi F., *Trattamento e scambio della prova digitali in Europa*, numero monografico di Informatica e Diritto, 2016, n. 1-2
13. Biasiotti M.A., "Opportunità e sfide per la prova elettronica", in Biasiotti M.A., Epifani M., Turchi F., *Trattamento e scambio della prova digitali in Europa*, numero monografico di Informatica e Diritto, 2016, n. 1-2
14. Biasiotti M.A., Epifani M., Turchi F., "Trattamento e scambio della prova digitali in Europa", numero monografico di Informatica e Diritto, 2016, n. 1-2
15. Bolognari M., "Ordine europeo di indagine penale ed esame a distanza", in *Rivista di diritto processuale*, 2018, n. 4-5
16. Bolognari M., Caianello M. et al., "L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. 108 del 2017", Giappichelli, 2018
17. Bonfanti A., "Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali", in *La rivista di diritto dei media*, 2018, n. 3
18. Bonnici J.P., Tudorica M., Cannataci J., "La regolamentazione delle prove elettroniche nei processi penali in "situazioni transnazionali": problemi in attesa di soluzioni", in Biasiotti M.A, Epifani M., Turchi F., *Trattamento e scambio della prova digitali in Europa*, numero monografico di Informatica e Diritto, 2016, n. 1-2
19. Cadoppi A., Canestrari S., Manna A., Papa M., "Cybercrime", UTET Giuridica – Collana Ominia, Trattati giuridici, 2018

20. Camaldo L., "La direttiva sull'ordine europeo di indagine penale (EIO): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione", in www.penalecontemporaneo.it, 2014
21. Camaldo L., "La normativa di attuazione dell'ordine europeo di indagine penale: le modalità operative del nuovo strumento di acquisizione della prova all'estero", in *Cassazione penale*, 2017, n. 1
22. Camaldo L., "Mandato d'arresto europeo e investigazioni difensive all'estero", Giuffrè, 2018
23. Caringella F., Falato F., "Scritti di cooperazione giudiziaria penale", Dike Giuridica, 2018
24. Carrier B.D., "Defining Digital Forensic Examination and Analysis Tool Using Abstraction Layers", in *International Journal of Digital Evidence*, Vol. 1, 2003, n. 4
25. Carrier B.D., "A Hypothesis-based Approach to Digital Forensic Investigations", CERIAS Tech Report 2006-06, disponibile su www.cerias.purdue.edu/assets/pdf/bibtex_archive/2006-06.pdf
26. Casey E., "Foundations of Digital Forensics", in Casey (ed.), *Digital Evidence and Computer Crime*, III ed., Waltham, Academic Press, 2011
27. Casey E., "Digital Evidence and Computer Crime. Forensic Science, Computers, and the Internet", Elsevier, III ed., 2011
28. Clough J., "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization", in *Monash University Law Review*, Vol. 40, 2014, n. 3
29. Colaiocco A., "La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria", in *Archivio penale*, 2019, n. 1
30. Comellini S., "Il Regolamento Generale sulla Protezione dei dati personali e la nomina del DPO nella Pubblica Amministrazione", Maggioli, 2018
31. Daniel L., Daniel L., "Digital Forensics for Legal Professionals. Understanding Digital Evidence from the Warrant to the Courtroom", Syngress, 2012
32. De Amicis G., "Limiti e prospettive del mandato europeo di ricerca della prova", in Grasso G., Picotti L., Sicurella R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Giuffrè, 2011

33. De Amicis G., "Dalle rogatorie all'ordine europeo di indagine: verso un nuovo diritto della cooperazione giudiziaria penale", in *Cassazione penale*, 2018, n. 1
34. De Hert P., Ganzalez Fuster G., Koops B.-J., "Fighting Cybercrime in the Two Europes. The Added value of the EU Framework Decision and the Council of Europe Convention", in *International Review of Penal Law*, Vol. 77, 2006, n. 3-4
35. De Gregorio E., "Riflessioni in tema di attualità e prospettive della raccolta e dello scambio della prova digitale", in *Informatica e diritto*, 2016, n. 2
36. Espina Ramos J.A., "The European Investigation Order and its Relationship with Other Judicial Cooperation Instruments", Eucrim platform, The European Criminal Law Association's Forum, 1-2019
37. Falato F., "Appunti di cooperazione giudiziaria penale", II ed., Edizioni Scientifiche Italiane, 2019
38. Finocchiaro G., "Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017
39. Graziani F., "L'acquisizione della prova digitale all'estero: verso un secondo protocollo addizionale alla convenzione di budapest sul cybercrime", in Marchisio S., Montuoro U., *Lo spazio cyber e cosmico*, Giappichelli, 2019
40. Guerra J.E., Janssens C., "Legal and Practical Challenges in the Application of the European Investigation Order", Eucrim platform, The European Criminal Law Association's Forum, 1-2019
41. Haapio, H., Passera, S., "Visual Law: What Lawyers Need to Learn from Information Designers", 2013, https://blog.law.cornell.edu/voxpop/2013/05/15/visual-law-what-lawyers-need-to-learn-from-information-designers
42. Hense-Ler J., "Computer Crime and Computer Forensics", in *The Encyclopedia of Forensic Science*, Academic Press, 2000
43. Hoofnagle J., van der Sloot B., Zuiderveen Borgesius F., "The European Union general data protection regulation: what it is and what it means", in *Information & Communications Technology Law*, Vol. 28, 2019, n. 1, https://www.tandfonline.com/author/Borgesius%2C+Frederik+Zuiderveen
44. Keyser M., "The Council of Europe Convention on Cybercrime", in *Journal of Transnational Law & Policy*, Vol. 12, 2003, n. 2

45. Koops B.-J.,Robinson T., "Cybercrime: A European perspective", in Casey E. (ed.), *Digital Evidence and computer crime*, III ed., 2011
46. Kostoris R., Marcello D., "L'ordine di indagine penale", Giappichelli, 2018
47. Kusak M., "Mutual admissibility of evidence and the European investigation order: aspirations lost in reality", ERA Forum, published on-line 7 Jan 2019
48. Labianca D., "Il Sistema delle tutele nel Regolamento europeo sulla protezione dei dati personali", in Cadoppi A., Canestrari S., Manna A., Papa M., *Cybercrime*, UTET Giuridica – Collana Ominia, Trattati giuridici, 2018
49. Magno T., "Il progetto Evidence e le principali criticità nell'accesso alle prove elettroniche transnazionali in materia penale: quale futuro?", in *Informatica e diritto*, 2016, n. 2
50. Manes V., Mezzacuva F., "GDPR e nuove disposizioni penali del Codice privacy", in *Diritto penale e processo*, 2019, n. 2
51. Mangiaricina A., "L'acquisizione europea della prova cambia volto: l'Italia attua la direttiva relativa all'ordine europeo di indagine penale", in *Diritto e processo*, 2018, n. 2
52. Marcello D., "L'impatto dell'ordine europeo di indagine sulle regole probatorie nazionali", in *Diritto penale contemporaneo*, 2016, n. 3
53. Marchetti M.R., Selvaggi E., Barrocu G., "La nuova cooperazione giudiziaria penale. Dalle modifiche al codice di procedura penale all'ordine europeo d'indagine", CEDAM, 2019
54. Marchetti M.R., "Ricerca e acquisizione probatoria all'estero: l'ordine europeo di indagine", in *Archivio penale*, 2018, n. 1S
55. Maranella S., "La cooperazione di polizia e giudiziaria in materia penale nel sistema dell'Unione Europea", L'Harmattan Italia, 2018
56. Marion N.E., "The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation", in *International Journal of Cyber Criminology*, Vol. 4, 2010, n. 1-2
57. Mason S., "Electronic Evidence", III ed., LexisNexis Butterworths, 2012
58. Molinari F.M., "Le attività investigative inerenti alla prova di natura digitale", in *Cassazione penale*, 2013, n. 3
59. Montero Garcimartín R., "The European Investigation Order and the Respect for Fundamental Rights in Criminal Investigations", in *The*

European Criminal Law Associations Forum (published by Max Planck Society for the Advancement of Science), 2017

60. Murphy C.C., "The European Evidence Warrant: Mutual Recognition", in Eckes C., Konstadinides T. (eds.), *Crime within the area of freedom security and justice. A European public Order*, Cambridge University Press, 2011
61. Oberto G., "La formazione professionale dei magistrati italiani nell'ottica della formazione del giurista europeo", relazione presentata al Convegno sul tema *Verso l'Unione Europea della giustizia – Zur europäischen Union der Justiz* organizzato dal Goethe Institut di Torino in collaborazione con il Deutscher Richterbund e l'Associazione Nazionale Magistrati (Torino, 8-9 novembre 2002)
62. Peruginelli G., Conti S., "INFORM: un modello e-learning per la formazione continua nel settore giudiziario", in *Scienza in rete*, https://www.scienzainrete.it/articolo/inform-modello-e-learning-formazione-continua-campo-giudiziario/ginevra-peruginelli-sara, 8 marzo 2019
63. Peruginelli G., Conti S., Francesconi E., "The e-learning approach and visualisation techniques in the judicial area", in *Journal of Open Access to Law*, special issue on Visual Law, Vol. 7, 2019, n. 1, https://ojs.law.cornell.edu/index.php/joal/issue/view/8
64. Piana D., "La formazione giudiziaria in Italia, fra politiche di qualità e vischiosità istituzionali", in *La Magistratura*, 2008, n. 1
65. Pisapia A., "La tutela per il trattamento e la protezione dei dati personali", Giappichelli, 2018
66. Poritskiy N., Oliveira F., Almeida F., "The benefits and challenges of general data protection regulation for the information technology sector", in *Digital Policy, Regulation and Governance*, Vol. 21, 2019, n. 5
67. Richardson J. (ed.), "Archbold: Criminal Pleading, Evidence and Practice", Sweet & Maxwell, Thomson Reuters, 2009
68. Ryolo L.A., "European Investigation Order: The Defence Rights Perspective", in Ruggeri S. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Springer, 2014
69. Rucker D., Kugler T., "New European General Data Protection Regulation, a Practitioner's Guide: Ensuring Compliant Corporate Practice", C.H. Beck, 2018

70. Ruggieri F., "Processo penale e regole europee", Vol. II, Giappichelli, 2018
71. Ruggieri F., "Le nuove frontiere dell'assistenza penale internazionale: l'ordine europeo di indagine penale", in *Processo penale e giustizia*, 2018, n. 1
72. Ruggeri S., "Introduction to the Proposal of a European Investigation Order: Due Process Concerns and Open Issues", in Ruggeri S. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Springer, 2014
73. Sayers D., "The European Investigation Order: Travelling without a roadmap", CEPS, Liberty and Security in Europe, https://www.ceps.eu/ceps-publications/european-investigation-order-travelling-without-roadmap, 2011
74. Schünemann B., "The European Investigation Order: A Rush into the Wrong Direction", in Ruggeri S. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Springer, 2014
75. Schafer B., Mason S., "The characteristics of digital evidence", in Mason S., *Electronic Evidence*, III ed., LexisNexis Butterworths, 2012
76. Selvaggi E., "L'ordine europeo di indagine - EIO: come funziona?", in *Cassazione penale*, 2018, n. 1
77. Siracusano F., "Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale", in *Archivio penale*, 2017, n. 2
78. Sottani S., "La formazione permanente dei magistrati. Esigenze formative", in *Questione giustizia*, 2016, n. 1
79. Teixeira G.A., Mira da Silva M., Pereira R., "The critical success factors of GDPR implementation: a systematic literature review", in *Digital Policy, Regulation and Governance*, Vol. 21, 2019, n. 4
80. Tinoco Pastrana A., "L'ordine europeo di indagine penale", in *Processo penale e giustizia*, 2017, n. 2
81. Torre M., "Indagini penali e processo penale", tesi di dottorato in Scienze giuridiche (Università di Firenze), 2015
82. Torre M., "La raccolta della prova digitale in Italia: dagli accertamenti statici al captatore itinerante", in *Informatica e diritto*, 2016, n. 2

83. Torre M., "Protezione dei dati personali, processo penale e intercettazioni", in *Diritto penale e processo*, 2019, n. 2
84. Vermeulen G.-De Bondt W.-Van Damme Y., "EU Cross-Border Gathering and Use of Evidence in Criminal Matters: Towards Mutual Recognition of Investigative Measures and Free Movement of Evidence?", IRCP-series, Vol. 37, Maklu Publishers, 2010
85. Vogler R., "The European Investigation Order: Fundamental Rights at Risk?", in Ruggeri S. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Springer, 2014
86. Voigt P., von dem Bussche A., "The EU Genaral Data Protection regulation (GDPR)", Springer, 2017
87. Weber A.M., "The Council of Europe's Convention on Cybercrime", in *Berkeley Technology Law Journal*, Vol. 18, 2003, n. 1
88. Winter L.B., "The Proposal for a Directive on the European Investigation Order and the Grounds for Refusal: A Critical Assessment", in Ruggeri S. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Springer, 2014