LUISS

Corso di laurea in Giurisprudenza

Cattedra di Diritto Processuale Penale

La Prova Digitale nel Procedimento Penale:

profili critici e prospettive future tra confini europei e nazionali

Prof. Alberto Macchia

RELATORE

Prof. Filippo Dinacci

CORRELATORE

Nicole Visco Comandini

Matr. 156083

CANDIDATO

Anno Accademico: 2022/2023

Indice

Lista di abbreviazioni

"*BBW*"	*Big Brother Watch e altri c Regno Unito;*
"BGH"	Corte di Cassazione tedesca;
"Carta"	Carta dei diritti fondamentali;
"CEDU"	Convenzione Europea dei Diritti Umani;
"CGUE"	Corte di Giustizia dell'UE;
"Codice della Privacy"	Decreto legislativo 30 giugno 2003, n. 196;
"Convenzione di Budapest"	Council of Europe, Convention on Cybercrime (Budapest Convention on Cybercrime) (2001) ETS No 185;
"Corte EDU"	Corte Europea dei Diritti Umani;
"cpp"	codice di procedura penale;
"Direttiva e-Privacy"	Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche OJ L 201/37;
"DOEI"	Direttiva che introduce lo strumento dell'Ordine Europeo di Indagine;
"Guida"	Electronic Evidence Guide (2014) <https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf> ultimo accesso 29 settembre 2023;
"HR"	Corte Suprema olandese;

"LQDN"	*La Quadrature du Net;*
"MAE"	Mandato di Arresto Europeo;
"OEI"	Ordine Europeo di Indagine;
"orientamento generale"	European Parliament, 'Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters' [2020] < https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html#_section1> ultimo accesso 29 settembre 2023;
"PI"	*Privacy International;*
"Relazione"	European Parliament, 'Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters'[2020] <https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html#_section1> ultimo accesso 29 settembre 2023;
"SIC"	Squadre Investigative Comuni;
"SLSG"	Spazio di Libertà, Sicurezza e Giustizia;
"TFUE"	Trattamento sul Funzionamento dell'UE;
"TUE"	Trattato sull'UE; e
"UE"	Unione europea.

Introduzione

Il progresso scientifico ha da sempre svolto un ruolo fondamentale nel procedimento penale, contribuendo alla creazione di innovativi mezzi di ricerca della prova e alla definizione di nuove categorie probatorie.[1] Tuttavia, l'avvento della c.d. "era digitale" ha rivoluzionato in modo senza precedenti il panorama del diritto penale sia sostanziale che procedurale.[2]

L'inarrestabile progredire delle tecnologie digitali ha portato all'affermarsi di inedite categorie di reato – appartenenti al reame della c.d. "criminalità informatica" – caratterizzate dall'impiego, ai fini della loro commissione, di strumenti o processi informatici o telematici. La pervasività di questi ultimi in ogni settore della società odierna ha altresì inciso sulla realizzazione di ipotesi delittuose "tradizionali", aumentandone la scala e la portata.[3]

Di conseguenza, sotto il profilo procedurale, la c.d. "prova digitale" – definita come quel "complesso delle informazioni digitali che sono in grado di stabilire se un crimine è stato commesso o che possono rappresentare un collegamento tra un crimine e i suoi esecutori"[4] – diventa, ad oggi, una risorsa investigativa essenziale al fine della ricostruzione del fatto di reato. Tuttavia, proprio in sede processuale, emerge una difficoltà, per gli operatori del diritto, di conciliare il mondo della tecnologia, in rapida e costante evoluzione, con le dinamiche processuali, caratterizzate, a loro volta, da un complesso bilanciamento, ai fini dell'accertamento, tra esigenze probatorie e garanzie individuali.[5] La ricerca di un equilibrio, che pur rappresentando da sempre il *punctum dolens* dell'incontro tra scienza e processo penale, assume, alla luce delle caratteristiche del dato digitale e delle correlate potenzialità delle indagini informatiche, inedite criticità.[6]

Da un lato, i sistemi informatici sono in grado di contenere una grande massa di dati di diversa natura, e dall'altro, non risulta possibile, allo stato dell'arte, circoscrivere la ricerca

---

[1] Marco Pittiruti, *Digital evidence e procedimento penale* (Giappichelli editore 2017), 1.
[2] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) ETS 185, 21.
[3] Nella dottrina anglofona e nordamericana si distingue tra i c.d. "*cyber-enabled crimes*" e "*cyber-related crimes*". Per un approfondimento sul tema si veda Mike Mcguire e Samantha Dowling, "Cybercrime: A review of the evidence" (2013) <https://www.semanticscholar.org/paper/Cyber-crime%3A-A-review-of-the-evidence-Mcguire Dowling/56624c6ef4e1d6f4cee7a0ab9a053724806bc669> ultimo accesso 29 settembre 2023.
[4] Eoghan Casey, *Digital evidence and computer crime* (Academic Press 2000), 196.
[5] Cesare Parodi, 'L'acquisizione della prova digitale' (2019) Il diritto vivente 1, 2.
[6] Marco Pittiruti, 'Digital evidence e categorie probatorie' in Marco Pittiruti, *Digital evidence e procedimento penale* (Giappichelli editore 2017), 2.

a determinati dati o informazioni.[7] Alla promiscuità del dato digitale, si aggiunge una sua natura volatile, immateriale e fragile, che rende la fonte digitale facilmente alterabile, manipolabile e duplicabile, in modo pressoché impercettibile.[8] Pertanto, diventa imperativo per le autorità investigative porre in essere una procedura di acquisizione e conservazione del dato digitale, volta a garantirne l'integrità e genuinità, con la finalità ultima di assicurarne un utilizzo come prova in sede dibattimentale.[9] Una procedura la cui attuazione e codificazione si scontrano con un rapido evolversi della tecnologia, rispetto al quale le autorità investigative, al pari del legislatore e della giurisprudenza, sembrano trovarsi sempre un passo indietro.

Simili difficoltà hanno condotto verso l'utilizzo di tecniche investigative sempre più invasive e accompagnate da un alone di "segretezza" circa le modalità impiegate, e al prediligere una raccolta c.d. integrale del materiale digitale, per poi filtrare le informazioni solo successivamente ed in un ambiente protetto.[10] Una prassi che rischia di collidere con due diritti fondamentali in uno Stato di diritto, quali il diritto alla riservatezza e il diritto alla difesa.

Da ultimo, alla luce del fatto che i dati possono circolare rapidamente in uno spazio virtuale senza confini, la fonte digitale è spesso conservata in una giurisdizione diversa da quella in cui si svolgono le indagini, rendendo necessario, ai fini dell'acquisizione, ricorrere ai canali di cooperazione giudiziaria internazionale.[11]

Il carattere spiccatamente transnazionale che connota la prova digitale unito ad una risposta tardiva e poco attenta alle esigenze garantiste da parte delle varie giurisdizioni nazionali di fronte alle nuove sfide emerse dall'incontro tra prova digitale e procedimento penale, hanno fatto presto nascere la necessità di creare, al livello europeo, uno scenario giuridico comune.[12]

Sotto questo profilo, gli interventi del legislatore europeo hanno contribuito a creare un sistema di cooperazione internazionale più efficiente, con il fine ultimo di creare un "un sistema

---

[7] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016) 3.
[8] Sepiso Rezen Chikuruwo, 'The Effects of Volatile Features on Digital Evidence Preservation' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4332846> ultimo accesso 29 settembre 2023, 1.
[9] Abel Yeboah-Ofori, 'Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence' (2020) 6 Journal of Forensic, Legal & Investigative Sciences 1, 1.
[10] Laura Bartoli, 'Parità delle armi e *discovery* digitale: qualche indicazione da Strasburgo' (2022) La legislazione penale 1, 3.
[11] Filippo Spiezia, 'International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime' (2022) ERA Forum 101, 103.
[12] Sara Conti, 'La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia' (2015) 24 Informatica e diritto 153, 153-154.

globale" di raccolta delle prove nella dimensione transnazionale, che superi le risposte disomogenee da parte degli ordinamenti nazionali.[13]

Allo stesso tempo, di fronte alle nuove sfide dell'era digitale si è presto creato un fruttuoso e dinamico dialogo tra le più alte corti in Europa, al livello nazionale e sovranazionale, alla ricerca di un nuovo ordine giuridico, basato sulla salvaguardia dei diritti fondamentali e sul rispetto di una normativa comune sostanziale e procedurale.[14] In particolare, per i legislatori e le corti nazionali, la Corte Europea dei Diritti Umani e la Corte di Giustizia dell'Unione europea hanno dunque rappresentato e, continuano a rappresentare, una guida preziosa, affinché lo spazio giuridico penale europeo non tramuti in un "*far west* tecnologico", in cui ogni Stato autorizzi mezzi di ricerca della prova digitali oltre i confini della propria sovranità, fino a dove la tecnologia lo permetta, anche a costo di violare le garanzie individuali.[15]

Ciò premesso, l'elaborato si propone di ricostruire l'attuale quadro giuridico europeo in tema di prova digitale e procedimento penale, evidenziandone i profili critici e identificando possibili prospettive future, alla luce dei più recenti sviluppi legislativi e giurisprudenziali.[16] A tal fine, l'analisi si divide in due parti. La prima è dedicata alla dimensione sovranazionale, in cui sono analizzate, rispettivamente al Capitolo 1 e al Capitolo 2, le giurisdizioni del Consiglio d'Europa e dell'Unione europea. Nella seconda parte, che esplora la dimensione nazionale, viene analizzata, al Capitolo 3, la ricezione da parte dell'ordinamento italiano delle influenze sovranazionali. Da ultimo, al Capitolo 4, l'analisi si conclude con la presentazione di un *case study*, in cui vengono esaminate le questioni giuridiche emerse dai più recenti casi investigativi transfrontalieri *Sky ECC* ed *EncroChat*, attraverso un'analisi comparata dei filoni giurisprudenziali sviluppatesi rispettivamente in Italia, Germania e Olanda.

[13] Fabiana Falato, 'La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale' (2018) Archivio Penale 1, 5.
[14] Ibid, 2.
[15] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016), 3.
[16] Il presente elaborato prende in considerazione i principali sviluppi in materia fino a settembre 2023.

PARTE PRIMA

La Dimensione sovranazionale

Capitolo 1

Il Consiglio d'Europa: la prima risposta internazionale alle nuove sfide dell'era digitale

SOMMARIO:

1. Introduzione

Quando l'Unione europea ("**UE**") era agli albori e le sue competenze in ambito penale erano ancora inimmaginabili nacque, sotto gli auspici del Consiglio d'Europa,[17] la Convenzione europea di assistenza giudiziaria in materia penale,[18] stabilendo, già nel lontano 1959, il primo quadro internazionale per l'assistenza giudiziaria reciproca in materia penale.[19] Tuttavia, tale strumento si rivelò presto inadeguato nel promuovere un'azione coordinata che proteggesse le società di fronte alle nuove sfide dell'era digitale.[20] A tal fine, il Consiglio d'Europa decise di stipulare il primo trattato internazionale in materia di contrasto al *cybercrime*, vale a dire la Convenzione di Budapest sulla criminalità informatica.[21] Quest'ultima rappresenta il primo tentativo internazionale che, al fine di combattere la criminalità informatica, abbia affrontato il tema dell'accesso nazionale e *cross-border* alla prova digitale nel procedimento penale, attraverso l'armonizzazione delle legislazioni nazionali delle Parti contraenti.

Tale strumento, risalente ai primi anni 2000, ha svolto un ruolo fondamentale nel plasmare le discipline nazionali in materia, riuscendo a mantenere nel tempo una sua centralità nel panorama internazionale grazie anche alla pubblicazione di strumenti di *soft law* che, *inter alia*,

---

[17] Il Consiglio d'Europa è un'organizzazione internazionale fondata il 5 maggio 1949, i cui Paesi membri attraverso una stretta collaborazione condividono l'obiettivo di salvaguardare i diritti umani, la democrazia e lo Stato di diritto. Lo strumento principale attraverso cui tali valori vengono salvaguardati sono accordi o convenzioni internazionali tra Paesi membri, con la possibilità di coinvolgere anche Stati terzi, che costituiscono la base per armonizzare le varie legislazioni nazionali.

[18] Consiglio d'Europa, 'Convenzione europea di assistenza giudiziaria in materia penale' (1959) STE No 030.

[19] Sotto questo profilo, i membri del Consiglio compresero presto che l'adozione di regole comuni in materia di cooperazione giudiziaria avrebbe fatto progredire i loro sistemi di giustizia penale, ma prudenti nel rinunciare alla competenza nazionale in questo settore, preferirono utilizzare uno strumento di diritto internazionale per raggiungere questo scopo.

[20] Council of Europe, 'Council of Europe action against Cybercrime' <https://www.coe.int/it/web/portal/coe-action-against-cybercrime> ultimo accesso 29 settembre 2023.

[21] Council of Europe, Convention on Cybercrime (Budapest Convention on Cybercrime) (2001) ETS No 185 ("**Convenzione di Budapest**"). Per una traduzione non ufficiale, viene fatto riferimento a Osservatorio Permanente sulla Criminalità Organizzata, 'Convenzione del Consiglio d'Europa sulla Criminalità Informatica' <https://www.poliziadistato.it/statics/14/convenzione-cybercrime.pdf> ultimo accesso 29 settembre 2023.

hanno contribuito alla recente adozione di un Secondo Protocollo Addizionale alla Convenzione,[22] volto a rafforzare la cooperazione tra le Parti contraenti e tra queste ultime e il settore privato.

Allo stesso tempo, la Convenzione di Budapest, come ribadito dal suo stesso preambolo, non è l'unico strumento rilevante in materia di prova digitale e procedimento penale adottato dal Consiglio d'Europa. Ciò alla luce del fatto che se l'acquisizione e la conservazione della prova digitale creano nuovi ostacoli per le autorità investigative, allo stesso tempo la raccolta e l'utilizzo della prova digitale possono interferire in maniera significativa con la protezione dei diritti fondamentali. A causa delle complessità tecniche caratterizzanti le indagini informatiche e alla promiscuità del dato digitale, al momento della ricerca e dell'acquisizione della prova digitale, non è spesso possibile fare una preselezione di ciò che potrà essere utile ai fini dell'accertamento del fatto di reato.[23] Questo porta alla raccolta di una grande quantità di dati, che oltre ad interferire significativamente con la vita privata di chi è sottoposto alle indagini e di terzi, allo stesso tempo, richiede una rilettura dell'esercizio del diritto alla difesa, la cui tutela è essenziale al fine di garantire un giusto processo. Sotto questo profilo, un ruolo importante è rivestito dalla Convenzione Europea dei Diritti Umani ("**CEDU**"),[24] firmata nel 1950 dal Consiglio d'Europa, così come interpretata e applicata dalla giurisprudenza della Corte Europea dei Diritti Umani ("**Corte EDU**").

Alla luce di tale quadro normativo, questo Capitolo mira ad analizzare come il Consiglio d'Europa, attraverso la Convenzione di Budapest e relativi Protocolli, letti in combinato disposto con la CEDU, abbia influenzato e continui ad influenzare, la legislazione e la giurisprudenza dell'Unione europea e dei suoi Stati membri, dettando una seria di norme e principi in materia di acquisizione, conservazione, scambio e utilizzo della prova digitale nel procedimento penale.

[22] Council of Europe, 'Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence' (2022) CETS 224.
[23] Laura Bartoli, 'Parità delle armi e *discovery* digitale: qualche indicazione da Strasburgo' (2022) La legislazione penale 1, 3.
[24] Consiglio d'Europa, 'Convenzione Europea dei Diritti dell'Uomo' (1950) ETS 5.

2. La Convenzione di Budapest sul *cyber-crime*: il primo trattato internazionale in materia di acquisizione e conservazione della prova digitale

Attraverso un'armonizzazione minima delle legislazioni nazionali, la Convenzione di Budapest nasce agli inizi degli anni 2000 al fine riconciliare la libertà di ricerca, accessibilità e condivisione dell'informazione offerta dalla rete con il bisogno di dare una risposta giuridica efficace nel caso di un suo utilizzo a fini criminosi. Al fine di rispettare tale bilanciamento, solo alcune fattispecie di reato sono oggetto di armonizzazione, e l'acquisizione di dati come "prova digitale" in procedimenti penali viene garantita nel rispetto dei diritti fondamentali e delle garanzie procedurali caratterizzanti uno Stato di diritto.25 Il Trattato si pone dunque tre obiettivi principali, ossia (i) armonizzare elementi di diritto penale sostanziale nell'area della criminalità informatica (ii) definire poteri di diritto penale nazionale processuale volti a facilitare l'indagine e la repressione dei reati informatici e dei reati comuni le cui prove sono in forma elettronica, ed infine (iii) istituire un regime rapido ed efficace di cooperazione internazionale. A tal fine, la Convenzione è strutturata in quattro capitoli, rubricati rispettivamente (I) Uso dei termini; (II) Provvedimenti da adottare a livello nazionale; (III) Cooperazione internazionale e (IV) Clausole finali.

2.1. La definizione di prova digitale

Il primo Capitolo è dedicato ad armonizzare, ai fini della Convenzione, una serie di definizioni, che le parti contraenti non sono obbligate a copiare *verbatim,* ma che dovranno essere implementate dalle legislazioni nazionali in accordo con i principi del Trattato.

Nonostante in numerose disposizioni si faccia riferimento al concetto di "prove in forma elettronica" e tale termine svolga la funzione di discrimine tra i reati rientranti nello scopo di applicazione della Convenzione, indipendentemente dalla loro appartenenza all'area della criminalità informatica, non è possibile trovare nel testo una definizione generale di "prova digitale". Per quanto sorprendente alla luce dello scopo prefissato dalla Convenzione di

[25] Cybercrime Convention Committee, 'The Budapest Convention on Cybercrime: benefits and impact in practice' (13 luglio 2020) <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac> accesso 29 settembre 2023.

armonizzare le normative nazionali, tale scelta risulta essere in linea con l'approccio generale adottato dai redattori nello stilare il Trattato, il quale non contiene tante definizioni concettuali quante è possibile trovare in altri modelli legislativi regionali.[26]

Tuttavia, all'art. 1, vengono definite due tipologie di dati, utilizzabili come prova digitale nel processo penale, vale a dire la categoria dei "*computer data*" e una loro sottocategoria, vale a dire i c.d. "*traffic data*". Nella prima nozione, traducibile in "dati informatici", rientra "qualsiasi rappresentazione di fatti, informazioni o concetti in una forma suscettibile di essere processata da una sistema informatico, incluso un programma adatto a consentire ad un sistema informatico di svolgere una funzione". Per "dati sul traffico" si intende invece "qualsiasi dato informatico relativo ad una comunicazione avvenuta attraverso un sistema informatico, facente parte di una catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio". La *ratio* della scelta di adottare una definizione di "*traffic data*" così ampia risiede nell'offrire la possibilità ai legislatori nazionali di differenziare la protezione giuridica dei dati sul traffico, sulla base della loro sensibilità, prevedendo criteri sostanziali e procedure diverse per autorizzare eventuali poteri investigativi volti all'acquisizione di tali dati.[27] Sebbene non evidenziato dalla Convenzione, occorre sottolineare l'appartenenza dei "*traffic data*" alla categoria dei c.d. "*metadata*", vale a dire una serie di dati che forniscono informazioni circostanziali circa la genesi del dato stesso.[28] L'analisi di questa tipologia di dati può dimostrarsi particolarmente utile ai fini dell'accertamento del fatto di reato in quanto è in grado di fornire una e vera propria "*time-line*" della vita privata di una persona, e allo stesso tempo permette di svelare se i dati abbiano subito alterazioni o manipolazioni.[29]

---

[26] Elaine Fahey, 'Developing EU cybercrime and cybersecurity on legal challenges of EU institutionalisation of cyber law-making' in Thomas Hoerber *et al* (eds.), *The Routledge Handbook of European Integrations* (prima edizione, Routledge 2021), 13.
[27] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) ETS 185, 6.
[28] Serena Quattrocolo, 'Processo penale e rivoluzione digitale: da ossimoro a endiadi?' (2020) 3 Rivista di d Diritto dei Media 121, 126.
[29] Giandonato Caggiano, 'Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione' (2018) 2 Rivista di Diritto dei Media 1, 15.

2.2. Le misure di diritto penale sostanziale

Il secondo Capitolo è diviso in tre sezioni, dedicate all'armonizzazione di regole rispettivamente in materia di diritto penale sostanziale (artt. 2-13) e procedurale (artt. 14-21), con un'ultima sezione (art. 22) volta a stabilire dei criteri in materia di giurisdizione.

La prima sezione stabilisce uno standard minimo comune per un elenco di reati informatici su cui, in fase di redazione, è stato raggiunto un consenso, senza che però possa essere pregiudicata la possibilità per le parti contraenti di estendere la lista al livello nazionale. Tale tipo di armonizzazione, volta a facilitare il contrasto alla criminalità informatica, sia a livello nazionale che internazionale, è essenziale per un duplice ordine di ragioni. In primo luogo, questa riduce il rischio che i criminali informatici possano sfruttare i c.d. "*safe havens*".[30] In altre parole, se una condotta non viene criminalizzata da un determinato sistema nazionale, gli individui in quel paese possono agire impunemente nel commettere reati, i cui effetti, tuttavia, possono interessare anche altre giurisdizioni. Ciò ostacola non solo la persecuzione di una possibile fattispecie criminosa, ma la stessa raccolta di prove e un'eventuale richiesta di estradizione. In secondo luogo, anche qualora una doppia incriminazione sia prevista, garantire degli standard minimi comuni circa gli elementi fondamentali rispetto ad una serie di fattispecie di reato, facilita e rende più efficiente la cooperazione transfrontaliera tra autorità investigative e giudiziarie.[31]

In particolare, quattro categorie di reati sono oggetto di armonizzazione nella Convenzione: reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici; reati informatici (falsificazione e frode informatica); reati relativi alla pornografia infantile; reati contro la proprietà intellettuale e diritti collegati. A questo elenco bisogna tuttavia aggiungere una serie di norme specifiche volte alla criminalizzazione di atti di natura razzista e xenofoba commessi e diffusi attraverso sistemi informatici, adottate nel Primo Protocollo Addizionale alla Convenzione, entrato in vigore il 1° marzo 2006.[32]

---

[30] Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation' (2014) Monash University Law Review 698, 701.
[31] Ibid.
[32] Council of Europe, 'First Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems' (2003) ETS 189.

2.3. Le misure di diritto penale procedurale

La sezione della Convenzione dedicata ad armonizzare misure di diritto penale procedurale viene basata in gran parte su un precedente documento adottato in materia dal Consiglio d'Europa.[33] Questa presenta uno scopo di applicazione più ampio rispetto alla parte di diritto penale sostanziale. La prima stabilisce infatti poteri e procedure da applicare non solo ai procedimenti penali aventi ad oggetto i reati armonizzati dalla Convenzione o altre fattispecie commesse per mezzo di un sistema informatico, ma alla anche alla raccolta di prove in formato elettronico, indipendentemente dal tipo di reato perseguito.[34]

Dunque, la sezione mira a definire una serie di poteri che consentano alle autorità competenti nazionali di affrontare le sfide della criminalità informatica, in particolare in relazione all'acquisizione e conservazione della "prova digitale". Difatti, all'epoca della redazione della Convenzione, la maggior parte dei legislatori nazionali degli Stati membri del Consiglio d'Europa non erano ancora intervenuti di fronte alle difficoltà sorte nello svolgimento di indagini nel mondo digitale, avendo a disposizione solo i tradizionali poteri procedurali, pensati per raccogliere prove fisiche e tangibili.[35] Alla luce di tale lacuna normativa, i redattori del Trattato decisero di adottare una duplice strategia: da un lato, adattare le tradizionali misure procedurali, quali la perquisizione e il sequestro, al nuovo contesto digitale; dall'altro, creare nuove misure di conservazione e acquisizione dei dati al fine di contrastarne la volatilità e la velocità di circolazione.[36] Inoltre, se alcune norme generali sono dettate per la raccolta di tutte le categorie di dati informatici, diverse procedure speciali sono invece previste per particolari tipologie, quali i dati relativi al traffico, al contenuto e agli abbonati.

Tuttavia, occorre sottolineare come, proprio alla luce dell'obiettivo perseguito dalla Convenzione di ampliare e rendere più efficiente il ventaglio delle misure investigative a disposizione degli Stati membri, la sezione in esame sia stata oggetto di un ampio dibattito,

[33] Council of Europe, 'Recommendation No. R (95) 13 concerning problems of criminal procedure law connected with information technology' (1995).
[34] Art. 14 Convenzione di Budapest.
[35] Peter Csonka, 'The Council of Europe's Convention on cyber-crime and other European initiatives' (2006) 3 77 Revue internationale de droit penal 473, 489.
[36] Ibid.

sollevato soprattutto in merito alla necessità di bilanciare l'efficacia di suddetta finalità con la protezione dei diritti fondamentali degli individui soggetti a tali misure.[37]

Sotto questo profilo, in primo luogo, all'art. 14 viene specificato che le misure armonizzate alla Convenzione possono essere emanate solo in relazione a specifiche indagini e procedimenti penali, ed avere ad oggetto specifici dati. Conseguentemente, l'acquisizione di questi ultimi non può essere finalizzata ad uno scopo di tipo preventivo, e, come approfondito in seguito, la Convenzione non include alcun obbligo di *data retention*.[38] In secondo luogo, se da un lato i legislatori nazionali sono liberi di stabilire le modalità di attuazione dei poteri e procedure, dall'altro, tale margine di discrezionalità viene ridotto dall'obbligo, ai sensi degli artt. 14 e 15, di introdurre specifiche condizioni e garanzie procedurali. Ciò al fine di bilanciare, alla luce del principio di proporzionalità, i poteri delle autorità investigative con un'adeguata tutela dei diritti umani e della libertà fondamentali, e in particolare dei diritti garantiti dalla CEDU. E se necessario alla luce della natura intrusiva del potere o della procedura prescritta, tali condizioni e garanzie devono includere l'esercizio di un potere di supervisione da parte di un'autorità giudiziaria o un'altra autorità indipendente circa lo scopo e la durata dei poteri e delle procedure disposti. Inoltre, le parti contraenti devono tenere in considerazione l'impatto delle misure previste dalla Convenzione anche sui "diritti, le responsabilità e gli interessi legittimi dei terzi", seppur nei limiti in cui ciò sia compatibile con il perseguimento dell'interesse pubblico e in particolare, di una buona amministrazione della giustizia.

2.3.1. La conservazione dei dati

Ai sensi dell'art. 16, viene imposto un obbligo alle parti contraenti di garantire che le autorità nazionali competenti possano emanare un ordine di conservazione rapida in relazione a specifici dati informatici, che sono stati conservati attraverso un sistema informatico e sono caratterizzati dall'essere particolarmente vulnerabili e suscettibili di modificazione o cancellazione. Conseguentemente, l'ordine di conservazione deve prevedere la nascita di un obbligo in capo ai soggetti, che si trovino in possesso o che abbiano il controllo di tali dati immagazzinati, di protezione e mantenimento dell'integrità per il periodo di tempo necessario, che non ecceda novanta giorni ma rinnovabile, per consentire alle suddette autorità di ottenere

[37] Marilena Arena, 'La Convenzione di Budapest Del Consiglio d'Europa sulla repressione della Criminalità Informatica' (2021) CRIO Papers, 27.
[38] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) ETS 185, 21.

successivamente la loro divulgazione. L'art. 17 specifica poi che qualora si tratti di dati sul traffico, oltre ad implementare le misure di cui all'art. 16, sia necessario, in primo luogo, garantire che tale rapida protezione sia possibile anche nel caso in cui uno o più *service providers*[39] siano coinvolti nella trasmissione della comunicazione in esame. In secondo luogo, bisogna assicurare una rapida divulgazione di una quantità sufficiente di dati affinché sia possibile identificare il *service provider* e la via attraverso cui la comunicazione è stata trasmessa. In entrambe le procedure previste, ogni parte è infine tenuta ad assicurare che chi sia incaricato all'adempimento di tali obblighi mantenga il segreto, per il periodo di tempo previsto dal proprio diritto nazionale, sulla procedura intrapresa.

2.3.2. L'ingiunzione di produzione

Ai sensi dell'art. 18(a), le parti contraenti devono adottare misure volte a consentire alle autorità competenti di ordinare ad un soggetto nel proprio territorio la trasmissione di specifici dati informatici, in suo possesso o controllo, immagazzinati in un sistema o in un supporto informatici. Il paragrafo b disciplina invece il potere di ordinare ad un *service provider*, che offre i suoi servizi nel territorio dalla parte contraente, di trasmettere dati sugli abbonati ai suddetti servizi,[40] che sono in suo possesso o controllo.

In un'ottica di comparazione tra le due disposizioni, l'art. 18(a) ha uno scopo di applicazione materiale più ampio rispetto all'art. 18(b) dal momento che si riferisce ad un generico "soggetto", termine che comprende ma non è limitato alla categoria dei *service providers*, e a "dati informatici", nozione che ingloba tutte le tipologie di dati, inclusi i dati sugli abbonati.[41] Tuttavia, rispetto invece allo scopo di applicazione territoriale, la misura di cui all'art. 18(b) è silente circa il luogo dove debba trovarsi il *service provider*, che dunque non deve essere necessariamente presente fisicamente o legalmente nel territorio della parte contraente, fin tanto che i suoi servizi siano comunque ivi offerti. Mentre, per entrambe le disposizioni, lo "*storage*"

---

[39] Ai sensi dell'art.1(c) Convenzione di Budapest, rientra nella categoria dei *service providers* "qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico" o "qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio".

[40] Questa tipologia di dati fornisce informazioni sul tipo di servizio offerto, sull'identità dell'abbonato e il suo indirizzo e così via. Allo stesso tempo però non consentendo di trarre conclusioni precise sulla vita privata e sulle abitudini quotidiane delle persone interessate, una loro divulgazione può avere un grado di intrusività inferiore rispetto alla divulgazione di altre categorie di dati, come i dati sul traffico.

[41] Cybercrime Convention Committee (T-CY), 'T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention)' (2017) <https://rm.coe.int/16806f943e> ultimo accesso 29 settembre 2023, 6.

in un'altra giurisdizione dei dati non rileva ai fini della loro applicazione, purché tali dati siano nel possesso o nel controllo rispettivamente del soggetto e del *service provider*. La *ratio* di queste norme risulta essere in linea con il recente approccio adottato dai sistemi penali nazionali, che tendono a considerare sempre di più la localizzazione dei dati come fattore irrilevante ai fini dello stabilire la propria giurisdizione.[42]

2.3.3. La perquisizione, il sequestro e la raccolta in tempo reale

Ai fini di innovare e armonizzare le legislazioni nazionali, l'art. 19 disciplina i tradizionali ordini di perquisizione e sequestro ma aventi ad oggetto dati informatici memorizzati in dispositivi o supporti informatici. Infatti, se tutte le giurisdizioni penali nazionali prevedono tali misure investigative in relazione ad "oggetti tangibili", diverse legislazioni domestiche spesso non permettono di salvaguardare, a causa della loro non tangibilità, i dati informatici in maniera autonoma rispetto al supporto fisico in cui sono stati memorizzati.[43]

Se la perquisizione e il sequestro di dati informatici previste dalla Convenzione presentano molte delle caratteristiche relative alle misure "tradizionali", alcune specifiche salvaguardie vengono adottate al fine di rendere la ricerca il più efficiente possibile alla luce delle caratteristiche della prova digitale.[44] Dunque, le autorità competenti devono poter non solo sequestrare o acquisire un sistema informatico o un supporto in cui i dati informatici sono stati immagazzinati, ma anche poter effettuare e trattenere una copia dei dati, preservarne l'integrità e bloccare l'accesso o rimuovere quei dati dal sistema informatico analizzato. Ciò risulta coerente con le definizioni di "supporto" e "dato informatico" fornite al primo capitolo della Convenzione. Inoltre, considerando l'alta complessità tecnica che potrebbe caratterizzare queste operazioni, le parti contraenti devono garantire la possibilità alle autorità competenti di ordinare a chi sia esperto del sistema o del programma, che deve essere perquisito o sequestrato, di fornire tutte le informazioni necessarie al fine di facilitare l'espletamento delle misure investigative armonizzate.

Gli artt. 20 e 21 sono invece dedicati a due misure che presentano un carattere particolarmente intrusivo in relazione al diritto alla riservatezza delle comunicazioni, ossia la raccolta in tempo reale di dati sul traffico e l'intercettazione in tempo reale di dati relativi al contenuto. I due

[42] Ibid, 7.
[43] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) ETS 185, 31.
[44] Ibid.

articoli sono praticamente identici, presentando come unico elemento distintivo i dati oggetto delle disposizioni, vale a dire rispettivamente i dati sul traffico e i dati sul contenuto. Differentemente dalle altre categorie di dati, la Convenzione non definisce la categoria dei dati sul contenuto, essendo possibile in via interpretativa, fare riferimento "al contenuto della comunicazione, cioè al significato o lo scopo, il messaggio o le informazioni trasmesse dalla stessa".[45]

In ogni caso, la Convenzione identifica l'intercettazione in tempo reale di dati relativi al contenuto come una misura particolarmente intrusiva nella vita privata di chi vi è sottoposto, e dunque sottolinea la necessità di adottare rigorose garanzie per assicurare un adeguato equilibrio tra gli interessi investigativi e i diritti fondamentali dell'individuo. Tuttavia, al di là del limitare l'utilizzo di tali intercettazioni ad indagini aventi ad oggetto reati definiti come "gravi" dal diritto nazionale, la Convenzione non prevede espressamente ulteriori salvaguardie. Ciononostante, il richiamo da parte degli Artt. 14 e 15 alla CEDU, comporta l'applicazione delle tutele elaborate dalla giurisprudenza della Corte EDU in materia, in seguito analizzate.

2.4. I criteri di giurisdizione

All'art. 22 vengono stabiliti una serie di criteri in base ai quali le parti contraenti sono tenute a stabilire la giurisdizione sui reati previsti nella prima sezione del capitolo. In primo luogo, la Convenzione stabilisce che uno Stato membro abbia giurisdizione sul reato se questo è stato commesso nel suo territorio (criterio della territorialità). In secondo luogo, si ha giurisdizione anche se il reato è commesso a bordo di una nave che batte la bandiera del paese o di un aeromobile che sia ivi immatricolato. In terzo luogo, viene stabilito il criterio della nazionalità c.d. attiva: la parte contraente ha giurisdizione se il reato è stato commesso da un proprio cittadino, sempre che la condotta sia prevista come reato nel territorio in cui è stata posta in essere o se l'infrazione non rientrerebbe nella competenza territoriale di alcun altro Stato.

La possibilità che più Stati possano rivendicare la loro giurisdizione su reati commessi mediante l'uso di sistemi informatici, è piuttosto frequente, perché, ad esempio, le vittime di tali reati potrebbero essere dislocate in più Stati membri.[46] Al fine di evitare una duplicazione degli

[45] Marilena Arena, 'La Convenzione di Budapest Del Consiglio d'Europa sulla repressione della Criminalità Informatica' (2021) CRIO Papers, 38.
[46] Jonathan Clough, 'The Council of Europe Convention on Cybercrime: defining 'crime' in a digital world' (2012) Criminal Law Forum 363, 370.

sforzi, qualora sorga un conflitto di giurisdizione, le parti interessate devono, ove opportuno, consultarsi per determinare la sede appropriata per l'azione penale. Se in alcuni casi, potrebbe rivelarsi più efficace la scelta di prediligere un'unica sede per l'esercizio dell'azione penale; in altri, potrebbe essere preferibile che ciascuno Stato, che possa vantare giurisdizione, persegua una parte dei partecipanti.

2.5. I profili di cooperazione internazionale

La c.d. "giurisdizione investigativa", vale a dire la capacità di condurre indagini nel territorio di altri Stati,[47] è trattata nel terzo capitolo della Convenzione, diviso in due sezioni, la prima dedicata a stilare una serie di principi generali, e la seconda che disciplina delle disposizioni specifiche.

La Convenzione esordisce all'art. 23 stilando tre principi da rispettare in materia di cooperazione internazionale. È infatti richiesto alle parti di (i) assicurare una cooperazione internazionale reciproca il più ampia possibile e di ridurre al minimo gli ostacoli (ii) nel rispetto delle disposizioni del capitolo, (iii) tenendo allo stesso tempo in considerazione gli strumenti internazionali sulla cooperazione giudiziaria in materia penale, gli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e le previsioni di diritto nazionale in materia. Allo stesso modo, le parti devono, ai sensi dell'art. 25, assicurare la più ampia mutua assistenza possibile, soggetta alle condizioni previste dalla legislazione della parte ricevente la richiesta (principio del *locus regit actum*) o dai trattati di mutua assistenza applicabili, inclusi i motivi sulla base dei quali la parte richiesta può rifiutare la cooperazione. Sotto questo ultimo profilo, il diritto di rifiutare la richiesta di mutua assistenza avente ad oggetto i reati armonizzati dalla Convenzione non può essere esercitato per il solo motivo che la domanda abbia ad oggetto un reato che la parte richiesta reputa di natura fiscale. Qualora invece lo Stato ricevente la richiesta sia autorizzato, nel rispetto delle disposizioni previste dal capitolo, a subordinare la mutua assistenza al requisito della c.d. "doppia incriminazione", tale condizione è soddisfatta se la condotta, per il quale la mutua assistenza è stata richiesta, sia punibile come reato in base al proprio diritto nazionale, a prescindere da eventuali divergenze terminologiche o classificatorie. Tuttavia, se, ai sensi dell'art. 27, la richiesta di mutua assistenza avviene in

[47] Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation' (2014) Monash University Law Review 698, 704.

assenza di accordi internazionali applicabili, questa deve essere eseguita in base alle procedure indicate dalla Parte richiedente (principio del *forum regit actum*)**,** salvo incompatibilità con la legislazione dello Stato che ha ricevuto la richiesta. Quest'ultimo può rifiutare, oltre ai motivi stabiliti dall'art. 25, se la domanda abbia connotazione politica o se l'esecuzione della richiesta possa pregiudicare la sua sovranità, sicurezza, ordine pubblico o atri interessi essenziali.

Riguardo alla sezione dedicata alle disposizioni specifiche, in primo luogo la Convenzione disciplina al livello internazionale le procedure di conservazione rapida di dati informatici immagazzinati (art. 29) e la divulgazione rapida di dati sul traffico conservati (art. 30), prevedendo dei meccanismi equivalenti a quelli dettati al livello domestico, rispettivamente agli artt. 16 e 17.[48]

In secondo luogo, vengono regolate le richieste di mutua assistenza in relazione ai poteri d'indagine. Ai sensi dell'art. 31 è possibile per una parte richiedere ad un'altra la perquisizione o il sequestro o altri mezzi di ricerca simili, o la divulgazione dei dati, inclusi quelli conservati in base all'art. 29, che sono stati immagazzinati attraverso un sistema informatico situato nel territorio dello Stato che ha ricevuto la richiesta.

In terzo luogo, viene disciplinato l'accesso *cross-border* a dati informatici immagazzinati (art. 32). Una Parte può accedere a tali dati, senza ulteriori autorizzazioni, indipendentemente da dove siano locati, se questi sono accessibili pubblicamente. Inoltre, una parte può accedere o ricevere, attraverso un sistema informatico nel proprio territorio, dati informatici immagazzinati situati in un altro Stato, ma solo se ottenuto il consenso legale e volontario della persona legalmente autorizzata alla divulgazione di tali dati. Appare chiaro che il sistema appena delineato non autorizza una parte contraente a superare il meccanismo mutua assistenza, accedendo direttamente alle prove elettroniche situate nel territorio di un'altra parte senza il consenso di quest'ultima.[49] D'altra parte, la questione circa la legittimità di condurre ricerche transfrontaliere senza dover ricorrere ai spesso "lunghi" meccanismi di mutua assistenza, è stata discussa a lungo dai redattori della Convenzione.[50] Questi ultimi hanno poi concluso che non fosse possibile adottare un regime completo e giuridicamente vincolante che regolasse questo settore, per un duplice ordine di ragioni. Da una parte, un fattore che ha influenzato tale scelta

[48] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) ETS 185, 50.
[49] Nathalie A. Smuha, 'Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency' (2018) 8(1) European Criminal Law Review 83, 87.
[50] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) ETS 185, 53.

è stata la mancata esperienza in materia, all'epoca della redazione, a causa del numero ancora esiguo di situazioni verificatesi in concreto. Dall'altra, vi era la consapevolezza che la soluzione migliore da adottare dipendesse spesso dalle circostanze precise del singolo caso in esame, rendendo difficoltosa la formulazione di una regola generale.[51] Dunque, i redattori hanno alla fine deciso, all'art. 32, di disciplinare solo le situazioni per le quali fosse stato raggiunto un consenso, lasciando comunque aperta la possibilità, grazie al carattere flessibile della Convenzione, di poter negoziare nuove soluzioni in futuro. Difatti, l'accesso transfrontaliero alle prove digitali ha costituito, *inter alia*, oggetto del nuovo Protocollo Addizionale, in seguito analizzato.

Da ultimo, la Convenzione impone alle parti di fornire mutua assistenza tra loro, regolata dalle condizioni e dalle procedure previste dal diritto interno, nella raccolta in tempo reale di dati sul traffico, associati a specifiche comunicazioni nel proprio territorio, trasmessi attraverso l'uso di un sistema informatico. Tale obbligo deve essere adempiuto almeno rispetto ai reati per i quali tale raccolta sarebbe stata possibile, in ambito interno, in una situazione analoga (principio di equivalenza) (art. 33). Una simile imposizione è prevista anche rispetto alla raccolta o intercettazione in tempo reale di dati relativi al contenuto di specificate comunicazioni, trasmesse attraverso l'uso di un sistema informatico, nella misura consentita dai trattati applicabili tra le parti coinvolte e dalle leggi interne (art. 34).

[51] Ibid.

2.6. La "*Electronic Evidence Guide*": le *best practices* offerte dal Consiglio d'Europa nell'acquisizione della prova digitale

Come evidenziato a più riprese dalla Convenzione di Budapest,[52] al pari di ogni altro elemento probatorio, la prova digitale deve essere affidabile e conservare la propria integrità. In particolare, è essenziale che nell'acquisizione della prova digitale venga seguite precise regole e procedure in modo che siano ricostruibili le modalità di accesso e di conservazione.[53] Tale esigenza rappresenta tuttavia la principale sfida di questa tipologia di prove: a causa della sua natura immateriale, la prova digitale è suscettibile di essere soggetta a manipolazioni o contraffazioni con maggiore facilità rispetto alla prova c.d. tradizionale.[54] Tale predisposizione si traduce nell'imperativa esigenza di impiegare metodi e procedure tecniche specifiche che conferiscano ai dati digitali una qualifica di affidabilità, integrità e trasparenza, elevando i medesimi al rango di elemento probatorio.[55] Sotto questo profilo, con l'obiettivo di offrire assistenza e direttive per identificare e gestire le fonti digitali, nel 2013 viene pubblicata l'*Electronic Evidence Guide*,[56] risultato di un progetto finanziato dal Consiglio d'Europa e dall'UE. Tale strumento, recentemente aggiornato,[57] ha costituito, sia una guida per i legislatori nazionali al fine di attuare e aggiornare nel tempo i principi e le norme stabilite dalla Convenzione di Budapest, che, in assenza di un'adeguata risposta legislativa, una preziosa risorsa per le autorità investigative di fronte alle nuove sfide poste dalla natura della prova digitale.

Oltre a fornire una serie di indicazioni tecniche circa le modalità di acquisizione e conservazione del dato digitale al fine di garantire l'autenticità della prova durante tutto il processo, il documento formula dei criteri di valutazione circa l'ammissibilità della prova

---

[52] Vedi le artt. 16, 17, 19, 20, 21, 30, 31, 33 e 34 Convenzione di Budapest.

[53] 'iPROCEEDS-2: Launching of the Electronic Evidence Guide v.3.0' <https://www.coe.int/en/web/cybercrime/-/iproceeds-2-launching-of-the-electronic-evidence-guide-v-3-0> ultimo accesso 29 settembre 2023.

[54] Raffaella Brighi and Michele Ferrazzano, 'Digital Forensics: Best Practices and Perspective' in Michele Caianiello and Alberto Camon (eds) *Digital Forensic Evidence Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Wolters Kluwer 2021), 15-16.

[55] La scienza che si occupa della formulazione e implementazione di tali metodi e procedure tecniche è comunemente denominata "*digital forensic*".

[56] Electronic Evidence Guide (2014) <https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf> ultimo accesso 29 settembre 2023 ("**Guida**").

[57] La Guida è stata aggiornata nel 2022, tuttavia a quest'ultima versione non è ancora stato dato pubblico accesso. Per ulteriori informazioni, si veda: 'iPROCEEDS-2: Launching of the Electronic Evidence Guide v.3.0'<https://www.coe.int/en/web/cybercrime/-/iproceeds-2-launching-of-the-electronic-evidence-guide-v-3-0> ultimo accesso 29 settembre 2023.

digitale e dei principi sulle fonti della prova digitale. I suddetti criteri e principi hanno lo scopo di fornire un'ulteriore guida per gli operatori nazionali, rimanendo la legislazione nazionale il principale punto di riferimento. Per quanto concerne il profilo dell'ammissibilità, la prova deve delineare con incontestabile precisione i fatti, attenendosi scrupolosamente alla loro concatenazione originaria (criterio dell'autenticità) e deve essere analizzata nella sua interezza (criterio della completezza).[58] Inoltre, non deve risultare alcun dettaglio riguardante la raccolta e il conseguente trattamento degli elementi probatori che possa suscitare incertezze circa la loro autenticità e veridicità (criterio dell'affidabilità) e la prova deve risultare agevolmente credibile e comprensibile ad un giudice (criterio della credibilità).[59] Infine, le metodologie adoperate per raccogliere una prova digitale devono risultare proporzionali rispetto alle esigenze di giustizia, vale a dire che l'eventuale pregiudizio arrecato ai diritti fondamentali delle parti coinvolte non deve eccedere il "valore probatorio" intrinseco della suddetta prova (criterio di proporzionalità).[60] Trai i principi sulle fonti di prova, si riportano in particolare il principio dell'integrità dei dati e della registrazione delle operazioni effettuate.[61] Questi si traducono nell'esigenza di garantire che nessuna delle operazioni eseguite dovrebbe arrecare modifiche ai dati, ai dispositivi o ai mezzi elettronici che potrebbero successivamente essere presentati al processo e che tutte le attività compiute durante la manipolazione delle fonti di prova digitali vengano registrate e documentate nel dettaglio.

3. Il Secondo Protocollo Addizionale alla Convenzione di Budapest e l'introduzione di una nuova forma di cooperazione

La Convenzione, che ad oggi conta 68 paesi membri, è riuscita a mantenere nel tempo la sua centralità nel panorama internazionale grazie a, *inter alia*, il suo carattere flessibile. Quest'ultimo le ha permesso di subire degli aggiornamenti attraverso l'autorizzazione di Protocolli Addizionali. In particolare, nel maggio 2022 è stato adottato un Secondo Protocollo Addizionale,[62] con l'obiettivo di rafforzare la cooperazione in materia di criminalità informatica

[58] Guida, 13.
[59] Ibid.
[60] Ibid.
[61] Ibid, 14.
[62] Council of Europe, 'Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence' (2022) CETS 224.

e la raccolta di prove in formato elettronico di qualsiasi reato ai fini di specifiche indagini penali o procedimenti.[63]

Al fine di comprendere la *ratio* di tale strumento è necessario considerare alcuni degli aspetti caratterizzanti la natura transfrontaliera della prova digitale. Tali caratteristiche sono: (i) la peculiarità della sua localizzazione e del suo "*storage*"; (ii) la provenienza da fonti private, vale a dire i *service providers*, che si trovano spesso in giurisdizioni diverse dal territorio in cui viene commesso il reato; (iii) l'operare *borderless* che contraddistingue le condotte di criminalità informatica. [64] Alla luce di un volume crescente di richieste di accesso *cross-border* alle prove digitali e della necessità di avere una procedura più rapida ed efficiente, le giurisdizioni nazionali hanno iniziato a bypassare le forme tradizionali di cooperazione previste dalla Convenzione di Budapest, per stabilire canali informali direttamente con i soggetti privati (c.d. *voluntary disclosure*).[65] Tuttavia, occorre considerare che i *service providers* non solo sono vincolati alla legislazione nella quale operano, ma sono mossi anche da interessi diversi rispetto alle autorità investigative.[66] Mentre, in una società democratica, le autorità pubbliche sono tenute a compiere un delicato bilanciamento tra esigenze investigative e valori costituzionali, i *service providers* sono guidati principalmente da interessi economici che giocano un ruolo importante nella loro decisione di accettare o meno la richiesta di accesso.[67]

Se da una parte il Secondo Protocollo Addizionale rafforza alcuni degli aspetti positivi già emersi nella Convenzione, come quello degli obblighi di collaborazione con i *service providers* ex art. 32, il quadro normativo complessivo viene ampliato e reso più efficiente, ponendo al centro la dimensione transfrontaliera e arricchendo gli strumenti a disposizione delle autorità nazionali competenti.[68] Come evidenziato nel suo preambolo, il Protocollo tiene conto del fatto

---

[63] Carlotta de Luca, 'Il secondo protocollo aggiuntivo alla convenzione sulla criminalità informatica relativo alla cooperazione rafforzata e alla circolazione di prove elettroniche' (2022) 3 Processo Penale e Giustizia 648, 648.
[64] Filippo Spiezia, 'International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime' (2022) ERA Forum 101, 103-104.
[65] Stanislaw Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161, 169.
[66] Teresa Quintel e Mark D Cole, 'Transborder Access to e-Evidence by Law Enforcement Agencies. A first comparative view on the Commission's Proposal for a Regulation on a European Preservation/Production Order and accompanying Directive' (2018) University of Luxembourg Law Working Paper 1, 2.
[67] Ibid.
[68] Council of Europe, 'PRESS RELEASE: Cybercrime: Council of Europe strengthens its legal arsenal' (17 novembre 2021) <https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a48ca6> ultimo accesso 29 settembre 2023.

che, da una parte, le prove relative a qualsiasi fattispecie di reato, non solo a quelle appartenenti all'area del *cybercrime*, sono sempre più spesso conservate in forma elettronica su sistemi informatici in più giurisdizioni straniere o alle volte anche sconosciute; dall'altra mancano strumenti internazionali che permettano di ottenere celermente tali prove. Allo stesso tempo, viene riconosciuta la necessità di una cooperazione più efficiente tra gli Stati e il settore privato, che garantisca una maggiore certezza giuridica per entrambe le parti. Sotto questo profilo, la seconda sezione del secondo capitolo del Protocollo disciplina le procedure volte a migliorare la cooperazione diretta con *service providers*, locati nel territorio di un'altra parte contraente.

In particolare, le procedure di cui agli artt. 6 e 7 si basano sulle conclusioni pubblicate dal *Cloud Evidence Group* del Comitato della Convenzione di Budapest.[69] Queste hanno evidenziato l'importanza di un accesso transfrontaliero tempestivo alle prove digitali in specifiche indagini o procedimenti penali, alla luce degli ostacoli posti dalle procedure esistenti per l'ottenimento delle prove elettroniche.[70]

Ai sensi dell'Art. 6, viene regolata la possibilità che le autorità competenti di una Parte contraente cooperino con un ente che fornisca, sul territorio di un altro Stato membro, dei servizi di registrazione di nomi di dominio, in maniera diretta, vale a dire senza l'intermediazione delle autorità pubbliche di quello Stato. In particolare, la cooperazione ha ad oggetto una richiesta di fornire informazioni, in possesso o sotto il controllo del predetto ente, al fine di identificare o contattare il titolare di un nome di dominio.

L'adozione di un tale strumento di cooperazione risulta essere perfettamente in linea con lo spirito del Protocollo.[71] Ottenere tali dati è spesso un primo passo indispensabile per la maggior parte delle indagini informatiche e per indirizzare future richieste di cooperazione internazionale. Questo perché diverse sono le forme di criminalità informatica facilitate dalla creazione e dallo sfruttamento di domini per scopi malevoli e illeciti. L'accesso alle

---

[69] In attuazione dell'art. 42 Convenzione di Budapest, tale Comitato è stato preposto a facilitare l'attuazione della Convenzione, lo scambio di informazioni e l'esame di eventuali emendamenti futuri. In particolare, i reports pubblicati dal *Cloud Evidence Group*, dedicati alla ricerca di innovative soluzioni in materia di accesso della giustizia penale alle prove conservate nel *cloud* e in giurisdizioni estere, hanno appunto costituito il fondamento delle principali novità introdotte nel Secondo Protocollo Addizionale.

[70] T-CY Cloud Evidence Group, 'Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group' (17 February 2016) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8> ultimo accesso 29 settembre 2023.

[71] Council of Europe, 'Explanatory Report to the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters' (2022) CETS 224, 13.

informazioni sulla persona fisica o giuridica che ha registrato un dominio risulta essere quindi essenziale per identificare un sospetto in una specifica indagine o procedimento penale.

Se in passato tali dati erano disponibili pubblicamente, oggi l'accesso è spesso limitato, in quanto queste informazioni vengono conservate da entità che forniscono servizi di registrazione di nomi di dominio.[72] Inoltre, in alcuni casi, tali informazioni possono essere qualificabili come dati personali, ed essere quindi protette dalle normative sulla protezione dei dati, previste dalla parte contraente in cui si trova il rispettivo ente che fornisce i servizi o dove si trova la persona a cui si riferiscono i dati.[73]

Dunque, il Protocollo se, da un lato, impone a ciascuna parte di adottare le misure necessarie per consentire a un ente sul proprio territorio di divulgare le informazioni richieste, dall'altro, permette di sottoporre l'adempimento della richiesta a ragionevoli condizioni previste dalla legislazione nazionale, incluse requisiti relativi alla protezione dei dati personali.[74] Allo stesso tempo, l'art. 14 prevede una serie di fattori volti a facilitare sia il trattamento ai sensi delle norme sulla protezione dei dati che la divulgazione dei dati richiesti in modo rapido ed efficace. Dal momento che molte parti contraenti sono tenute, al fine di adempiere ai propri obblighi costituzionali, comunitari o internazionali, a garantire, nell'attuazione delle previsioni del Protocollo, la protezione dei dati personali, è stato deciso di includere una serie di garanzie per la protezione dei dati che consentano alle parti di rendere compatibile il trattamento dei dati personali ai fini del presente Protocollo con tali obblighi.

L'art. 7 presenta una *ratio* simile a quella sottostante l'art. 6. La disposizione prescrive alle parti di adottare misure al fine di autorizzare le proprie autorità ad inviare un ordine direttamente al *service provider* nel territorio di un'altra parte. Ciò al fine di ottenere la divulgazione di specifiche informazioni memorizzate relative agli abbonati, in possesso o sotto il controllo del suddetto *service provider*, qualora tali informazioni siano necessarie per la parte che ha emesso l'ordine, ai fini di specifiche indagini o procedimenti penali.

All'art. 8, che introduce la terza sezione del secondo capitolo rubricata "Procedure che rafforzano la cooperazione internazionale tra le autorità per la divulgazione di dati informatici memorizzati", il Protocollo istituisce invece un meccanismo, volto ad integrare le disposizioni

[72] Ibid.
[73] Ibid, 14.
[74] Ibid, 15.

della Convenzione in materia di mutua assistenza. La *ratio* è quella di prevedere un meccanismo più snello di quanto non lo siano le procedure previste dalla Convenzione, limitando la quantità di informazioni che la parte richiedente deve fornire e rendendo il processo per ottenere i dati più rapido.[75]

Viene infatti previsto che qualora il *service provider* non adempia nei termini o rifiuti la richiesta, le autorità del territorio in cui è presente tale *provider* possano intervenire, emettendo un ordine che imponga a quest'ultimo la divulgazione delle informazioni relative agli abbonati e dei dati relativi al traffico, in suo possesso, di cui necessita il paese richiedente. La scelta circa il meccanismo attraverso cui imporre l'adempimento al *service provider* rimane nella discrezionalità dello Stato che ha ricevuto la richiesta, che potrà sottoporre tale procedura ai limiti previsti dalla propria legislazione nazionale, compresi eventuali requisiti costituzionali e in tema di diritti fondamentali. Rispetto ai motivi di rifiuto della richiesta, si applica la disciplina prevista agli artt. 25 e 27 Convenzione, fermo restando il principio generale di garantire una cooperazione più ampia possibile e di minimizzare possibili ostacoli.

Alla luce delle novità introdotte dal Secondo Protocollo, il quale, come analizzato in seguito, persegue obiettivi affini a quelli prestabiliti nel "*E-evidence package*"[76] recentemente adottato dall'UE, sarà interessante vedere come tali disposizioni verranno attuate dalle legislazioni nazionali, in particolare dagli Stati membri dell'UE firmatari, inclusa l'Italia.[77]

4. La conservazione dei dati vs la *data retention*

Al fine di concludere l'analisi del quadro normativo fino ad ora delineato, è importante sottolineare che la Convenzione di Budapest e i suoi due Protocolli Addizionali non contengano alcun obbligo di *data retention*. Sebbene la possibilità di imporre un obbligo in tal senso in capo ai *service providers*, in relazione a specifici dati sul traffico, sia stata discussa dai redattori, tale eventualità non è stata tradotta nel testo finale della Convenzione. D'altra parte, ai tempi della redazione, numerose organizzazioni per i diritti civili manifestarono i loro timori circa la

[75] Ibid, 23.
[76] European Commission, 'E-evidence - cross-border access to electronic evidence, Improving cross-border access to electronic evidence' <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en> ultimo accesso 29 settembre 2023.
[77] Veronica Tondi, 'Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione' (2019) 2 Diritto Penale Contemporaneo Rivista Trimestrale 439, 452.

possibilità che dietro alla Convenzione si celasse l'intento di istituire un sistema "orwelliano" di sorveglianza elettronica.[78]

Abbandonata dunque l'idea di inserire delle previsioni in materia di *data retention*, la Convenzione prevede invece agli artt. 16 e 30 che le Parti adottino misure per consentire la "conservazione rapida" (*expedited preservation*) di determinati dati informatici a livello rispettivamente nazionale e internazionale. Come accennato in precedenza, tale potere rende possibile per le autorità competenti di ordinare ad un *service provider* o altra persona fisica o legale, di "conservare" tempestivamente qualsiasi tipologia di dato informatico qualora sia necessario utilizzarlo come prova in una specifica indagine o processo penale.[79] Tuttavia, tale richiesta può avere ad oggetto solo dati specifici e immagazzinati, vale a dire una serie di dati selezionati già esistente. Si tratta dunque di una misura che presenta un carattere provvisorio ma che riveste un ruolo essenziale per le indagini, in quanto permette di ottenere in seguito, qualora sorga la necessità, attraverso ad esempio formali procedure di sequestro o perquisizione, i dati che sono stati prontamente conservati.[80] Tale possibilità risulta essere particolarmente rilevante nel quadro di cooperazione internazionale, in quanto permette di conservare, in maniera tempestiva, specifici dati la cui acquisizione avverrà in un secondo momento, una volta espletate tutte le formalità che potrebbe richiedere una richiesta formale di mutua assistenza, senza correre dunque il rischio che nell'attesa tali dati vadano dispersi.[81]

Sebbene spesso venga spesso assimilato al procedimento di conservazione di cui agli Art. 16 e 30, il processo di "*data retention*" consiste invece nello di "*storing*" dei dati, cioè nel mantenere dei dati, che sono nel processo di essere generati, nel possesso di colui in capo al quale sorge il relativo obbligo.[82] Un tale procedura è dunque caratterizzata dall'accumulo di dati nel presente e dal mantenere il possesso di questi ultimi per un periodo futuro prestabilito. Pur prevedendo due procedure distinte, le misure di conservazione rapida e di *data retention* possono avere

[78] Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation' (2014) Monash University Law Review 698, 708.
[79] Council of Europe ed European Union, 'Data retention in the States Parties to the Budapest Convention on Cybercrime. Survey report 2020' (2020) <https://rm.coe.int/2088-32-data-retention-report-2020/1680a1f305>, ultimo accesso 29 settembre 2023, 3.
[80] Ibid.
[81] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) ETS 185, 25.
[82] Ibid.

natura complementare ed essere dunque applicate insieme al fine di perseguire più finalità.[83] Se imporre un obbligo di *data retention* ai *service provider* incrementa le possibilità che i dati storici sul traffico, sulla posizione e sugli abbonati oggetto di tale obbligo siano ancora disponibili, qualora invece un periodo di *retention* stesse per scadere, una richiesta di conservazione consente di salvaguardare, oltre tale scadenza, degli specifici dati ai fini di una determinata indagine. Allo stesso tempo, in quanto presentano un livello differente di intrusività, mentre è possibile accedere ai "*retained data*" solo in relazione a reati "gravi", gli ordini di conservazione possono essere emanati, e le relative prove digitali raccolte, in relazione a qualsiasi tipo di crimine.

Nonostante la Convenzione non armonizzi norme in materia, molte Parti contraenti, recependo il dettato convenzionale di cui agli artt. 16 e 30, hanno modificato o introdotto la loro disciplina nazionale in materia *data retention*. Sotto quest'ultimo profilo, occorre segnalare che gli Stati Membri dell'UE, i quali sono allo stesso tempo tutti anche Parti contraenti della Convenzione, hanno dovuto introdurre nei loro ordinamenti una disciplina in materia di *data retention* in attuazione della Direttiva relativa alla conservazione dei dati, entrata in vigore nel 2006.[84]

[83] Cybercrime Convention Committee, 'Assessment report, implementation of the provisions of the Budapest Convention. Adopted by the T-CY at its 8th Plenary (5-6 December 2012)' (2012) < https://www.coe.int/en/web/cybercrime/assessments>, 75.

[84]Direttiva 2006/24/CE del Parlamento e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione [2006] OJ L 105/54. Sebbene, come approfondito in seguito, tale strumento sia poi stato dichiarato invalido, la Direttiva è servita come modello per i regimi nazionali di *data retention*.

5. L'acquisizione e l'ammissibilità della prova digitale nel procedimento penale e i limiti imposti dalla Convenzione Europea dei Diritti Umani

L'acquisizione, la conservazione e l'utilizzo della prova digitale richiedono un alto livello di conoscenza tecnica. Ciò si traduce in una crescente difficoltà per le autorità investigative, "direttamente proporzionale alle potenzialità" del mondo virtuale.[85] Una volta acquisiti gli strumenti e le tecniche investigative adeguate, sorge dunque un interesse per chi conduce le indagini a non rendere di pubblico dominio le tecnologie impiegate per la raccolta dei dati o il modo in cui questi siano stati processati. Conseguentemente, le modalità di conduzione delle indagini vengono spesso solo parzialmente divulgate, il che non solo impedisce una valutazione della proporzionalità e necessità della misura investigativa alla luce dell'interferenza nella vita privata di chi vi è sottoposto, ma lede anche il diritto della difesa.[86] Ciò mal si concilia, da un lato, con la capacità dei sistemi informatici di contenere una serie infinita di dati di diversa natura, riguardanti una parte significativa della vita, delle relazioni e delle attività di un grande numero di persone, e dall'altro, con l'impossibilità, allo stato dell'arte, di circoscrivere la ricerca a determinati dati o informazioni.[87] Queste due caratteristiche portano l'acquisizione e l'uso della prova digitale ad interferire sempre con il diritto alla riservatezza delle persone coinvolte e ad incrementare il rischio di condurre indagini pro-attive, ovvero di carattere meramente esplorativo che mirano alla prevenzione del reato più che alla sua repressione.[88] In una realtà, in cui appare sempre più predominante una logica pro securitaria di fronte alle nuove minacce della criminalità e del terrorismo, il rischio è di arrivare ad una raccolta massiva e indiscriminata di dati, che sfrutta le potenzialità delle indagini digitali per realizzare un sistema di sorveglianza c.d. di massa.[89]

---

[85] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016), 2.
[86] Philip Anderson *et al*, 'Digital investigations: relevance and confidence in disclosure' (2021) 22 ERA Forum 587, 597.
[87] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016), 3.
[88] Ibid.
[89] Parlamento Europeo, 'Il diritto al rispetto della vita privata: le sfide digitali. Una prospettiva di diritto comparato' (2018)<https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628243/EPRS_STU(2018)628243_IT.pdf> ultimo accesso 29 settembre 2023, 12.

Sotto questi profili, la giurisprudenza della Corte EDU ha fornito nel tempo un'importante guida per i legislatori e le corti nazionali in materia di prova digitale e procedimento penale, attraverso l'interpretazione e applicazione degli Artt. 6 e 8 CEDU, che salvaguardano rispettivamente il diritto ad un equo processo e il diritto al rispetto della vita privata e familiare.[90]

5.1. Il diritto al rispetto della vita privata e familiare (Art. 8 CEDU)

Ai sensi dell'Art. 8(1) CEDU, "*ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza*".

Rispetto all'acquisizione della prova digitale nel procedimento penale, rilevano le due nozioni di "vita privata" e "corrispondenza", i quali sono stati oggetto di un'interpretazione molto ampia da parte della Corte, che ha adattato la loro protezione alle nuove sfide dell'era digitale.

Il diritto in esame non protegge solo la sfera intima della persona e il suo *ius excludendi alios* da tale cerchia, ma tutela anche lo sviluppo della personalità individuale attraverso l'instaurazione e la coltivazione di rapporti con gli altri. In particolare, rileva, ai fini classificatori, la scomposizione del diritto in tre aree: (i) l'integrità fisica, psicologica o morale di una persona, (ii) la sua riservatezza e (iii) la sua identità e la sua autonomia.[91] Nell'era digitale, ciò si traduce nel diritto di ogni individuo a che venga garantita la riservatezza e lo sviluppo della sua vita, della sua personalità e dei suoi rapporti *online*.

In relazione al rispetto della "corrispondenza", il diritto mira, *inter alia*, a tutelare la riservatezza delle comunicazioni rispetto ad un ampio ventaglio di tecnologie, rientrando nel suo campo di applicazione, ad esempio, dati provenienti da uno smartphone e/o la loro copia speculare,[92] l'utilizzo di internet,[93] e i dati memorizzati nei server informatici.[94]

---

[90] Ai sensi degli artt. 34 e 35 CEDU, la Corte EDU può ricevere, una volta esauritisi tutti i rimedi nazionali, dei ricorsi da ogni persona, organizzazione non governativa, o gruppi di individui, che sostengano di essere vittima di una violazione, posta in essere da una delle parti contraenti, dei diritti garantiti dalla Convenzione.

[91] Corte Europea dei Diritti dell'Uomo, 'Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza' (31 agosto 2021) <https://www.giustizia.it/cmsresources/cms/documents/guida_cedu_articolo8_agg31ago2021.pdf> ultimo accesso 29 settembre 2023, 24.

[92] *Saber c Norvegia*, App no 459/18 (Corte EDU, 17 dicembre 2020), para 48.

[93] *Copland c Regno Unito*, App no 62617/00 (Corte EDU 3 luglio 2007), paras 41-42.

[94] *Wieser e Bicos Beteiligungen GmbH c Austria*, App no 74336/01 (Corte EDU 16 ottobre 2007), para 45.

Al secondo paragrafo, viene sancita la natura relativa dei diritti garantiti dall'Art. 8(1). Vengono infatti specificate le condizioni affinché un'autorità pubblica possa interferire nel godimento di tali diritti. In primo luogo, l'ingerenza deve essere giustificata alla luce del perseguimento di un interesse in relazione "alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del Paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". In secondo luogo, tale limitazione deve essere "prevista dalla legge" e mostrarsi come necessaria "in una società democratica" al fine di tutelare uno o più degli obiettivi ivi elencati. Infine, sebbene non sia previsto espressamente come requisito, la Corte EDU specifica una serie di obblighi procedurali da applicare nel momento in cui viene conferito in capo alle autorità nazionali l'esercizio di un potere di ingerenza rispetto ai diritti garantiti dall'Art. 8. Il processo decisionale che conduce ad autorizzare misure che possano interferire con i diritti di cui all'Art. 8 "deve essere equo e tale da rispettare debitamente gli interessi della persona [ivi] tutelati".[95] Ciò comporta che il soggetto i cui diritti vengono limitati deve poter prendere parte a tale processo, considerato nel suo complesso, affinché venga a lui garantita la necessaria tutela dei suoi diritti, così come salvaguardati dall'Art. 8,[96] e che il processo in sé comporti un bilanciamento tra tutti gli interessi coinvolti.[97]

5.1.1. L'art. 8 CEDU e le indagini informatiche

Grazie ad un'interpretazione liberale ed evolutiva da parte della Corte EDU degli interessi garantiti dall'Art. 8 e delle possibili limitazioni ivi previste, è stato possibile adeguare lo scopo di applicazione della norma agli sviluppi sociali e tecnologici. Dunque, ad oggi l'Art. 8 assume un ruolo di vero e proprio "baluardo" rispetto alle diverse misure nazionali di indagine informatica.[98] Garantire tale protezione si dimostra essenziale dal momento che il progresso tecnologico ha ampliato tanto il numero quanto il livello di intrusività degli strumenti di ricerca e sorveglianza elettroniche adoperati dalle autorità investigative e di *intelligence* nazionali. Sotto questo profilo, proprio sulla base del grado di interferenza di tali attività con i diritti

[95] Corte Europea dei Diritti Dell'uomo, 'Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza' (31 agosto 2021) <https://www.giustizia.it/cmsresources/cms/documents/guida_cedu_articolo8_agg31ago2021.pdf> ultimo accesso 29 settembre 2023, 7.
[96] *Lazoriva c Ucraina*, App no 6878/14 (Corte EDU 17 luglio 2018), para 63.
[97] *Liebscher c Austria*, App no 5434/17 (Corte EDU 6 aprile 2021), paras 64-69.
[98] Federica Iovene, 'Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale' (2014) 3-4 Diritto Penale Contemporaneo 329, 337.

garantiti all'Art. 8(1), la Corte EDU concede un diverso margine di discrezionalità alle Parti contraenti per stabilire, applicare ed interpretare requisiti specifici per ciascun mezzo di ricerca della prova digitale, alla luce delle condizioni stabilite all'Art. 8(2) CEDU. La Corte di Strasburgo ha infatti chiarito che ogni Parte, che rivendichi un ruolo pionieristico nello sviluppo di nuove tecnologie investigative, deve anche assumere la responsabilità di stabilire un giusto equilibrio tra l'interesse pubblico alla prevenzione e repressione dei reati e la protezione della vita privata degli individui sottoposti a tali misure.[99] Sebbene la Corte EDU non si sia ancora pronunciata sulle tecniche investigative più recenti, come ad esempio le tecniche di *hacking*, *open source intelligence* o *predictive policing*, ha tuttavia stabilito garanzie minime in relazione ad altre misure investigative, come le intercettazioni "mirate" (c.d. "*targeted interception*"), le intercettazioni di massa (c.d. "*bulk interception*"), e le perquisizioni e sequestri digitali.[100]

Le intercettazioni "mirate"

Qualsiasi forma di intercettazione di telecomunicazioni, in quanto recante una grave intrusione nella vita privata e nella corrispondenza di chi vi è sottoposto, deve rispettare le condizioni di cui all'Art. 8(2) CEDU, vale a dire (i) l'esistenza di una base legale appropriata, (ii) il perseguimento di un fine legittimo, e (iii) la sussistenza, in una società democratica, della necessità di perseguire tale fine. Tuttavia, ad oggi le nuove misure adottate da diversi sistemi nazionali di intercettazioni c.d. di massa si differenziano in maniera significativa rispetto al modello tradizionale di intercettazione.[101] Le misure appartenenti a quest'ultima categoria sono "mirate", vale a dire vengono autorizzate in relazione ad uno specifico procedimento penale nei confronti di determinati soggetti. [102] Diversamente, le intercettazioni di massa mirano al monitoraggio di comunicazioni tra persone, al fine di indagare su una serie di reati "gravi", solitamente al di fuori della giurisdizione territoriale dello Stato, anche se è possibile che la

[99] Marianne Hirsch Ballin e Maša Galič, 'Digital investigation powers and privacy' (2021) 4 Boom Strafblad 148, 149.
[100] Ibid.
[101] Veljko Turanjanin, 'When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights Approach' (2022) 4 International Cybersecurity Law Review.
[102] Corte Europea dei Diritti dell'Uomo, 'Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza' (31 agosto 2021) <https://www.giustizia.it/cmsresources/cms/documents/guida_cedu_articolo8_agg31ago2021.pdf> ultimo accesso 29 settembre 2023, 138.

misura sia effettuata all'interno dei confini domestici.[103] Alla luce di tali differenze occorre analizzare separatamente le garanzie previste dalla Corte EDU per i due strumenti investigativi.

Rispetto alle intercettazioni "tradizionali", la giurisprudenza della Corte EDU ha adottato un approccio particolarmente rigoroso circa l'interpretazione delle condizioni di cui all'Art. 8(2) CEDU.

In primo luogo, affinché la condizione di riserva di legge sia soddisfatta, le norme che stabiliscono le circostanze e le condizioni in cui l'intercettazione possa essere autorizzata e attuata devono essere precise e dettagliate affinché il quadro normativo complessivo garantisca certezza giuridica.[104] Allo stesso tempo, devono garantire accessibilità e prevedibilità. Rispetto a questo ultimo requisito, la Corte chiarisce che ciò non si traduce nella necessità che un individuo debba essere in grado di prevedere quando le autorità probabilmente intercetteranno le sue comunicazioni, in modo da poter adattare la propria condotta di conseguenza.[105] Tuttavia, è necessario tenere in considerazione che tali misure investigative, proprio perché necessitano per la loro efficacia di essere attuate "in segreto", non vengono sottoposte al controllo delle persone le cui comunicazioni vengono intercettate.

Al fine di evitare abusi, è quindi essenziale garantire, in uno Stato di diritto, una serie di limiti per regolare il margine di discrezionalità giuridica, che deve essere concessa alla polizia e alle autorità giudiziarie a causa della natura stessa delle intercettazioni. In particolare, la legge deve definire in maniera precisa le categorie di soggetti suscettibili di essere sottoposti a tali misure, individuando altresì la tipologia di reati che possono giustificare l'applicazione di tali strumenti investigativi.[106] Inoltre, deve essere stabilito un termine temporale massimo entro il quale tali intercettazioni possono essere effettuate, al fine di garantire un adeguato bilanciamento tra l'esigenza di perseguire l'attività criminosa e la tutela della vita privata e della corrispondenza di chi è soggetto a tali misure. In aggiunta, è fondamentale che la normativa delinei in modo chiaro le condizioni e i requisiti per la redazione di verbali, volti a riassumere le conversazioni

[103] *Big Brother Watch e altri c Regno Unito*, Apps nos 58170/13, 62322/14 e 24960/15 (Corte EDU 25 maggio 2021), paras 322 e 345.
[104] *Huvig c Francia*, App no 11105/84 (Corte EDU 24 aprile 1990), para 32.
[105] *Karabeyoğlu c Turchia*, App no 30083/10 (Corte EDU 7 giugno 2016), para 67.
[106] *Karabeyoğlu c Turchia*, App no 30083/10 (Corte EDU 7 giugno 2016), para 88.

intercettate. Infine, devono essere menzionate le circostanze in cui le registrazioni possono o devono essere cancellate o distrutte.[107]

In secondo luogo, rispetto al requisito della necessità in una società democratica di perseguire uno scopo legittimo, la Corte ha riconosciuto che, nel bilanciare l'interesse pubblico a proteggere la propria sicurezza nazionale attraverso misure di intercettazione segreta da una parte, e la gravità dell'interferenza con il diritto del richiedente al rispetto della propria vita privata dall'altra, le autorità nazionali godono di un certo margine di apprezzamento nella scelta dei mezzi per raggiungere lo scopo legittimo di proteggere la sicurezza nazionale.[108] Tuttavia, questo margine è soggetto a un controllo da parte della Corte EDU circa l'operato sia del legislatore che delle corti nazionali. Al fine di evitare che tali misure investigative possano minare o addirittura distruggere la democrazia con il pretesto di difenderla, la Corte deve accertarsi che esistano garanzie adeguate ed efficaci contro gli abusi.[109] Tale valutazione dipende da tutte le circostanze del caso, come la natura, la portata e la durata delle possibili misure, i motivi necessari per ordinarle, le autorità competenti ad autorizzarle, eseguirle e controllarle e il tipo di rimedio previsto dal diritto nazionale.[110] In particolare, la Corte deve stabilire se il riesame e le procedure di supervisione dell'ordine e dell'attuazione delle misure investigative siano tali affinché l'interferenza non ecceda quanto necessario in una società democratica.[111]

Sotto questo profilo, il riesame e la supervisione delle misure di intercettazione possono intervenire in tre fasi: quando questa viene ordinata per la prima volta, durante la sua esecuzione o una volta conclusasi l'intercettazione.[112]

Per quanto riguarda le prime due fasi, la natura stessa e la logica della misura investigativa impongono che non solo l'attuazione stessa, ma anche il relativo riesame sia effettuato in "segreto".[113] Di conseguenza, poiché all'individuo sarà necessariamente impedito di cercare un

---

[107] Ibid.
[108] Corte Europea dei Diritti dell'Uomo, 'Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza' (31 agosto 2021) <https://www.giustizia.it/cmsresources/cms/documents/guida_cedu_articolo8_agg31ago2021.pdf> ultimo accesso 29 settembre 2023, 135.
[109] Ibid.
[110] *Roman Zakharov c Russia*, App no 47143/06 (Corte EDU 4 dicembre 2015), para 232.
[111] Ibid.
[112] Ibid, paras 233-234.
[113] Corte Europea dei Diritti dell'Uomo, 'Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza' (31 agosto 2021)

rimedio efficace di propria iniziativa o di partecipare direttamente a qualsiasi procedimento di revisione, è essenziale che le procedure stabilite forniscano esse stesse garanzie adeguate ed equivalenti a tutela dei suoi diritti. Inoltre, i valori di una società democratica devono essere seguiti il più fedelmente possibile nelle procedure di controllo, se non si vogliono superare i limiti della necessità di cui all'Art. 8(2). Alla luce di questo tanto delicato quanto essenziale equilibrio da raggiungere, è auspicabile stabilire una riserva di giurisdizione, in modo da affidare il controllo ad un'autorità giudiziaria che possa garantire l'indipendenza, l'imparzialità e la correttezza di tale riesame e supervisione.[114] Una volta terminata l'esecuzione della misura, se l'Art. 8(2) viene letto in combinato disposto con l'Art. 6(1) CEDU, in seguito analizzato, la persona sottoposta a intercettazione telefonica deve avere accesso, ad un certo punto del procedimento, ad "riesame effettivo" al fine di poter impugnare tali misure.[115]

Le intercettazioni di massa

Spinti dall'esigenza di affrontare nuove e diverse minacce da parte di una vasta gamma di attori internazionali che sfruttano i mezzi di comunicazione elettronica con finalità terroristiche e di criminalità organizzata, gli Stati moderni ricorrono sempre più spesso all'impiego di intercettazioni di massa a fini di tutelare la sicurezza pubblica nazionale e proteggere la propria democrazia, con particolare enfasi sulla finalità preventiva.[116] Tuttavia, alla luce delle loro caratteristiche pervasive, che le rendono efficaci strumenti di *intelligence* e le distinguono dalle intercettazioni "tradizionali", le intercettazioni di massa interferiscono gravemente con i diritti fondamentali necessari per il mantenimento di uno Stato di diritto e in particolare con gli interessi tutelati all'Art. 8(1) CEDU.[117]

Nel 2021, la Corte EDU ha approfonditamente elaborato rispetto alla compatibilità di tali sistemi con la CEDU, in occasione delle sentenze della Grande Camera in merito ai ricorsi contro il Regno Unito e la Svezia e i loro regimi di sorveglianza di massa. La storica sentenza *Big Brother Watch e altri c Regno Unito*[118]("***BBW***"), rappresenta l'esito finale di una lunga

<https://www.giustizia.it/cmsresources/cms/documents/guida_cedu_articolo8_agg31ago2021.pdf> ultimo accesso 29 settembre 2023, 135.

[114] *Klass e altri c Germania*, App no 5029/71 (Corte EDU 6 settembre 1978), para 55.

[115] Ibid.

[116] Paolo Viafora, 'Le intercettazioni di massa all'esame della CEDU' (2023) Amministrazioni in Cammino, 1.

[117] Ibid.

[118] *Big Brother Watch e altri c Regno Unito*, Apps nos 58170/13, 62322/14 e 24960/15 (Corte EDU 25 maggio 2021).

battaglia, iniziata dopo le rivelazioni di Snowden nel 2013,[119] che ha visto protagoniste diverse organizzazioni per i diritti umani contro il regime di sorveglianza di massa del governo britannico.[120] Questa famosa sentenza ha anche una "sorella minore", la decisione *Centrum för Rättvisa c Svezia*,[121] avente ad oggetto le leggi delle agenzie di *intelligence* svedesi e le loro pratiche di sorveglianza di massa.

Sulla base del *dictum* di queste decisioni, è possibile trarre una serie di garanzie che le parti contraenti sono tenute ad implementare affinché i loro sistemi di *mass surveillance* siano compatibili con la CEDU e in particolare con le condizioni di cui all'Art. 8(2). La decisione *BBW* apre con un'importante premessa: i sistemi di intercettazione di massa sono di per sé compatibili con la Convenzione.[122] Dunque, la Corte concorda con il previo giudizio della Camera sul fatto che, ai sensi della CEDU, le intercettazioni di massa non sono di per sé inammissibili e ribadisce l'ampio margine di apprezzamento di cui godono i governi quando si tratta di scelte politiche di sicurezza nazionale. La *ratio* di tale approccio risiede nella constatazione da parte della Corte che ad oggi tali sistemi rivestono un ruolo chiave per "identificare le nuove minacce" del dominio digitale e dunque la loro impostazione da parte dei regimi nazionali sia inevitabile per combattere la criminalità nella nuova era digitale.[123] Di conseguenza, il fulcro della valutazione si sposta sul rispetto da parte degli Stati contraenti alle c.d. "*end-to-end safeguards*", vale a dire delle salvaguardie fondamentali che dovrebbero costituire, secondo la Corte, il caposaldo di qualsiasi regime di intercettazione di massa conforme all'Art. 8 CEDU.[124]

---

[119] Nel mese di giugno del 2013, grazie alle rivelazioni di Edward Snowden, ex dipendente della CIA, l'esistenza del programma di sorveglianza elettronica statunitense noto come PRISM fu portata all'attenzione dei media e della comunità internazionale. Tale programma consentiva alle autorità di polizia e di *intelligence* degli Stati Uniti, in particolare alla *National Security Agency* (NSA) e al *Federal Bureau of Investigation* (FBI), di accedere direttamente alle informazioni personali di individui, inclusi cittadini europei, che utilizzavano i principali *service providers* americani. Questo accesso consentiva una sorveglianza indiscriminata e prolungata dei dati, violando apertamente le norme internazionali ed europee sulla privacy individuale.

[120] Juraj Sajfert, 'The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?' (European Law Blog 8 giugno 2021) <https://europeanlawblog.eu/2021/06/08/big-brother-watch-and-centrum-for-rattvisa-judgments-of-the-grand-chamber-of-the-european-court-of-human-rights-altamont-of-privacy/> ultimo accesso 29 settembre 2023.

[121] *Centrum för Rättvisa c Svezia,* App no 35252/08 (Corte EDU 25 maggio 2021).

[122] *Big Brother Watch e altri c Regno Unito,* Apps nos 58170/13, 62322/14 e 24960/15 (Corte EDU 25 maggio 2021), paras 322-323.

[123] Ibid.

[124] Ibid, para 350.

Innanzitutto, la Corte EDU descrive il sistema di intercettazioni di massa come un processo graduale, in cui il grado di interferenza causato nella vita privata degli intercettati aumenta progressivamente al passaggio ad una nuova fase del procedimento.[125] Le prime fasi consistono infatti nel captare e conservare "tutto il traffico di dati e metadati in transito per un determinato punto di raccolta", ai quali vengono poi applicati dei selettori o filtri, consistenti ad esempio nell'utilizzo di parole-chiave.[126] Questa fase è funzionale al fine di effettuare in un passaggio successivo una selezione circa il materiale più rilevante. Infine, i dati selezionati vengono usati e trasmessi a parti terze.[127]

Alla luce di tali passaggi, la Corte ha elaborato una serie di garanzie, aggiornando la sua previa giurisprudenza in materia. È dunque necessario garantire al livello nazionale, in primo luogo, che in ogni fase del procedimento, venga effettuata una valutazione circa la necessità e la proporzionalità delle misure adottate. In secondo luogo, tali misure devono essere autorizzate *ex ante* da un'autorità indipendente, che definisca l'oggetto e la portata dell'operazione. Rispetto a tali garanzie, la Corte sottolinea come la qualifica di autorità giudiziaria per quanto sia un fattore importante contro potenziali abusi, non è necessaria purché sia comunque garantita la caratteristica dell'indipedenza.[128] Inoltre, viene specificato che, alla luce dell'impossibilità pratica di includere nell'autorizzazione tutti i selettori che si andranno ad utilizzare, visto il grande numero solitamente impiegato, l'autorizzazione potrà limitarsi ad identificare solo le macro categorie di selettori utilizzati. In terzo luogo, devono essere garantiti una supervisione e un controllo da parte di un'autorità indipendente anche *ex post*.[129] Rispetto alle intercettazioni tradizionali, l'importanza di garantire una fase di supervisione e controllo risulta essere amplificata.[130] L'esigenza di segretezza caratterizzante le intercettazioni di massa non presenta solo la conseguenza di non permettere un controllo durante la fase di autorizzazione e attuazione delle misure, ma ha effetti anche rispetto alla possibilità di garantire un rimedio *ex post*. Questo perché per motivi di sicurezza nazionale, gli Stati spesso non

[125] Ibid, para 330.
[126] Paolo Viafora, 'Le intercettazioni di massa all'esame della CEDU' (2023) Amministrazioni in Cammino, 3.
[127] *Big Brother Watch e altri c Regno Unito*, Apps nos 58170/13, 62322/14 e 24960/15 (Corte EDU 25 maggio 2021), para 325.
[128] Ibid, para 351.
[129] Ibid, para 350.
[130] Ibid, para 349.

potranno essere liberi di divulgare informazioni relative al funzionamento dei regimi, necessarie ai fini di esercitare una loro contestazione efficace.[131]

Dunque, sulla base di queste considerazioni e alla luce dei criteri di cui all'Art. 8 della "previsione per legge" e della "necessità in una società democratica", al fine di valutare la compatibilità con la Convenzione del regime nazionale di *mass surveillance*, la Corte EDU deve verificare se il quadro normativo nazionale definisca in maniera chiara: (i) i motivi che consentono l'autorizzazione di intercettazioni di massa; (ii) le circostanze che consentono l'intercettazione delle comunicazioni di una persona; (iii) la procedura da seguire per la concessione dell'autorizzazione; (iv) le procedure da seguire per la selezione, l'esame e l'utilizzo del materiale intercettato; (v) le precauzioni da adottare per la comunicazione del materiale a terzi; (vi) i limiti alla durata dell'intercettazione e della conservazione del materiale intercettato e le circostanze che ne impongono la cancellazione e la distruzione; (vii) le procedure e le modalità della vigilanza esercitata da un'autorità indipendente nel rispetto delle suddette garanzie e i suoi poteri in caso di inosservanza; e (viii) le procedure per un riesame *ex post* dell'osservanza e i poteri conferiti all'organo competente per trattare i casi di inosservanza.[132]

Sia in *BBW*[133] che in *Centrum för Rättvisa c. Svezia*[134], avendo riscontrato una serie di carenze rispetto alle garanzie elencate, la Corte ha dichiarato l'incompatibilità con la CEDU di entrambi i sistemi.

Le perquisizioni e i sequestri digitali

La Corte EDU si è occupata anche di diversi casi di perquisizione e sequestro digitale, vale a dire l'accesso e il sequestro di dati elettronici memorizzati su vari supporti fisici, quali, ad esempio, uno smartphone, un computer portatile o un disco rigido.[135] Rispetto alla perquisizione e sequestro tradizionali o "materiali", la Corte riconosce che queste ultime interferiscono con i diritti di cui all'Art. 8(1) CEDU e dunque devono essere regolate ed applicate alla luce dei limiti

[131] Ibid.
[132] Ibid, para 361.
[133] Ibid, para 425.
[134] *Centrum för Rättvisa c Svezia*, App no 35252/08 (Corte EDU 25 maggio 2021), para 369.
[135] Marianne Hirsch Ballin e Maša Galič, 'Digital investigation powers and privacy' (2021) 4 Boom Strafblad 148, 151.

imposti dall'Art. 8(2).[136] Alla luce di una recente giurisprudenza della Corte EDU,[137] ad oggi è possibile affermare che tali garanzie si applicano anche ai sequestri e alle perquisizioni digitali.

Dunque, la perquisizione e il sequestro, che abbiano o meno ad oggetto dati elettronici, possono rappresentare una grave interferenza con la vita privata, il domicilio e la corrispondenza e devono quindi basarsi su una "legge" particolarmente precisa, chiara e dettagliata.[138] Rispetto al verificare se tali misure siano necessarie in una società democratica, la Corte deve valutare se il rapporto tra lo scopo che si vuole raggiungere e i mezzi impiegati possa essere considerato proporzionato.[139] Per stabilire se tale bilanciamento sia stato raggiunto, la Corte esamina se la misura si basi su un mandato emesso da un giudice, fondato su un "ragionevole sospetto" che deve sussistere al momento dell'emissione del mandato. Inoltre, la portata di quest'ultimo deve essere ragionevolmente limitata.[140] Qualora tale condizione non venga soddisfatta e vengano dunque autorizzati una perquisizione e un sequestro di dati informatici in modo generale e illimitato, la Corte deve verificare se tali carenze siano state compensate da sufficienti garanzie procedurali, in grado di proteggere il ricorrente da qualsiasi abuso o arbitrarietà.[141] Tali salvaguardie possono riferirsi alla fase di esecuzione del mandato, rispetto alla quale la Corte valuta sia la sussistenza di garanzie procedurali "tradizionali" come, ad esempio, se le misure siano state attuate in presenza dell'indagato e del suo difensore o l'esistenza di garanzie che assicurino l'integrità del dato digitale.[142] In aggiunta, la Corte considera anche se l'indagato abbia avuto il diritto di impugnare *ex post* le misure investigative. Sotto questo profilo, riveste particolare importanza le modalità in cui la corte nazionale ha esercitato il proprio potere di supervisione circa la proporzionalità e la necessarietà delle misure ordinate, in particolare rispetto alla quantità di dati memorizzati oggetto di perquisizione e sequestro.[143]

---

[136] *Petri Sallinen e altri c Finlandia,* App no. 50882/99 (Corte EDU 27 settembre 2005), para 90.
[137] Ibid.
[138] *Saber c Norvegia,* App no 459/18 (Corte EDU, 17 dicembre 2020), para 50.
[139] *Robathin c Austria,* App no 30457/06 (Corte EDU 3 ottobre 2012), para 43.
[140] Ibid, para 44.
[141] Ibid, para 47.
[142] Ibid, para 49.
[143] Ibid, 51.

5.2. Il diritto ad un equo processo (Art. 6 CEDU)

L'Art. 6 CEDU tutela il diritto ad un processo equo, la cui definizione è funzionale e viene valutata in base alle circostanze particolari del caso concreto.[144] Lo scopo di applicazione della norma si estende ad ogni procedimento penale, a prescindere dal tipo di reato perseguito,[145] fin dal momento in cui viene formulata l'"accusa penale". Quest'ultimo concetto viene definito in maniera autonoma dalla Corte, vale a dire a prescindere da possibili categorizzazioni al livello nazionale. Il termine viene interpretato in una sua accezione materiale,[146] venendo dunque considerata "accusata in materia penale" ai sensi dell'Art. 6 una persona sospettata che viene soggetta ad interrogatorio in relazione alla sua eventuale partecipazione a fatti costitutivi di un reato.[147] La fase delle indagini assume infatti un'importanza particolare nella preparazione del procedimento penale, poiché le prove acquisite durante questa fase spesso delineano il contesto in cui il reato imputato sarà valutato nel corso del processo.[148] Le leggi nazionali possono attribuire conseguenze decisive all'atteggiamento dell'indagato durante le prime fasi degli interrogatori di polizia, il che influisce significativamente sulle prospettive della difesa in un possibile futuro processo penale. Di conseguenza, il sospettato può trovarsi in una posizione di particolare vulnerabilità durante questa fase del procedimento, e tale vulnerabilità può essere amplificata da una legislazione sempre più complessa in materia di procedura penale, soprattutto per quanto riguarda le norme che regolano la raccolta e l'utilizzo delle prove.[149]

L'Art. 6(1) CEDU garantisce il diritto di accesso ad un tribunale costituito per legge, indipendente ed imparziale, e il diritto ad avere una causa che venga decussa equamente, entro un termine ragionevole e la cui sentenza venga resa pubblicamente. Al terzo paragrafo sono poi elencate una serie di garanzie che contribuiscono a salvaguardare il carattere equo del processo penale nel suo complesso.[150] I "diritti della difesa", elencati in modo non esaustivo dall'Art. 6(3), sono stati istituiti con la finalità principale di garantire, per quanto possibile, l'uguaglianza

[144] *Ibrahim e altri c Regno Unito*, Apps nos 50541/08, 50571/08, 50573/08 e 40351/09 (Corte EDU 13 settembre 2016), para 250.
[145] *Negulescu c Romania*, App no 11230/12 (Corte EDU 31 maggio 2021), paras 39-42.
[146] *Deweer c Belgio*, App no 6903/75 (Corte EDU, 27 febbraio 1980), para 44.
[147] *Aleksandr Zaichenko c Russia*, App no 39660/02 (Corte EDU 18 febbraio 2010), paras 41-43.
[148] *Ibrahim e altri c Regno Unito*, Apps nos 50541/08, 50571/08, 50573/08 e 40351/09 (Corte EDU 13 settembre 2016), para 254.
[149] Ibid.
[150] Ibid, 251.

tra l'accusa e la difesa.[151] Sotto questo profilo, il principio della parità delle armi e il diritto al contraddittorio sono entrambi al centro del diritto alla difesa e costituiscono una "caratteristica intrinseca" di un processo penale equo.[152] In particolare, il principio della parità delle armi richiede che a ciascuna parte del procedimento penale venga data una ragionevole opportunità di presentare il proprio caso in condizioni che non la pongano in una posizione di svantaggio rispetto all'avversario.[153] Il principio del contradditorio garantisce invece alle parti la possibilità di conoscere e commentare tutte le prove inserite nel fascicolo del procedimento, sul quale il giudice baserà la sua decisione. In aggiunta, un processo penale equo richiede che le prove siano prodotte in presenza dell'imputato in un'udienza pubblica al fine di creare un contraddittorio (principio dell'oralità e principio del contraddittorio) [154] e che le autorità dell'accusa permettano alla difesa di accedere, nei tempi e con le facilitazioni necessarie per preparare la difesa, a tutte le prove in loro possesso sia *favor* che *contra rei* (principio della divulgazione delle prove).

Tuttavia, il diritto ad un processo equo e tutte le garanzie in esso comprese non presentano una natura assoluta, potendo dunque subire delle limitazioni al fine di stabilire un equilibrio con altri interessi concorrenti. Conseguentemente, è possibile che la difesa non abbia accesso ad alcune prove e alle modalità attraverso cui tali prove siano state raccolte, al fine di tutelare dei diritti fondamentali di terzi, come ad esempio il diritto ad una vita privata e familiare, oppure per salvaguardare un interesse pubblico, come ad esempio ragioni di ordine pubblico e sicurezza nazionale.[155] Tali restrizioni devono tuttavia rispettare il principio di proporzionalità ed essere "controbilanciate dalle procedure seguite dalle autorità giudiziarie".[156] Tale valutazione deve essere effettuata dal giudice nazionale che dovrà assicurare in ogni caso che l'essenza del principio di parità delle armi sia rispettata, e dunque che, ad un certo punto del

[151] Corte Europea dei Diritti dell'Uomo, 'Guida sull'articolo 6 della Convenzione europea dei diritti dell'uomo Diritto a un processo equo (profilo penale)' (30 aprile 2022) <https://www.echr.coe.int/documents/d/echr/Guide_Art_6_criminal_ITA> ultimo accesso 29 settembre 2023, 80.
[152] Ibid, 34.
[153] Ibid.
[154] *Kostovski c Olanda*, App no 11454/85 (Corte EDU 20 novembre 1989), para 41.
[155] Ibid 61.
[156] Ibid 62.

procedimento, venga comunque garantito all'imputato di contestare le prove acquisite *contra rei*, che abbiano "un peso importante sulle accuse formulate a suo carico".[157]

5.2.1. L'ammissibilità della prova e lo scrutinio della Corte EDU

Sebbene l'Art. 6 CEDU garantisca il diritto ad un equo processo, la disposizione non contiene alcuna norma sull'ammissibilità delle prove, che è quindi principalmente una questione regolata dal diritto nazionale.[158] In linea di principio, la Corte di Strasburgo non è dunque tenuta a pronunciarsi sull'ammissibilità delle prove, la cui valutazione rientra nella competenza delle corti nazionali.[159]

Allo stesso tempo, la Corte deve valutare, ai sensi dell'Art. 6 CEDU, l'equità del processo penale nel suo complesso, compreso il modo in cui le prove sono state raccolte.[160] Ciò comporta un esame dell'eventuale "illegalità" contestata e, nel caso di violazione di un altro diritto della Convenzione, della natura della violazione riscontrata.[161] È altresì imprescindibile valutare se siano stati debitamente rispettati i diritti della difesa. In particolare, occorre verificare se sia stato offerto al ricorrente l'opportunità di mettere in discussione l'autenticità dell'elemento di prova e di opporsi al suo utilizzo.[162] Tuttavia, sotto questo profilo, non rileva il fatto che l'esercizio di tale diritto non abbia portato ad un esito *favor rei* nelle varie fasi del procedimento.[163] Inoltre, è indispensabile considerare anche la qualità dell'elemento di prova, esaminando se le circostanze in cui è stato acquisito sollevino dubbi sulla sua affidabilità o precisione. Sebbene l'equità non necessariamente venga compromessa quando la prova ottenuta non è corroborata da altri elementi, quando l'elemento di prova è estremamente solido e non viene contestato, diventa superflua la necessità di ulteriori elementi a sostegno.[164] Tenendo conto di ciò, la Corte ritiene fondamentale, alla luce delle circostanze del caso

---

[157] Corte Europea dei Diritti dell'Uomo, 'Guida sull'articolo 6 della Convenzione europea dei diritti dell'uomo Diritto a un processo equo (profilo penale)' (30 aprile 2022) <https://www.echr.coe.int/documents/d/echr/Guide_Art_6_criminal_ITA> ultimo accesso 29 settembre 2023, 38.
[158] *Dragojević c Croatia*, App no 68955/11 (Corte EDU, 15 gennaio 2015), para 127.
[159] *Schenk c Svizzera*, App no 10862/84 (Corte EDU 12 luglio 1988), paras 45-46.
[160] *Ayetullah Ay c Turchia*, Apps nos 29084/07 and 1191/08 (Corte EDU 27 ottobre 2020), paras 123-130.
[161] *Khan c Regno Unito*, 35394/97 (Corte EDU 4 ottobre 2000), para 34.
[162] Corte Europea dei Diritti dell'Uomo, 'Guida sull'articolo 6 della Convenzione europea dei diritti dell'uomo Diritto a un processo equo (profilo penale)' (30 aprile 2022) <https://www.echr.coe.int/documents/d/echr/Guide_Art_6_criminal_ITA> ultimo accesso 29 settembre 2023, 44.
[163] *Schenk c Svizzera*, App no 10862/84 (Corte EDU 12 luglio 1988), para 7.
[164] *Jalloh c Germania*, App no 54810/00 (Corte EDU 11 luglio 2006), para 96.

concreto, stabilire se l'elemento di prova in questione abbia avuto un ruolo determinante nell'esito del procedimento penale.[165]

Dunque, è stato riconosciuto dalla Corte che determinate violazioni dei diritti fondamentali in relazione alla raccolta nazionale o transfrontaliera di prove possano compromettere l'equità del procedimento al punto tale da portare la corte nazionale ad escludere tale prova.[166] La stessa conseguenza può verificarsi quando le prove anche se legittimamente raccolte vengano poi utilizzate nel processo in assenza di fondamentali garanzie procedurali.[167] Tuttavia, la Corte EDU lascia un margine di discrezionalità alle corte nazionali, le quali pur dovendo esaminare il modo in cui le prove sono state ottenute e utilizzate nel procedimento penale, rimangono libere di decidere se l'esclusione di tali prove sia il rimedio adeguato, alla luce dell'obiettivo finale di garantire l'equità del procedimento nel suo complesso.[168] Del resto, è necessario considerare che assicurare l'effettività della giustizia penale è considerata dalla Corte EDU come una funzione fondamentale dello Stato, che giustifica la compressione delle garanzie individuali in misura ancor maggiore rispetto ad altri ambiti.[169] L'unica eccezione che richiede sempre come rimedio un'esclusione obbligatoria è quando la prova è stata ottenuta in violazione di diritti umani assoluti, come il divieto di tortura e di trattamenti inumani (Art. 3 CEDU).[170] La Corte ha chiarito che l'ammissione di confessioni ottenute mediante tortura o altri maltrattamenti, in violazione dell'Art. 3 CEDU, come prova per stabilire i fatti rilevanti in un procedimento penale, rende il procedimento intrinsecamente iniquo. Ciò vale indipendentemente dal valore probatorio delle dichiarazioni stesse e dal fatto che un loro utilizzo abbia rivestito un ruolo decisivo rispetto alla condanna dell'imputato.[171]

5.2.2. L'ammissibilità della prova digitale

Le considerazioni espresse riguardo alla relazione tra la tutela delle garanzie stabilite dall'Art. 6 CEDU, interpretate dalla Corte EDU, e la disciplina sull'ammissibilità delle prove acquisite

---

[165] *Gäfgen c Germania*, App no 22978/05 (Corte EDU 1° giugno 2010), para 164.
[166] John Vervaele, 'Lawful and fair use of evidence from a European Human Rights Perspective' in Fabio Giuffrida and Katalin Ligeti (eds) *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings* (University of Luxembourg 2019), 94.
[167] Ibid.
[168] *A.M. c Italia* App no 40020/03 (Corte EDU 13 luglio 2012), paras 24-25.
[169] Silvia Allegrezza, 'Giustizia penale e diritto all'autodeterminazione dei dati' (2007) Protezione dei dati personali e accertamento penale, 74.
[170] *Ibrahim e altri c Regno Unito*, Apps nos 50541/08, 50571/08, 50573/08 e 40351/09 (Corte EDU 13 settembre 2016), para 254.
[171] Ibid.

o utilizzate in violazione delle norme nazionali o dei diritti garantiti dalla Convenzione, trovano applicazione anche nel contesto delle prove digitali.

Il rapporto tra gli artt. 8 e 6 CEDU

In considerazione dell'interferenza causata dalle indagini digitali con il diritto al rispetto della vita privata e alla segretezza della corrispondenza, può sorgere la questione se l'utilizzo di prove ottenute in violazione dell'Art. 8 CEDU privi il procedimento nel suo complesso della necessaria equità richiesta dall'Art. 6 CEDU. Questa problematica è stata sollevata in diverse occasioni davanti alla Corte EDU in merito, ad esempio, a cause relative all'utilizzo di prove raccolte con misure illegali di sorveglianza segreta.[172] Infatti, anche nel caso in cui la Corte riscontri una violazione dell'Art. 8 della CEDU tale da rendere ingiustificata l'ingerenza pubblica nella sfera privata dell'individuo, ciò non comporta automaticamente l'esclusione dei dati illegittimamente acquisiti dal materiale probatorio. In diverse occasioni, nonostante la Corte abbia ritenuto che l'uso di intercettazioni "nascoste" violasse l'Art. 8, in quanto tale interferenza non era "conforme alla legge", l'ammissibilità come prova digitale delle informazioni ottenute in tal modo non è stata considerata in contrasto con i requisiti di equità garantiti dall'Art. 6(1) nelle specifiche circostanze del caso concreto.[173]

Rispetto alle violazioni di cui all'Art. 8 CEDU, la Corte si è anche espressa circa l'utilizzo di prove raccolte illegalmente ma in una dimensione transfrontaliera, adottando un approccio simile a quello intrapreso per casi dal carattere squisitamente domestico. In *Echeverri Rodriguez c Olanda,*[174] è stata posta di fronte alla Corte EDU la questione se il successivo utilizzo in un procedimento penale olandese di intercettazioni illegali effettuate negli Stati Uniti potesse essere compatibile con la CEDU. In tale occasione, la Corte ha ribadito che le questioni relative all'ammissibilità delle prove sono principalmente disciplinate dal diritto nazionale. Il compito della Corte è quello di verificare se, ai sensi della CEDU, il procedimento nel suo complesso, comprese le modalità di assunzione delle prove, sia stato equo. Da una parte, la Corte ha ritenuto che la CEDU non precluda la possibilità di affidarsi, nella fase istruttoria, alle informazioni ottenute attraverso indagini penali svolte all'estero. Tuttavia, l'utilizzo successivo di tali informazioni può sollevare problemi ai sensi della CEDU, qualora vi siano ragioni per

[172] A titolo esemplificativo, si veda *Khan c Regno Unito*, 35394/97 (Corte EDU 4 ottobre 2000), para 34.
[173] Ibid.
[174] *Echeverri Rodriguez c Olanda*, App no 43286/98 (Corte EDU 27 giugno 2000), para 8.

ritenere che in tale indagine transfrontaliera siano stati violati i diritti della difesa garantiti dall'Art. 6 CEDU.[175]

Il diritto alla digital discovery e il principio di parità delle armi

La raccolta di prove digitali oltre a interferire con la vita privata di chi è sottoposto a tali misure investigative, possono rappresentare una vera propria sfida sia per la polizia e le autorità giudiziarie, a causa dell'elevato livello di complessità tecnica che le prove digitali possono apportare al procedimento. Questo problema può essere inquadrato nella questione più generale del rapporto tra progresso scientifico e diritto penale, che spinge la polizia e le autorità giudiziarie ad aggiornare costantemente le proprie competenze tecniche per stare al passo con gli ultimi progressi scientifici che possono essere sfruttati dalla criminalità.[176] Al fine di superare tali ostacoli, una volta appresi gli strumenti e le tecniche investigative appropriate, la polizia e le autorità giudiziarie non hanno interesse a rendere noti tali sviluppi, al fine di non perdere il vantaggio acquisito ma soprattutto spesso rivendicando ragioni di ordine pubblico e sicurezza nazionale. Dunque, una conseguenza importante della natura altamente tecnica delle prove digitali è che la polizia e le autorità giudiziarie hanno iniziato ad etichettare il modo di condurre le indagini come "segreto" e dunque solo parzialmente accessibile alla difesa, basando le loro rivendicazioni rispetto ad interessi di difesa e sicurezza nazionale. In tempi di grandi scandali sulla privacy,[177] questa mancanza di trasparenza incide sulla fiducia dei cittadini nei confronti dei sistemi di giustizia penale e soprattutto ostacola il diritto della difesa alla divulgazione delle prove.[178]

Come precedentemente analizzato, il diritto alla divulgazione di prove digitali, conosciuto anche come diritto alla "*digital discovery*", garantito dall'Art. 6 CEDU, rappresenta un elemento fondamentale per garantire l'equità di un procedimento penale, consentendo una parità di mezzi tra la difesa e l'accusa. Tuttavia, la salvaguardia di tale garanzia nel contesto

---

[175] Ibid, para.
[176] Gianrico Ranaldi, 'Processo penale e prova informatica: profili introduttivi' (*Diritto pubblico europeo rassegna online* 2020) <http://www.serena.unina.it/index.php/dperonline/article/view/7031/7976> ultimo accesso 29 settembre 2023.
[177] Vedi ad esempio gli scandali legati alle rivelazioni di Snowden e *Cambridge Analytica*. Per un maggior approfondimento sul tema vedi Philip Di Salvo, 'From Snowden to Cambridge Analytica. An overview of whistleblowing cases as scandals' in Howard Tumber e Silvio Waisbord (eds), *The Routledge Companion to Media and Scandal* (prima edizione Routledge 2019).
[178] Philip Anderson *et al*, 'Digital investigations: relevance and confidence in disclosure' (2021) 22 ERA Forum 587, 597.

delle indagini digitali comporta una serie di problematiche peculiari da tenere in considerazione. In particolare, alla luce delle caratteristiche delle indagini volte ad acquisire prove digitali, sorge il dubbio di come potere garantire un diritto alla *digital discovery*, compatibile con il principio della parità delle armi, quando enormi quantità di dati volatili vengono raccolte con tecniche investigative complesse, che spesso le autorità di polizia non sono disposte a rivelare completamente.[179] A questo proposito, la Corte EDU ha fornito alcune indicazioni sulla quantità di materiale da condividere con l'imputato e sulle condizioni da garantire a quest'ultimo per preparare efficacemente la propria difesa.[180] La Corte ha riconosciuto che le indagini digitali possono comportare la raccolta di una massa di dati che non sono tutti rilevanti ai fini dell'accertamento del fatto di reato. Pertanto, l'accusa in possesso di un vasto volume di materiale non elaborato può essere legittimata a vagliare le informazioni al fine di identificare ciò che è probabilmente rilevante e quindi ridurre il fascicolo a proporzioni gestibili.[181] Tuttavia, in linea di principio, la difesa deve avere la possibilità di (i) partecipare alla definizione dei criteri per determinare ciò che possa essere considerato rilevante e (ii) condurre ulteriori ricerche di prove a suo favore.[182] D'altra parte, a causa di una mancanza di competenze e di risorse necessarie, la difesa potrebbe incontrare numerose difficoltà a comprendere il significato dei dati forniti, rimanendo potenzialmente all'oscuro circa l'esistenza di prove a proprio favore, e rendendo di conseguenza un esercizio effettivo di tali garanzie difficoltoso nella pratica.[183]

---

[179] Laura Bartoli, 'Parità delle armi e *discovery* digitale: qualche indicazione da Strasburgo' (2022) La legislazione penale 1, 3.
[180] *Sigurđur Einarsson e altri c Islanda*, App no 39757/15 (Corte EDU 4 settembre 2019).
[181] Ibid 90.
[182] Ibid.
[183] Fair Trial, 'Policy Brief: The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters' (2018) <https://www.fairtrials.org/app/uploads/2022/02/JUD-IT-Fair-Trials-Policy-Brief-October-2018.pdf> ultimo accesso 29 settembre 2023, 6.

Capitolo 2

L'Unione europea e la prova digitale nel procedimento penale: tra esigenze investigative, *mutual trust* e principio di proporzionalità

SOMMARIO:

1. Introduzione

A partire dagli anni '90, l'UE ha progressivamente acquisito competenze nel settore del diritto penale,[184] affiancando agli strumenti adottati dal Consiglio d'Europa diverse iniziative in materia, volte principalmente a migliorare e rendere più efficiente la cooperazione in materia penale tra le autorità competenti degli Stati membri. Tuttavia, sotto il profilo della prova digitale nel procedimento penale, solo nell'aprile 2018 la Commissione ha annunciato la presentazione di un pacchetto composto da un Regolamento e da una Direttiva, volto a creare, sulla scia degli obiettivi perseguiti dal Secondo Protocollo Addizionale alla Convenzione di Budapest, un quadro giuridico che consentisse alle autorità nazionali di uno Stato membro di richiedere direttamente ai *service providers* di un altro Stato membro di produrre o conservare dati.[185] Dopo cinque anni di complessi negoziati, tale iniziativa è giunta ad un punto di approdo con l'adozione di un testo di compromesso tra Consiglio e Parlamento annunciata a gennaio 2023.[186] Il Regolamento[187] e la Direttiva[188] sono stati pubblicati in Gazzetta Ufficiale il 28 luglio e si applicheranno a decorrere dal 18 agosto 2026.

---

[184] Valsamis Mitsilegas, EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe, (Oxford Hart Publishing 2016), 4.

[185] Stanislaw Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161, 164.

[186] Council of the European Union, 'PRESS RELEASE. Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence' <https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/> ultimo accesso 29 settembre 2023.

[187] Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio del 12 luglio 2023 relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali [2023] OJ L 191/118.

[188] Direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio del 12 luglio 2023 recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali [2023] OJ L 191/181.

Tuttavia, queste misure dovranno coordinarsi, *inter alia*, con il complesso quadro legislativo e la frenetica attività giurisprudenziale dell'Unione in materia di *data retention*. Già nel 2006, venivano infatti adottate dal legislatore dell'UE norme comuni al fine di stabilire un regime di *data retention*, che imponesse agli Stati membri di adottare misure per garantire che i *services providers* conservassero i dati relativi al traffico e all'ubicazione, ad esclusione del contenuto della comunicazione, per un periodo compreso tra sei mesi e due anni, al fine di consentire l'accesso da parte delle autorità nazionali competenti a fini di indagine, accertamento e perseguimento di reati gravi.[189] Questo primo tentativo di istituire un regime di *data retention* al livello europeo è stato, tuttavia, dichiarato invalido dalla Corte di Giustizia dell'UE ("**CGUE**") nel 2014, nella sua storica decisione *Digital Rights Ireland*.[190] A partire da questa pronuncia, si è così instaurato un interessante dialogo giurisprudenziale tra la CGUE, la Corte EDU e le più alte corti nazionali, al fine di verificare se i regimi di *data retention* possano, di fronte alle sfide imposte dall'era digitale, rappresentare o meno un valore aggiunto nella prevenzione e nell'investigazione dei reati e nella protezione della pubblica sicurezza, e dove possa segnarsi il confine rispetto alla protezione dei diritti fondamentali fondanti lo spazio giuridico europeo.[191]

Infine, ai fini del presente elaborato, è interessante analizzare, una volta che la prova digitale sia stata acquisita in un contesto squisitamente domestico o in una dimensione transfrontaliera, a che condizioni tale prova possa essere utilizzata nel processo penale di fronte al giudice nazionale. Nonostante infatti l'introduzione, con il Trattato di Lisbona, di una base legale, vale a dire l'Art. 82 del Trattamento sul Funzionamento dell'UE ("**TFUE**"), e la pubblicazione di successivi *policy documents* che affrontano il problema della necessità di standard comuni in materia di ammissibilità delle prove nei procedimenti penali *cross-border*,[192] gli Stati membri hanno da sempre espresso la loro riluttanza a cedere la propria sovranità in questo settore,[193]

[189] Direttiva 2006/24/CE del Parlamento e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione [2006] OJ L 105/54.
[190] Casi C-293/12 and C-594/12, *Digital Rights Ireland* [2014] ECLI:EU:C:2014:238.
[191] Ibid, 266.
[192] Si veda, a titolo esemplificativo, 'Green paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility' COM (2009) 624 final.
[193] Recentemente gli Stati membri hanno mostrato una certa resistenza a adottare norme comuni sull'ammissibilità delle prove in occasione del nuovo pacchetto sulle prove elettroniche.

sostenendo una potenziale violazione dei principi di sussidiarietà e proporzionalità.[194] Pertanto, sebbene ad oggi la disciplina dell'ammissibilità delle prove in procedimenti penali, sia nazionali che *cross-border*, rimanga principalmente una questione di diritto nazionale, recentemente si è creato un interessante e vivace dialogo tra le istituzioni dell'UE, i suoi Stati membri e la CGUE e sull'ammissibilità delle prove digitali nei procedimenti penali. Mentre la CGUE ha iniziato a fornire indicazioni agli Stati membri sull'ammissibilità delle prove digitali in un contesto nazionale, emettendo diverse sentenze significative in relazione, *inter alia*, alle prove digitali raccolte attraverso i regimi nazionali di *data retention*,[195] le Corti nazionali hanno pronunciato le prime sentenze sull'ammissibilità delle prove raccolte nelle più recenti indagini informatiche *cross-border*,[196] sollevando un primo rinvio pregiudiziale in materia di fronte alla CGUE.[197]

Considerando tali premesse, il seguente Capitolo approfondisce il tema della prova digitale nel procedimento penale nel quadro giuridico dell'Unione, esaminando, in particolare, tre profili: (i) l'accesso *cross-border* alla prova digitale, alla luce delle novità introdotte dal nuovo pacchetto; (ii) la *data retention saga*; e da ultimo (iii) l'ammissibilità della prova digitale domestica e *cross-border* attraverso l'analisi della rilevante giurisprudenza della CGUE.

1.1. La creazione di uno Spazio di Libertà, Sicurezza e Giustizia. Cenni.

Prima di procedere ad un'analisi approfondita dei profili sopra delineati, occorre prima specificare le distintive caratteristiche della cooperazione penale tra Stati membri all'interno dell'Unione.

Fino al Trattato di Maastricht, le questioni relative alla giustizia e agli affari interni erano confinate nel c.d. "terzo pilastro", dove il processo decisionale era principalmente intergovernativo. Tale metodo era dipendente dalla volontà dei governi, in quanto basato esclusivamente dal potere decisionale del Coniglio europeo che adottava atti privi di efficacia

[194] Balázs Garamvölgyi *et al*, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 eucrim 201, 202.
[195] Si veda Caso C-511/18 *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791; Caso C-746/18 *Prokuratuur - Conditions d'accès aux données relatives aux communications électroniques* [2021] ECLI:EU:C:2021:152.
[196] Si vedando i casi *EncroChat* and *Sky ECC*.
[197] Decisione del 19 ottobre 2022 – LG Berlin (525 KLs) 279 Js 30/22 (8/22).

diretta sulle giurisdizioni nazionali e soprattutto sottratti allo scrutinio da parte della CGUE.[198] D'altra parte, gli Stati membri non solo erano riluttanti a cedere le loro competenze penali, ma le differenze nei loro approcci politici in materia, che toccavano questioni molto delicate relative ai diritti fondamentali, rendevano indesiderabile un controllo sovranazionale.[199] Allo stesso tempo, si riconosceva che la cooperazione in materia penale, soprattutto in considerazione della crescente natura transfrontaliera dei reati, fosse indispensabile e che i semplici strumenti internazionali non fossero a tal scopo sufficienti.[200]

Con il c.d. processo di integrazione europea, viene quindi modificato il tradizionale modello di cooperazione giudiziaria internazionale, per lasciare spazio ad una cooperazione fondata sul principio del mutuo riconoscimento.[201] Questo viene enunciato per la prima volta già nel 1999 nella conclusione n. 36 del Consiglio europeo di Tampere, secondo cui "le prove legalmente raccolte dalle autorità di uno Stato membro dovrebbero essere ammissibili dinanzi ai tribunali degli altri Stati membri, tenuto conto delle norme ivi applicabili".[202] In tale occasione viene ribadito come garantire l'ammissibilità delle prove raccolte nei procedimenti penali transfrontalieri giochi un ruolo essenziale nella creazione di uno spazio giuridico unico europeo.[203]

La comunitarizzazione della competenza in materia di giustizia e affari interni è stata quindi avviata dal Trattato di Amsterdam (1997) e completata con il Trattato di Lisbona (2009), in cui i diversi profili della materia vengono ricongiunti in un'unica area, disciplinata dal Titolo V TFUE, che articolandosi in tre filoni, crea ufficialmente uno Spazio di Libertà, Sicurezza e Giustizia ("**SLSG**").[204] Il principio del mutuo riconoscimento delle decisioni penali viene assunto a fondamento della cooperazione giuridica e giudiziaria in materia penale e include "il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri" nel settore del diritto penale procedurale.[205] Sotto quest'ultimo aspetto, all'Art. 82(2)(a) TFEU, viene

---

[198] Roberto Adam e Antonio Tizzano, *Lineamenti del Diritto dell'Unione europea* (Quarta Edizione Giappichelli Editore 2019), 33.
[199] Nathalie A Smuha, 'Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency' (2018) 8(1) European Criminal Law Review 83, 88.
[200] Ibid.
[201] Gaetano De Amicis, 'Limiti e Prospettive del Mandato Europeo di Ricerca della Prova' (2011) Diritto Penale Contemporaneo, 1.
[202] Tampere Consiglio europeo 15 e 16 ottobre 1999 Conclusioni presidenziali, 36.
[203] Ibid.
[204] Roberto Adam e Antonio Tizzano, *Lineamenti del Diritto dell'Unione europea* (Quarta Edizione Giappichelli Editore 2019), 361.
[205] Art. 82(1) TFUE.

previsto che il Parlamento e il Consiglio, deliberando secondo la procedura legislativa ordinaria, adottano, al fine di facilitare il suddetto riconoscimento reciproco, misure intese "a definire norme e procedure per assicurare il riconoscimento in tutta l'Unione di qualsiasi tipo di sentenza e di decisione giudiziaria". Occorre poi sottolineare che eliminando la struttura a pilastri, le misure adottate in materia diventano possibile oggetto di scrutinio da parte della CGUE. Sotto questo profilo, un'altra importante novità introdotta dal Trattato di Lisbona deve essere menzionata ai fini dell'elaborato. Dopo aver elaborato il principio del rispetto dei diritti fondamentali attraverso la giurisprudenza della CGUE e "aver consacrato lo stesso nell'Art. 6 TUE sostanziandolo con un riferimento esplicito a quelli garantiti dalla CEDU e dalle tradizioni comuni agli Stati membri", nel 2000 viene adottata a margine del Consiglio europeo di Nizza la Carta dei diritti fondamentali ("**Carta**"), contenente tutti i diritti sanciti dalla CEDU[206] e tutti quei diritti che costituiscono lo *status* di cittadino dell'Unione.[207] Ai sensi dell'Art. 51 Carta, le disposizioni della Carta si applicano alle istituzioni, organi e organismi dell'Unione nel rispetto del principio di sussidiarietà, come anche agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione. Con il Trattato di Lisbona, la Carta acquisisce efficacia vincolante, assumendo lo stesso valore giuridico dei Trattati.

Alla luce di tale quadro normativo, è possibile affermare che due importanti principi governano l'attuale cooperazione penale tra Stati membri nello SLSG, vale a dire il principio del mutuo riconoscimento e il principio della fiducia reciproca.[208] Se, a differenza del primo principio, non è possibile trovare per il secondo una base legale nei Trattati, si può sostenere che il principio della fiducia reciproca trovi le sue fondamenta nei valori democratici fondamentali dell'Unione (Art. 2 Trattato sull'UE ("**TUE**")), nel principio di uguaglianza tra gli Stati membri nonostante le loro differenze (Art. 4(2) TUE) e nel principio di cooperazione leale e sincera (Art. 4(3) TUE).[209] In particolare, secondo la CGUE, l'esistenza del principio di fiducia

[206] In particolare, ai sensi dell'art. 52(3) Carta: "3. Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa.

[207] Roberto Adam e Antonio Tizzano, *Lineamenti del Diritto dell'Unione europea* (Quarta Edizione Giappichelli Editore 2019), 123.

[208] Valsamis Mitsilegas, 'Mutual recognition, mutual trust and fundamental rights after Lisbon' in Valsamis Mitsilegas et al (eds) *Research Handbook on EU Criminal Law* (Edward Elgar Publishing Limited 2016), 150-151.

[209] Aart de Vries e Rob Widdershoven 'Constitutional Principles and Composite Punitive Enforcement in the EU' in Michiel Luchtman, Katalin Ligeti, John Vervaele (eds) *EU Enforcement Authorities - Punitive Law Enforcement in a Composite Legal Order* (Hart Publishing 2023), 54.

reciproca, che sta alla base del principio del mutuo riconoscimento, sottintende e viene giustificata dalla "fondamentale premessa" che tutti gli Stati Membri condividano, e riconoscano di condividere, un insieme di valori comuni fondatori dell'Unione, come enunciato all'Art. 2 TUE.[210]

Nello SLSG, il principio della fiducia reciproca impone a ciascuno Stato membro di presumere che l'altro ordinamento giuridico nazionale sia in grado di fornire una protezione equivalente ed efficace dei diritti fondamentali riconosciuti a livello dell'UE, in particolare nella Carta.[211] Di conseguenza, nell'attuazione del diritto dell'UE, gli Stati membri non possono esigere da un altro Stato membro un livello di protezione nazionale dei diritti fondamentali superiore a quello previsto dal diritto dell'UE.[212] Questo perché, come sottolineato dalla CGUE, mentre, secondo l'Art. 53 Carta, le autorità e i tribunali nazionali rimangono liberi di applicare in materia di diritti fondamentali standard più elevati, questi incontrano comunque il limite di non compromettere sia il livello di protezione fornito dalla Carta, come interpretato dalla CGUE, che il primato, l'unità e l'efficacia del diritto dell'UE.[213] Soprattutto, sulla base della presunzione di fiducia reciproca, viene impedito agli Stati membri di effettuare dei controlli per verificare se gli altri Stati membri rispettino i diritti fondamentali.[214] Tuttavia, tale presunzione è di natura relativa, il che significa che è possibile una confutazione in presenza di circostanze eccezionali.[215]

2. Accesso *cross-border* alla prova digitale: alla ricerca di un equilibrio tra nuove forme di cooperazione e la protezione dei diritti fondamentali

Un primo tentativo di affrontare a livello comunitario il problema della raccolta *cross-border* di prove è rappresentato dalla Convenzione del 29 maggio 2000 relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea,[216] adottata sulla base

[210] Caso C-216/18 PPU, *LM* [2018] ECLI:EU:C:2018:586, para 35.
[211] Casi C-404/15 and C-659/15 PPU, *Aranyosi e Căldăraru* [2016] ECLI:EU:C:2016:198, para 77.
[212] Opinione 2/13, *Adhésion de l'Union à la CEDH* [2013] ECLI:EU:C:2014:2454, paras 192.
[213] Caso C-399/11, *Stefano Melloni c Ministerio Fiscal* [2013] ECLI:EU:C:2013:107, para 60.
[214] Opinione della Corte 2/13, paras 191-92.
[215] Ibid.
[216] 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 [2000] OJ C 197/1.

dell'Art. 34 dell'allora Trattato dell'Unione Europea con l'obiettivo di rendere più efficiente la cooperazione giudiziaria tra gli Stati membri, senza tuttavia abbandonare il tradizionale approccio di mutua assistenza. Rispetto al tema della prova digitale, se nella Convenzione viene sottolineata l'importanza di tenere conto, nel settore della cooperazione giudiziaria, delle più importanti innovazioni e sviluppi della tecnologia, non viene fatta alcuna distinzione tra le varie tipologie di prova.[217]

Successivamente vengono affiancate a tale strumento due misure basate sul principio del mutuo riconoscimento e aventi ad oggetto solo alcuni specifici profili della raccolta di prove *cross-border*. La differenza di queste due misure rispetto alla Convenzione del 2000 risiede nel fatto che mentre il sistema di cooperazione creato da quest'ultima è relativamente flessibile e offre allo Stato che riceve una richiesta di assistenza un'ampia discrezionalità nel decidere se trattarla o meno, il sistema di mutuo riconoscimento mira ad eliminare tale discrezionalità.[218]

In particolare, nel 2003, viene adottata una decisione-quadro volta a stabilire delle norme per il riconoscimento e l'esecuzione da parte di uno Stato membro di un provvedimento di blocco dei beni o di sequestro probatorio, rilasciato dall'autorità giudiziaria di un altro Stato membro in un procedimento penale.[219] La divisione in due fasi della procedura, che imponeva che il provvedimento di blocco o sequestro venisse sempre accompagnato da una separata e ulteriore richiesta di trasferimento della prova nello Stato richiedente, ha compromesso l'efficienza di tale misura, portando ad un suo utilizzo limitato nella pratica.[220] A tale strumento si è poi aggiunta un'altra decisione quadro, che sul modello del mandato di arresto europeo, delinea un "mandato europeo di ricerca delle prove", diretto all'acquisizione da parte di uno Stato membro di oggetti, documenti e dati in un altro Stato membro al fine di utilizzarli nel procedimento penale nazionale. Tale strumento ha tuttavia presentato fin dall'inizio l'importante limite di avere un ambito di applicazione piuttosto circoscritto, in quanto avente ad oggetto solo prove già "precostituite", mentre per l'acquisizione delle prove

[217] Si vedano artt. 10, 11 e da 17 a 22 relativi alle intercettazioni di telecomunicazioni.
[218] Nathalie A Smuha, 'Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency' (2018) 8(1) European Criminal Law Review 83, 89.
[219] 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 [2003] OJ L 196/45.
[220] Lucio Camaldo, 'La Direttiva sull'Ordine Europeo di Indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione' (27 maggio 2014 Diritto Penale Contemporaneo) <https://archiviodpc.dirittopenaleuomo.org/d/3078-la-direttiva-sull-ordine-europeo-di-indagine-penale-oei-un-congegno-di-acquisizione-della-prova-dot#_ftnref> ultimo accesso 29 settembre 2023.

"costituende", come ad esempio le intercettazioni di comunicazioni, rimaneva necessario ricorrere ancora alle tradizionali forme di assistenza giudiziaria.[221] Dunque, nel contesto pre-Lisbona, lo scambio e la conservazione delle prove nel contesto *cross-border* veniva regolato da una combinazione di strumenti giuridici: (i) per le prove già esistenti venivano inviati mandati europei di ricerca; (ii) per le prove costituende venivano invece adoperati i tradizionali strumenti di cooperazione come le lettere rogatorie; (iii) per la conservazione delle prove dovevano essere inviati gli ordini di blocco o sequestro probatorio.[222] A completare questo quadro, vi era poi la trasmissione "spontanea" tra autorità giudiziarie di informazioni utilizzate, non come prove nel processo penale, ma al fine di assumere una decisione circa l'adozione di misure investigative.[223]

2.1. L'Ordine di Indagine Europeo

Alla luce di questa tanto complessa, quanto poco funzionale nella pratica, combinazione di misure, solo un anno dopo l'adozione della decisione quadro sul mandato europeo di ricerca, con il Programma di Stoccolma, il Consiglio europeo dichiara che sia necessario trovare una nuova soluzione che preveda l'adozione di un unico strumento giuridico, che abbia ad oggetto tutti i tipi di prova, che vada a sostituire gli strumenti preesistenti e sia basato sul principio del mutuo riconoscimento, pur tenendo conto della flessibilità dei meccanismi di mutua assistenza.[224] Nel 2009, entra infatti in vigore il Trattato di Lisbona, che introduce importanti cambiamenti in materia di cooperazione giudiziaria penale. Sulla base dell'Art. 82(1)(a) TFUE, in risposta all'invito del Consiglio europeo, viene adottata nel 2014 una Direttiva che introduce lo strumento dell'Ordine Europeo di Indagine ("**DOEI**"),[225] la quale per la prima volta offre una soluzione onnicomprensiva per la raccolta transfrontaliera di prove nell'ambito dello

[221] Ibid.
[222] Marcello Daniele, 'Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles' (2015) 6(2) New Journal of European Criminal Law 179, 180.
[223] Silvia Allegrezza, 'Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality' in Stefano Ruggeri (ed), *Transnational Evidence and Multicultural Inquiries in Europe* (Springer 2014) 57.
[224] Council of the European Union, 'The Stockholm Programme – An open and secure Europe serving and protecting the citizens' [2009] 17024/09, 13.
[225] Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale [2014] OJ L 130/1.

SLSG, sostituendo un frammentato e poco efficiente mosaico di strumenti[226] e fornendo invece un unico ordine standardizzato, applicabile ad ogni atto investigativo e probatorio.[227]

Ai sensi dell'art. 1 DOEI, l'Ordine Europeo di Indagine ("**OEI**") "è una decisione giudiziaria emessa o convalidata da un'autorità competente di uno Stato membro (lo Stato di emissione) per compiere uno o più atti di indagine specifici in un altro Stato membro (lo Stato di esecuzione) ai fini di acquisire prove […]". Pertanto, contrariamente al mandato europeo di ricerca delle prove, il fulcro della decisione è l'atto investigativo e non i singoli elementi di prova, essendo l'acquisizione di questi ultimi lo scopo dell'atto.[228] Allo stesso tempo, ciò non preclude che la misura investigativa oggetto dell'OEI si riferisca a prove già in possesso delle autorità competenti. Inoltre, ai sensi dell'art. 4 DOEI, un OEI può essere emesso sia in relazione ad un procedimento penale avviato da un'autorità giudiziaria relativamente a un illecito penale ai sensi del diritto nazionale dello Stato di emissione, che per un procedimento avviato dalle autorità amministrative in relazione a fatti punibili in base al diritto nazionale dello Stato di emissione, nel caso in cui la decisione possa dare comunque luogo a un procedimento davanti ad un giudice competente in materia penale. Non sono pertanto stabilite limitazioni rispetto a determinate fattispecie o categorie di reato, scomparendo, per la prima volta, ogni ulteriore riferimento alla tradizionale condizione della verifica della doppia incriminabilità, caratterizzante gli strumenti internazionali di mutua assistenza in materia penale.[229]

Rispetto alle condizioni per inviare un OEI, l'emissione deve essere necessaria e proporzionata ai fini del procedimento, alla luce dei diritti dell'indagato o imputato. In aggiunta, la misura investigativa indicata nell'ordine deve rispettare il principio di equivalenza, vale dire che la misura può essere ordinata unicamente se sarebbe potuta essere emessa alle stesse condizioni

---

[226] La DOEI ha sostituito la Convenzione europea di assistenza giudiziaria del 1959 e i relativi protocolli, la Convenzione di applicazione dell'accordo di Schengen del 1990, la Convenzione relativa all'assistenza giudiziaria in materia penale dell'Unione del 2000, la decisione-quadro 2003/577 sul sequestro probatorio e la decisione-quadro 2008/978 con riguardo al mandato europeo di ricerca delle prove.

[227]Tuttavia, alcune eccezioni sono previste in materia di atti di indagine: la formazione o la raccolta di prove che avvenga nel contesto delle Squadre Investigative Comuni ("**SIC**") (art. 3 DOEI), le intercettazioni e la trasmissione immediata delle comunicazioni di cui all'art. 18, par. 1, lett. a) e b), della Convenzione di Bruxelles del 29 maggio 2000, e la misura di *cross-border surveillance* prevista Convenzione di applicazione dell'accordo di Schengen (considerando 9 DOEI).

[228] Stanislaw Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161, 169.

[229] Gaetano De Amicis, 'Limiti e prospettive del mandato europeo di ricerca della prova' (2011) Diritto penale contemporaneo, 32.

in un caso domestico analogo.[230] Quest'ultima condizione rappresenta un'importante novità in quanto impedisce il *forum shopping* da parte delle autorità investigative e giudiziarie, impedendo loro di emettere un OEI per aggirare i limiti imposti dal diritto nazionale.[231] Tuttavia, questa salvaguardia non è equivalente alle condizioni stabilite dall'art. 8(2) CEDU, secondo il quale qualsiasi interferenza con il diritto al rispetto ad una vita privata e familiare da parte delle autorità pubbliche deve essere prevista dalla legge, in modo da offrire garanzie adeguate ed efficaci contro possibili abusi. Sotto questo profilo, l'inclusione di tale requisito procedurale, derivante dalla CEDU, sarebbe stata particolarmente rilevante nel contesto dell'OEI, in quanto, a causa del suo ampio campo di applicazione, la DOEI copre misure investigative che spesso non trovano una base legale adeguata nel diritto nazionale.[232] In ogni caso, qualora lo Stato di esecuzione ritegna che le suddette condizioni non siano rispettate potrà aprire delle consultazioni con lo Stato emittente, all'esito delle quali quest'ultimo potrebbe decidere di ritirare l'OEI.[233]

Una volta verificato però il rispetto delle condizioni, il riconoscimento e l'esecuzione dell'OEI devono avvenire senza imporre ulteriori formalità, fatta salva l'opposizione dei motivi di non riconoscimento o di non esecuzione tassativamente elencati all'art. 11 DOEI. In particolare, l'esecuzione delle misure investigative segue la regola, formulata all'art. 9(2) DOEI, del *forum regit actum*, che prevede che l'autorità di esecuzione si attenga "alle formalità e alle procedure espressamente indicate dall'autorità di emissione, salvo qualora la presente direttiva disponga altrimenti". Tuttavia, viene previsto un limite alla regola del *forum regit actum*, rappresentato dalla possibilità che tali formalità e procedure siano in conflitto con i principi fondamentali del diritto dello Stato di esecuzione.

Rispetto all'accesso alle prove digitali, la DOEI disciplina all'art. 30 la misura investigativa dell'intercettazione sia in relazione al contenuto delle comunicazioni che ai relativi metadati. Tuttavia, questo articolo parte dal presupposto che per l'esecuzione del provvedimento sia necessaria l'assistenza di un altro Stato, ovvero lo Stato in cui si trova il soggetto intercettato.[234]

---

[230] Art. 6(1) e (2) DOEI.
[231] Inés Armada, 'The European Investigation Order and the Lack of European Standards for Gathering Evidence. Is a Fundamental Rights-Based Refusal the Solution?' (2015) 6(1) New Journal of European Criminal Law 8, 17.
[232] Ibid, 18.
[233] Art. 6(3) DOEI.
[234] Nathalie A. Smuha, 'Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency' (2018) 8(1) European Criminal Law Review 83, 93.

Il lungo lasso di tempo generalmente applicabile di 30 giorni per lo Stato che riceve l'OEI per decidere sulla sua esecuzione, e il lasso di tempo di 90 giorni per questo Stato per eseguire l'OEI, rimangono in vigore. Inoltre, data l'invasività del provvedimento, è previsto un ulteriore motivo per non eseguire l'ordine oltre ai generali motivi di rifiuto elencati all'art. 11 DOEI: all'art. 30(5) DOEI, viene stabilito che l'esecuzione di un OEI che richiede l'intercettazione di telecomunicazioni può essere rifiutata anche quando la misura non sarebbe stata autorizzata in un caso nazionale analogo.

Qualora l'indirizzo di comunicazione della persona intercettata indicata nell'Ordine è utilizzato sul territorio di un altro Stato membro (Stato membro notificato) ma non sia necessaria l'assistenza tecnica di quest'ultimo per effettuare l'intercettazione, viene previsto all'art. 31 che lo Stato membro interessato ad effettuare l'intercettazione deve comunque notificare l'autorità competente dello Stato membro notificato. La notifica può essere preventiva, contestuale o postuma all'intercettazione a seconda di quando l'autorità competente venga a conoscenza del fatto che la persona soggetta a intercettazione si trova, o si trovava durante l'intercettazione, sul territorio dello Stato membro notificato. Rispetto invece al diritto del soggetto intercettato di essere notificato, nel silenzio della DOEI, la disciplina viene governata dal diritto nazionale. Occorre inoltre ribadire che tale meccanismo si applica solo all'intercettazione delle telecomunicazioni, mentre è escluso l'accesso alle prove memorizzate. Per quest'ultimo tipo di dati, gli Stati devono emettere un OEI preventivo, a cui si applicano i limiti di tempo sopra menzionati.

Dunque, sebbene la procedura dell'OEI abbia certamente dei meriti nel facilitare lo scambio di prove e l'esecuzione di misure investigative in situazioni transfrontaliere, non fornisce un quadro completo per la raccolta di prove elettroniche ed è ben lungi dall'essere adatta al rapido ritmo del mondo digitale.[235]

2.2. La proposta di un "*e-evidence package*": la risposta dell'UE alle nuove sfide della prova digitale

Alla luce delle menzionate lacune normative, trascorso poco meno di un anno dalla scadenza del termine per l'attuazione della DOEI e nonostante le misure di indagini informatiche e le

[235] Ibid, 93.

prove digitali rientrassero nello scopo di applicazione di quest'ultima, nell'aprile 2018, la Commissione decide di proporre un nuovo pacchetto legislativo, il c.d. "*e-evidence package*" composto da un Regolamento e da una Direttiva, volto a creare un quadro giuridico *ad hoc* per l'acquisizione e la conservazione *cross-border* delle prove digitali.[236]

La decisione della Commissione di proporre un nuovo pacchetto legislativo dedicato interamente all'accesso *cross-border* alla prova digitale può infatti essere interpretata come una risposta dell'UE agli attacchi terroristici di Bruxelles del 2016.[237] A seguito di tali eventi, il Consiglio UE individua come prioritario un intervento legislativo che assicuri di ottenere più rapidamente ed efficacemente le prove digitali, intensificando la cooperazione con i paesi terzi e con i *service providers* operanti nel territorio dell'Unione.[238] D'altra parte se da un lato, ad oggi, più di due terzi delle indagini penali richiedono la raccolta di prove elettroniche, queste ultime differiscono in modo significativo dalle altre tipologie di prove, rendendo l'allora attuale quadro giuridico, basato sui tradizionali concetti di territorialità e giurisdizione, estremamente poco efficiente per le autorità competenti degli Stati membri.[239]

In particolare, le prove digitali vengono spesso conservate su server di proprietà dei c.d. *service providers*. L'elemento transfrontaliero deriva dunque dal fatto che i principali attori appartenenti a quest'ultima categoria sono spesso società straniere, si pensi ad esempio a *Google* e *Microsoft,* i cui dati possono venire poi gestiti da filiali con sede nei territori dell'Unione.[240] Allo stesso tempo, le indagini e i procedimenti giudiziari sono tuttavia limitati dai confini nazionali e uscire da questi ultimi comporta l'utilizzo di strumenti di cooperazione internazionale o comunitaria.[241] Sotto questo profilo, se l'OEI può servire ad acquisire prove

---

[236] 'Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale' COM(2018) 225 final; 'Proposta di Direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali' COM(2018) 226 final.

[237] Mitja Gialuz e Jacopo Della Torre, 'Lotta alla Criminalità nel Cyberspazio: la Commissione presenta due Proposte per facilitare la Circolazione delle Prove Elettroniche nei Processi Penali' (2018) 5 Diritto Penale Contemporaneo 277, 278.

[238] Consiglio dell'Unione Europea, 'Dichiarazione comune dei ministri della giustizia e degli interni dell'UE e dei rappresentanti delle istituzioni dell'UE sugli attentati terroristici di Bruxelles del 22 marzo 201' (24 marzo 2016) <https://www.consilium.europa.eu/it/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/> ultimo accesso 29 settembre 2023.

[239] Stanislaw Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161, 168.

[240] Ibid.

[241] Commission Staff Working Document, Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for

elettroniche in contesti *cross-border*, le sue scadenze sono eccessivamente lunghe, imponendo un obbligatorio passaggio di collaborazione con le autorità pubbliche, e creando dunque il rischio che i dati vengano, nell'attesa, cancellati o alterati.[242] Allo stesso tempo nessuna soluzione viene offerta per risolvere la questione della territorialità. Se infatti la DOEI si pone l'obiettivo di raccogliere prove sfruttando il principio del muto riconoscimento degli ordini di altri Stati membri, la componente transfrontaliera caratterizzante la prova digitale è differente. Se la necessità di introdurre nell'ordinamento dell'Unione uno strumento come l'OEI deriva dalla libera circolazione delle persone e dall'abolizione delle frontiere, gli ostacoli posti dalla raccolta della prova digitale risiedono nella mancanza di frontiere nel cyberspazio.[243] Non è la popolazione a spostarsi, ma i servizi ad essere collocati in altri Paesi rispetto ai loro utenti.[244] A titolo esemplificativo, la prova digitale può aggiungere una dimensione transfrontaliera anche in un caso dal carattere puramente nazionale, solo perché i dati da utilizzare come prove sono in possesso di un *service provider* di un altro Stato membro.

Per superare questi ostacoli, la polizia e le autorità giudiziarie hanno iniziato a ricorrere alla cooperazione volontaria con i *service providers*.[245] Ciò permetteva non solo di ovviare all'eccessiva lunghezza delle tempistiche e al problema del criterio territoriale, ma occorre sottolineare anche come un rapporto collaborativo con i *service providers* fornisse un vantaggio pratico alle autorità investigative e giudiziarie non trascurabile. Se le autorità competenti dispongono solitamente dei poteri necessari per compiere una perquisizione in un'azienda che si rifiuta di produrre dei documenti richiesti, adottare la stessa strategia in un centro dati di proprietà di un *server provider* non disposto a collaborare comporterebbe un impiego di ingenti risorse tecniche ed economiche, nonché un dispiego di misure altamente intrusive e spesso sproporzionate rispetto alla necessità di trovare i dati ricercati.[246]

---

electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' SWD(2018) 118 final, 19.

[242] Ibid, 23.

[243] Stanislaw Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161, 177.

[244] Ibid.

[245] Teresa Quintel e Mark D Cole, 'Transborder Access to e-Evidence by Law Enforcement Agencies. A first comparative view on the Commission's Proposal for a Regulation on a European Preservation/Production Order and accompanying Directive' (2018) University of Luxembourg Law Working Paper 1, 2.

[246] Stanislaw Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161, 168.

Alla luce di tali eventi storico-politici e delle difficoltà pratiche riscontrate dalle autorità investigative e giudiziarie nazionali, nelle sue Conclusioni sul miglioramento della giustizia penale nel cyberspazio, adottate il 9 giugno 2016, il Consiglio invita la Commissione a intraprendere azioni concrete basate su un approccio comune dell'UE al fine di (i) migliorare la cooperazione con i fornitori di servizi, (ii) rendere più efficiente l'assistenza giudiziaria reciproca e (iii) proporre soluzioni ai problemi di determinazione e applicazione della giurisdizione nel cyberspazio.[247] Per individuare le strategie più efficienti per raggiungere tali obiettivi, i servizi della Commissione hanno organizzato una serie di incontri bilaterali: con le autorità nazionali competenti, con organizzazioni internazionali come il Consiglio d'Europa e l'Interpol, ma anche con diversi *service providers* e rappresentanti di organizzazioni per i diritti civili.[248]

In particolare, rispetto ai meccanismi di cooperazione diretta e volontaria con i *service providers*, la Commissione ha identificato una serie di ostacoli per entrambe le parti coinvolte.

In primo luogo, le autorità nazionali competenti riscontravano difficoltà nell'identificare e contattare i *service providers* in grado di fornire i dati relativi. Sebbene la maggior parte dei fornitori offra un punto di contatto speciale per ricevere richieste ufficiali, questi punti di contatto possono essere istituiti a livello nazionale, regionale, o addirittura coincidere direttamente con la sede centrale dell'azienda, che potrebbe essere situata ovunque nel mondo.[249] In secondo luogo, una volta stabilito il punto di contatto, rimane comunque complesso formulare, in assenza di un canale di comunicazione prestabilito, una richiesta, dovendo la polizia e le autorità giudiziarie adattarsi all'approccio adottato da ogni singola azienda.[250] Infine, anche qualora tale richiesta venga inviata con successo, viene lamentata una mancanza di trasparenza e una conseguente incertezza giuridica in relazione alle procedure aziendali che determinano la decisione finale dei *service providers*, i quali, dal momento che la

[247] Council of the European Union, 'Conclusions of the Council of the European Union on improving criminal justice in cyberspace,' (9 giugno 2016) <https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf> ultimo accesso 29 settembre 2023.
[248] Council of the European Union, 'Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2 December 2016, 15072/16; Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward (22 maggio 2017) <https://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf> ultimo accesso 29 settembre 2023, 2.
[249] Ibid, 8.
[250] Ibid.

cooperazione avviene su base volontaria, non sono titolari di alcun obbligo di rispondere alle richieste e, in caso di rifiuto, di motivare la propria decisione.[251]

D'altra parte, i *service providers* riscontrano una mancanza di risorse adeguate al fine di gestire un'ampia varietà di formati di richiesta e di valutare se tali richieste siano autentiche e conformi al quadro giuridico nazionale dell'autorità richiedente: una cooperazione diretta con i *service providers* stranieri, pur non essendo di per sé *contra legem*, non è solitamente regolata dalla legislazione nazionale. In aggiunta, i *service providers* potrebbero essere titolari di obblighi di notifica degli utenti i cui dati vengono richiesti, al fine di autorizzarne l'accesso.[252] Ciò crea numerose difficoltà per tutte le parti coinvolte, in quanto le varie leggi nazionali e le politiche aziendali prevedono modalità ed eccezioni diverse per la notifica agli utenti.

2.3. Gli Ordini di Produzione e Conservazione Europei: un nuovo "mutuo riconoscimento" e la cooperazione diretta con i *service providers*

Alla luce di tali considerazioni, la Commissione decide di proporre un quadro giuridico che regoli i meccanismi di cooperazione diretta tra autorità nazionali competenti e *service providers*, al fine di stabilire un processo rapido ed efficiente in cui sia garantita maggiore certezza giuridica e venga ridotto il rischio di conflitti di leggi all'interno dell'UE.

Come misura principale, viene proposta l'adozione di un Regolamento che istituisca un meccanismo di cooperazione tra autorità nazionali competenti e *services providers* attraverso l'emissione di ordini europei di produzione e di conservazione.[253] La proposta della Commissione modifica il paradigma della cooperazione giudiziaria penale, introducendo la possibilità di un rapporto diretto tra l'autorità giudiziaria di uno Stato membro con il *service provider* di un altro Stato membro, senza che sia necessario un controllo *ex ante* o un coinvolgimento da parte delle autorità dello Stato membro del *service provider*, se non *ex post* e solo in determinati casi.[254] La scelta della Commissione per la base giuridica ricade sull'Art.

---

[251] Ibid, 7.
[252] Ibid.
[253] 'Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale' COM(2018) 225 final.
[254] Oscar Calavita, 'La Proposta di Regolamento sugli Ordini di Produzione e Conservazione Europei: Commissione, Consiglio e Parlamento a Confronto' (2021) La Legislazione Penale 1, 6.

82(1) TFUE. Come sottolineato da dottrina sovranazionale e domestica,[255] sono stati sollevati dubbi in merito a tale decisione, che hanno messo in discussione l'adeguatezza dell'Art. 82(1) TFUE a regolare il mutuo riconoscimento anche tra autorità giudiziarie e il settore privato. A sostegno della scelta della Commissione, deve essere tenuto in considerazione che, da una parte, un simile approccio non è una novità assoluta nello SLSG: già da tempo le decisioni giudiziarie in materia civile possono essere eseguite direttamente dalle parti private senza l'intervento delle autorità pubbliche dello Stato membro in cui avviene l'esecuzione.[256] Dall'altra, si potrebbe argomentare che il regolamento costituisca esso stesso il fondamento del reciproco riconoscimento, a prescindere da un intervento delle autorità competenti dello Stato membro in cui l'ordine viene eseguito.[257] Infine, l'art. 82(1) TFUE non definisce il concetto di "mutuo riconoscimento", né specifica che esso debba avvenire nell'ambito di un'interazione tra due autorità.[258]

La Commissione giustifica poi la scelta della natura giuridica dell'atto in quanto il regolamento, essendo direttamente applicabile, garantisce chiarezza, certezza giuridica ed evita interpretazioni divergenti tra gli Stati membri, nonché problemi di recepimento riscontrati sia per l'attuazione delle decisioni-quadro che della DOEI.[259]

In aggiunta al Regolamento, viene proposta anche una Direttiva, adottata sulla base degli Artt. 53 e 62 TFEU, al fine di imporre a tutti i *service providers*, compresi coloro che non sono stabiliti nell'UE, ma che offrono servizi nei territori di quest'ultima, di designare un rappresentante legale o uno stabilimento, responsabile della ricezione degli ordini, della loro ottemperanza e applicazione.[260] L'obiettivo è garantire che tutti i *service providers* che operino

---

[255] Si veda, a titolo esemplificativo, Oscar Calavita, 'La Proposta di Regolamento sugli Ordini di Produzione e Conservazione Europei: Commissione, Consiglio e Parlamento a Confronto' (2021) La Legislazione Penale 1, 6; Stanisław Tosza, 'The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?' (2023) 2 EDPL 163, 169.

[256]Vanessa Franssen, 'The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?' (European Law Blog 12 ottobre 2023) <https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/> ultimo accesso 29 settembre 2023.

[257] Ibid.

[258] Stanisław Tosza, 'The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?' (2023) 2 EDPL 163, 169.

[259] 'Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale' COM(2018) 225 final.

[260] 'Proposta di Direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali' COM(2018) 226 final.

nell'UE, indipendentemente da dove siano stabiliti, abbiano gli stessi obblighi per quanto riguarda l'accesso alle prove elettroniche.

La proposta della Commissione è stata oggetto di intensi negoziati tra il Consiglio dell'UE e il Parlamento, i quali hanno introdotto significativi cambiamenti e presentato numerose modifiche rispetto al progetto iniziale. In particolare, il Parlamento ha assegnato la discussione della proposta alla Commissione LIBE (Commissione per le libertà civili, la giustizia e gli affari interni), che ha presentato il 24 ottobre 2019 un progetto di relazione contenente numerosi emendamenti, volti ad intensificare la tutela dei diritti fondamentali di tutte le parti coinvolte.[261] Il Consiglio si è invece riunito da aprile a novembre del 2018, e il risultato di questi incontri è un testo assunto come orientamento generale nella sessione del Consiglio tenuta il 6 e 7 dicembre 2018.[262]

Delineate le posizioni, dopo cinque anni di complesse trattative, nel gennaio 2023 il Consiglio ha annunciato il raggiungimento di un accordo con il Parlamento e la pubblicazione di un testo di compromesso.[263] Il pacchetto è stato poi adottato e pubblicato a fine luglio.[264] In definitiva, è possibile affermare che le istituzioni dell'UE abbiano accolto in parte l'approccio proposto dal Parlamento e Consiglio, mantenendo un ampio coinvolgimento dello Stato di esecuzione e optando invece per un ruolo molto più limitato dei *service providers*, ridimensionando quindi l'ambiziosa portata innovatrice della proposta della Commissione. Tuttavia, l'attenzione alla protezione dei diritti fondamentali e l'approccio spiccatamente garantista del Parlamento sono stati invece parzialmente ridotti.

2.3.1. Lo scopo materiale del Regolamento: la definizione di *service providers* e di prova digitale

[261] European Parliament, 'Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters'[2020] <https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html#_section1> ultimo accesso 29 settembre 2023 ("**Relazione**").

[262] Council of the European Union, 'Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - general approach' [2019] 2018/0108(COD) ("**orientamento generale**").

[263] Il testo di compromesso è disponibile al seguente link <https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf> ultimo accesso 29 settembre 2023.

[264] L'analisi in seguito svolta ha ad oggetto il testo di compromesso adottato a gennaio 2023. Rispetto al testo del Regolamento e della Direttiva pubblicati in Gazzetta Ufficiale a fine luglio, non si riscontrano sostanziali divergenze.

La Proposta della Commissione attribuisce un ruolo essenziale ai *service providers*, che salvo casi patologici previsti dalla stessa Proposta, sostituiscono nell'acquisizione e conservazione delle prove digitali *cross-border* il ruolo tradizionalmente attribuito in materia di cooperazione giudiziaria alle autorità nazionali competenti dello Stato di esecuzione che nella proposta diventa infatti "*enforcing State*".[265] A questo proposito, la scelta circa quali operatori far rientrare, ai fini della Proposta, nella categoria di *service providers*, merita un'attenta analisi. A differenza della Convenzione di Budapest, che prevede una definizione piuttosto ampia della nozione di "*service providers*" (art. 1(c) Convenzione di Budapest), la Proposta definisce la prova elettronica attraverso la sua appartenenza a specifiche sottocategorie.[266] Non è dunque consentito alle autorità dello Stato membro di emissione di cooperare con tutti i *service providers* di altri Stati membri indiscriminatamente, ma i destinatari vengono circoscritti ad alcune categorie. L'art. 2(3) della Proposta definisce un *service provider* come una persona fisica o giuridica che fornisce determinate categorie di servizi. In particolare, vi rientrano i *service providers* che offrono: (i) servizi di comunicazione elettronica come definiti dalla direttiva che istituisce il codice europeo delle comunicazioni elettroniche,[267] tra cui rientrano, a titolo esemplificativo, la messagistica istantanea o i servizi di posta elettronica; (ii) servizi della società dell'informazione, per i quali la conservazione dei dati è una componente propria del servizio fornito all'utente, tra cui i social network, i mercati online che agevolano le operazioni tra utenti e altri prestatori di servizi di hosting; (iii) servizi di nomi di dominio internet e di numerazione IP, quali i prestatori di indirizzi IP, i registri di nomi di dominio, i registrar di nomi di dominio e i connessi servizi per la privacy o proxy. Questi ultimi vengono compresi nella Proposta dal momento che "possono essere rilevanti per i procedimenti penali in quanto possono fornire indizi che permettono di identificare persone o entità coinvolti in attività criminali."[268]

---

[265] Tale sfumatura si perde in una traduzione italiana dal momento che sia "*executing State*" che "*enforcing State*" vengono tradotti come "Stato di esecuzione".

[266] Vanessa Franssen, 'The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?' (European Law Blog, 12 ottobre 2018) <https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/> ultimo accesso 29 settembre 2023.

[267] Direttiva (UE) 2018/1972 del Parlamento Europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche [2018] OJ L 321/36.

[268] 'Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale' COM(2018) 225 final, 15.

Non rientrano, invece, nello scopo di applicazione della Proposta i servizi della società dell'informazione per i quali "la conservazione dei dati non è una componente principale del servizio fornito all'utente bensì un elemento puramente accessorio, quali i servizi giuridici, architettonici, ingegneristici e contabili forniti online o a distanza".[269] Questa eccezione finale sembra essere una corretta applicazione del principio di proporzionalità, considerando da una parte la sensibilità di determinati argomenti e dati trattati durante suddette attività professionali e, dall'altra, l'onere eccessivo che ricadrebbe su soggetti per i quali la conservazione dei dati non rientra nelle attività principali.[270]

Definite le categorie rilevanti, l'art. 2 prosegue al paragrafo 4 stabilendo un ulteriore condizione affinché i *service providers* rientrino nello scopo di applicazione del Regolamento, vale a dire questi devono offrire alle persone fisiche o giuridiche di uno o più Stati membri uno più servizi delle categorie indicate al paragrafo precedente e, in aggiunta, avere un "collegamento sostanziale" con l'Unione. Qualora il *service provider* non abbia uno stabilimento nel territorio di quest'ultima, ai sensi del considerando 28, "il collegamento sostanziale dovrebbe essere valutato sulla base dell'esistenza di un numero significativo di utenti in uno o più Stati membri, o dell'orientamento delle attività verso uno o più Stati membri". Quest'ultimo può essere valutato tenendo conto di una serie disparata di circostanze come la disponibilità di un'applicazione nell'apposito negozio *online* nazionale, la fornitura di pubblicità a livello locale o nella lingua usata nello Stato membro in questione e così via.[271] Sotto questo profilo, occorre sottolineare come il Regolamento produca importanti effetti extraterritoriali, con un impatto su un numero significativo di attori internazionali situati al di fuori dell'UE. Tuttavia, il criterio legato all'offerta sul territorio piuttosto che alla presenza di uno stabilimento da parte del *service provider* era già stato introdotto dalla Convenzione di Budapest all'art. 18(1)(b), ma solo per la produzione di dati sugli abbonati.

Rispetto alla definizione di *service provider* proposta dalla Commissione, viene precisato dall'orientamento generale adottato dal Consiglio che il Regolamento dovrebbe essere applicabile ai *service provider* che offrono la possibilità agli utenti di comunicare tra loro oppure che trattano dati per conto degli utenti, escludendo dunque dal novero dei *service*

---

[269] Ibid.
[270] Oscar Calavita, 'La Proposta di Regolamento sugli Ordini di Produzione e Conservazione Europei: Commissione, Consiglio e Parlamento a Confronto' (2021) La Legislazione Penale 1, 11.
[271] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale' COM(2018) 225 final, 16.

providers: (i) coloro che offrono servizi finanziari,[272] (ii) coloro che offrono la possibilità agli utenti di comunicare esclusivamente con il *provider* ma non tra di loro, (iii) coloro che non offrono la possibilità di tracciare o conservare dati o quando questi ultimi servizi non sono parte essenziale rispetto all'attività svolta.

La definizione di *service provider,* come proposta dalla Commissione e ristretta dal Consiglio, è stata adottata all'Art. 2(3) dal testo di compromesso adottato a gennaio 2023.

Rispetto alla nozione di "prova elettronica", la Proposta della Commissione fornisce una definizione indiretta finalizzata a definire le misure investigative oggetto del Regolamento, più che a delineare che cosa costituisca una prova digitale.[273] In particolare, gli ordini possono avere ad oggetto qualsiasi prova in formato elettronico conservata dal *service provider* o per suo conto al momento della ricezione del certificato di ordine europeo di produzione o di conservazione, se rientrante nelle categorie di dati relativi agli abbonati, agli accessi, alle operazioni o al contenuto,[274] per le quali viene previsto un diverso livello di protezione sulla base del diverso grado di interferenza dei vari provvedimenti.

Tuttavia, al di là della classificazione dei dati in categorie, la definizione di "prova elettronica" merita attenzione anche da un'altra prospettiva. Secondo quanto espressamente proposto dalla Commissione e confermato nel testo dii compromesso (considerando 19a), le relative prescrizioni si estendono anche ai dati criptati. Evidente è la rilevanza di tali previsioni quando vengano in considerazione applicazioni, quali *WhatsApp* o *Skype*, che utilizzino tecniche di questo genere al fine di ostacolare l'accesso ai dati.[275] Allo stesso tempo, l'applicazione del regolamento non pregiudica l'uso della criptografia da parte dei *service providers* o dei loro utenti, non stabilendo il regolamento alcun obbligo per i prestatori di servizi di decriptare i dati.

In aggiunta, l'ambito di applicazione materiale è limitato ai dati conservati, vale a dire a dati detenuti dal *service providers* al momento della ricezione di un certificato di ordine europeo di produzione o di conservazione.[276] In base alla proposta di Regolamento, l'autorità nazionale

---

[272] Così come definiti all'art. 2(2)(b) Direttiva 2006/123/CE del Parlamento Europeo e del Consiglio del 12 dicembre 2006 relativa ai servizi nel mercato interno [2006] OJ L 376/36.
[273] Stanislaw Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161, 171.
[274] Art. 2(6) Proposta.
[275]Veronica Tondi, 'Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione' (2019) 2 Diritto Penale Contemporaneo Rivista Trimestrale 439, 449.
[276] Art. 2(6) Proposta.

non ha il potere di richiedere al *service provider* la produzione o la conservazione di dati registrati in un momento successivo all'ordine ricevuto.[277] Ciò limita l'utilità dello strumento non rendendo possibile, *inter alia*, richiedere ai *service providers* la conservazione e l'accesso *pro futuro* a dati sul traffico e sulla locazione, ad oggi preziosa risorsa probatoria per la polizia e le autorità giudiziarie.[278] Inoltre, alla luce del complesso dialogo tra la Corte di Giustizia e gli Stati membri in materia di *data retention*, analizzato in seguito, la scelta di escludere tale materia dallo scopo di applicazione della Proposta, e poi anche del testo di compromesso, è piuttosto sorprendente.[279] Allo stesso tempo, rimane dubbio se la tradizionale distinzione tra la raccolta di dati in tempo reale e la raccolta di dati memorizzati sia ancora così rilevante nell'era digitale, in quanto per alcuni tipi di dati, come ad esempio per la messagistica istantanea, non è sempre chiaro se siano dati "in trasmissione" o già "memorizzati".[280] Da ultimo, si osserva che la conservazione di dati ancora inesistenti o l'intercettazione di flussi telematici o informatici interferiscono con la sfera individuale con un grado di intrusività molto più elevato rispetto al diritto ad una vita privata garantito dall'Art. 7 Carta di Nizza.[281] Dunque, alla luce di un'assente doppia tutela giurisdizionale nello Stato di emissione e in quello di esecuzione caratterizzante il modello di cooperazione in esame, la scelta di limitare l'applicazione ai soli dati già acquisiti è coerente con lo scopo della proposta di Regolamento.[282]

Se l'orientamento generale del Consiglio non apporta significative modifiche a tale definizione, il testo presentato dalla Relazione del Parlamento, in primo luogo, sostituisce il termine "prove elettroniche" con "informazioni elettroniche".[283] Quest'ultima scelta è dovuta al fatto che se la proposta della Commissione tratta tutte le informazioni a cui si accede in base alla nuova legge come se fossero prove ammissibili, ciò a cui le autorità accedono effettivamente sono i dati delle persone e solo una parte di questi dati è probabilmente rilevante per i procedimenti penali

---

[277] Raffaella Pezzuto, 'Accesso Transnazionale alla Prova Elettronica mel Procedimento Penale: la Nuova Iniziativa Legislativa della Commissione Europea al Vaglio del Consiglio dell'Unione' (2019) 1 Diritto Penale Contemporaneo 57, 72.
[278] Vanessa Franssen, 'The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?' (European Law Blog 12 ottobre 2018) <https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/> ultimo accesso 29 settembre 2023.
[279] Ibid.
[280] Ibid.
[281] 'Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale' COM(2018) 225 final, 7.
[282] Oscar Calavita, 'La Proposta di Regolamento sugli Ordini di Produzione e Conservazione Europei: Commissione, Consiglio e Parlamento a Confronto' (2021) La Legislazione Penale 1, 9.
[283] Art. 2(6) Relazione.

in corso.[284] In secondo luogo, la categoria dei "dati sul traffico" sostituiscono le precedenti categorie di dati "di accesso" e "sulle operazioni",[285] che si sovrapponevano nella Proposta della Commissione.

Nel testo di compromesso se da una parte viene preferito il termine proposto dalla Commissione di "prova elettronica", dall'altra, viene adottata la diversa classificazione di dati proposta dal Parlamento, che risulta, *inter alia*, anche più in linea con quella in uso nella giurisdizione dell'Unione, in particolare in materia di *data retention*. Le categorie di dati previste all'art. 2(6) sono: dati sugli abbonati,[286] sul traffico[287] e di contenuto[288]. Viene poi specificato all'art. 2(8) che per "dati richiesti al solo scopo di identificare l'utente" si intendono gli indirizzi IP e, se necessario, le relative *source ports* e *time stamp* (data/ora), o gli equivalenti tecnici di tali identificatori e le informazioni correlate, se richieste dalle autorità competenti con l'unico scopo di identificare l'utente nell'ambito di una specifica indagine penale. Per questa tipologia di dati, che può includere sia dati sugli abbonati che dati sul traffico, viene garantito dal testo di compresso il medesimo livello di protezione previsto per i dati sugli abbonati.

Rispetto ai procedimenti rientranti nello scopo di applicazione del Regolamento, la Proposta della Commissione prevedeva che tali ordini potessero essere emessi esclusivamente nell'ambito di un procedimento penale, il cui arco temporale comprende la fase preprocessuale delle indagini preliminari fino alla chiusura del procedimento con sentenza o altra decisione. Tale scopo di applicazione materiale è stato poi ampliato dall'orientamento generale del Consiglio e tale modifica viene mantenuta nel testo di compromesso. Ai sensi dell'art. 3(2) testo di compromesso, gli ordini possono essere emessi non solo nel corso di un procedimento

---

[284] 'E-Evidence compromise blows a hole in fundamental rights safeguards' (EDRi7 febbraio 2023) <https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/> ultimo accesso 29 settembre 2023.

[285] Art. 2(8) Relazione.

[286] Ai sensi dell'art. 2(7) testo di compromesso, per "dati dell'abbonato" si intende qualsiasi dato in possesso di un fornitore di servizi relativo all'abbonamento ai servizi, relativi a: (a) l'identità di un abbonato o di un cliente, come il nome, la data di nascita, l'indirizzo postale o geografico, i dati di fatturazione e di pagamento, il numero di telefono o l'indirizzo e-mail o indirizzo geografico, dati di fatturazione e pagamento, numero di telefono o indirizzo e-mail; (b) il tipo di servizio e la sua durata, compresi i dati tecnici e i dati che identificano le misure tecniche o le interfacce correlate utilizzate o fornite all'abbonato o al cliente al momento della i registrazione o dell'attivazione iniziali, e i dati relativi alla convalida dell'uso del servizio, ad esclusione delle password o di altri mezzi di autenticazione utilizzati al posto di una password forniti da un utente o creati su richiesta di un utente.

[287] Ai sensi dell'art. 2(9) testo di compromesso, per "dati sul traffico" si intende qualsiasi dato relativo alla fornitura di un servizio offerto da un fornitore di servizi che servono a fornire informazioni di contesto o aggiuntive su tale servizio e sono generati o processati da un elaborato da un sistema informativo del fornitore di servizi.

[288] Ai sensi dell'art. 2(10) testo di compromesso, per "dati sul contenuto" qualsiasi dato in formato digitale, come testo, voce, video, immagini e suoni, diversi dai dati degli abbonati o del traffico.

penale ma anche per l'esecuzione di pene detentive o di ordini di custodia cautelare non pronunciati in contumacia, nel caso in cui il condannato si sia sottratto alla giustizia. Come sottolineato dal considerando (24b), se il Regolamento dovrebbe applicarsi ai procedimenti avviati dall'autorità di emissione per localizzare un condannato che si è sottratto alla giustizia per eseguire pene detentive o ordini di custodia, qualora la sentenza o la misura di custodia cautelare sia stata pronunciata in contumacia, non dovrebbe essere possibile emettere gli ordini di produzione o conservazione, dal momento che le legislazioni nazionali degli Stati membri in materia di sentenze in contumacia variano notevolmente in tutta l'UE.

2.3.2. Il rapporto con altri strumenti di cooperazione

Il Regolamento si applica alla raccolta di prove elettroniche, vale a dire a qualsiasi dato sugli abbonati, sul traffico o sul contenuto che, al momento della ricezione dell'ordine, sia immagazzinato in formato elettronico da o per conto di un *service provider*, che offre servizi nell'Unione.[289] Tuttavia, la sussistenza di una serie di diverse condizioni potrebbe comportare la non applicazione del Regolamento anche qualora vengano raccolte prove elettroniche, lasciando spazio all'OEI o anche, in un numero minore di casi, ad altri strumenti di cooperazione.

Dal punto di vista dello scopo di applicazione territoriale, due Stati membri hanno una partecipazione limitata nello SLSG, ossia Danimarca e Irlanda. Se l'Irlanda non fa parte dell'OEI, ha invece deciso di aderire al Regolamento.[290] Ciò comporta una serie di conseguenze significative. Se la raccolta di prove elettroniche, nelle condizioni sopra delineate, ricadrebbe nello scopo di applicazione del Regolamento, l'acquisizione *cross-border* delle altre tipologie di prove, continuerà ad essere disciplinata attraverso i mezzi offerti dalla Convenzione di Mutua Assistenza del 1959 del Consiglio d'Europa, dal momento che l'Irlanda non fa nemmeno parte della Convenzione dell'UE del 2000. Allo stesso tempo, la scelta di partecipazione dell'Irlanda è di fondamentale importante alla luce degli obiettivi del Regolamento, in quanto questo Stato membro è sede in Europa di diversi *service providers*. Diversamente la Danimarca non avendo aderito né alla DOEI, né dal Regolamento, rimane vincolata, per tutte le tipologie di prova, alla Convenzione dell'UE di mutua assistenza del 2000.[291] Occorre tuttavia sottolineare che sebbene

[289] Art. 2(6) testo di compromesso.
[290] Vedi considerando 64 testo di compromesso.
[291] Vedi considerando 65 testo di compromesso.

la Danimarca non faccia parte del Regolamento, farà comunque automaticamente parte della Direttiva, che basandosi sulle disposizioni del mercato comune di cui agli articoli 53 e 62 del TFUE, non permette l'applicazione delle condizioni di *opt in/opt out* previste dal Protocollo n.22.

Rispetto allo scopo di applicazione materiale, diversamente dall'attuale testo del Regolamento, lo scopo di applicazione della DOEI comprende oltre ai procedimenti penale anche a procedimenti avviati dalle autorità amministrative purché la decisione possa dar luogo a un procedimento davanti a un organo giurisdizionale penale e ai procedimenti avviati dalle autorità giudiziarie quando la decisione può dar luogo a un procedimento davanti a un organo giurisdizionale penale. In aggiunta, l'OEI può essere emesso anche in connessione con i suddetti procedimenti relativi a reati o violazioni per i quali una persona giuridica può essere considerata responsabile o punita nello Stato di emissione. Inoltre, come ribadito, viene esplicitamente esclusa dallo scopo di applicazione del Regolamento, ma è inclusa in quello della DOEI, la raccolta in tempo reale di dati, dal momento che gli ordini possono avere ad oggetto solo dati già conservati presso il *provider* al momento dell'emissione dell'ordine. Dunque, l'obbligo di conservazione dei dati e le intercettazioni in tempo reale del traffico informatico o telematico potrebbero essere comunque richiesti per mezzo di un OEI, il quale, a differenza degli ordini di produzione e conservazione, garantisce il citato doppio vaglio giurisdizionale dello Stato di emissione e di esecuzione.

2.3.3. Le condizioni di emissione

Per Ordine di produzione europeo s'intende una decisione vincolante di un'autorità di uno Stato membro che ordina ad un *service provider* che offre servizi nell'Unione ed è stabilito o rappresentato in un altro Stato membro di produrre prove elettroniche. Questo contiene una serie di informazioni dalla la categoria di dati richiesti e se del caso, l'intervallo di tempo per il quale è richiesta la produzione, ai motivi della necessità e della proporzionalità della misura.[292] L'ordine di conservazione europeo consiste invece in una decisione con la medesima natura e caratteristiche dell'ordine di produzione, ma avente ad oggetto la richiesta di conservazione delle prove elettroniche per impedire la rimozione, la cancellazione o la modifica di dati in vista

[292] Art. 1(1) testo di compromesso.

di una successiva richiesta di produzione, tramite i canali di assistenza giudiziaria in caso di paesi terzi o attraverso un OEI o un ordine di produzione.[293]

Gli ordini sono rivolti direttamente allo stabilimento previsto o al rappresentante legale designato dal *service provider* ai fini dell'acquisizione delle prove nei relativi procedimenti nazionali, ai sensi della Direttiva proposta nel pacchetto.[294] In via eccezionale, nei casi di emergenza come delineati dal Regolamento, se lo stabilimento o il rappresentante non ottemperano all'ordine di produzione entro le scadenze previste, l'ordine può essere rivolto a qualsiasi stabilimento o rappresentante legale del *service provider* nell'Unione.[295]

Rispetto alle condizioni di emissione degli ordini, la Proposta della Commissione aveva previsto, in primo luogo, che questi potessero essere emessi solo se necessario e proporzionato al caso di specie. In aggiunta a questo requisito, in un'ottica garantista, la relazione del Parlamento aveva previsto anche un compendio probatorio minimo ai fini dell'emissione dell'ordine, con lo scopo di scongiurare il rischio di indagini preventive e meramente conoscitive, sprovviste di un certo livello di sospetto che il reato sia stato commesso.[296] Se il compendio probatorio minimo viene eliminato dal testo di compromesso, la condizione della necessarietà e della proporzionalità vengono mantenuti sia per gli ordini di produzione che di conservazione.[297] Rispetto al requisito in esame, la necessità delle misure deve essere valutata alla luce degli obiettivi da perseguire in una società democratica, come elencati dall'Art. 8(2) CEDU. La proporzionalità, invece, deve leggersi con riferimento allo scopo legittimo perseguito e richiede all'autorità giudiziaria competente di assicurare un giusto equilibrio tra gli interessi pubblici e diritti fondamentali dell'imputato/indagato.

In secondo luogo, come proposto dalla Commissione e confermato nel testo di compromesso, l'ordine di produzione può essere emesso se una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione. È rilevante notare che non viene fatto ricorso al concetto di "doppia criminalità", presupponendo dunque un

[293] Art. 1(2) testo di compromesso.
[294] Art. 7(1) testo di compromesso.
[295] Art. 7(2) testo di compromesso
[296] Oscar Calavita, 'La Proposta di Regolamento sugli Ordini di Produzione e Conservazione Europei: Commissione, Consiglio e Parlamento a Confronto' (2021) La Legislazione Penale 1, 38.
[297] Vedi artt. 5(2) e 6(2) testo di compromesso rispettivamente per l'ordine di produzione e per l'ordine di conservazione.

elevato livello di fiducia nel rispetto dei diritti fondamentali in tutti gli Stati membri.[298] Allo stesso modo, l'ordine di conservazione può essere emesso se avrebbe potuto essere richiesto sotto le medesime condizioni in un simile caso al livello domestico.

Per quanto concerne la previsione di ulteriori condizioni di emissione, gli ordini di conservazione, come confermato dal testo di compromesso all'art. 6, possono essere emessi sia da un giudice che da un pubblico ministero e per qualsiasi tipo di reato. Diversamente, in ragione della loro maggiore afflittività, gli ordini di produzione prevedono condizioni diverse a seconda della categoria di dati oggetto dell'ordine.

Come sottolineato in precedenza, la Proposta della Commissione presentava le seguenti categorie: ii dati relativi agli abbonati, agli accessi, alle operazioni o al contenuto.[299] Da una parte, tali categorie di dati comprendono dati personali e quindi rientrano nell'ambito delle garanzie stabilite dall'*acquis* europeo per il trattamento e la protezione dati personali. Tuttavia, dall'altra, l'impatto sulla tutela dei diritti fondamentali derivante dalla loro acquisizione varia notevolmente a seconda del tipo di dati richiesto.[300] A differenza di quanto stabilito dalla Convenzione di Budapest, vengono quindi previste dalla Proposta condizioni diverse per ottenere i dati relativi agli abbonati e agli accessi da un lato, e i dati relativi alle operazioni e di contenuto dall'altro, alla luce del diverso grado di interferenza delle varie categorie. Per i primi l'ordine di produzione europeo può essere emesso da un pubblico ministero o da un giudice per qualsiasi tipo di reato, indipendentemente dalla sua gravità.[301] Per contro, la produzione di dati relativi alle operazioni e di contenuto richiede l'intervento di un giudice ed è limitata a determinate categorie di reati.

Rispetto alla Proposta della Commissione, l'orientamento generale del Coniglio aggiunge importanti novità. In primo luogo, in relazione al solo ordine di produzione europeo per dati concernenti le operazioni, se la richiesta riguarda una persona non residente nel territorio dello Stato di emissione e sussiste il dubbio che i dati possano essere oggetto di protezione nello Stato di esecuzione, in quanto coperti da immunità, privilegi, norme a tutela della libertà della stampa,

---

[298] Mitja Gialuz e Jacopo Della Torre, 'Lotta alla criminalità nel Cyberspazio: la Commissione presenta due Proposte per facilitare la circolazione delle prove elettroniche nei processi penali' (2018) 5 Diritto Penale Contemporaneo 277, 285.
[299] Art. 2(6) Proposta.
[300] Raffaella Pezzuto, 'Accesso Transnazionale alla Prova Elettronica mel Procedimento Penale: la Nuova Iniziativa Legislativa della Commissione Europea al Vaglio del Consiglio dell'Unione' (2019) 1 Diritto Penale Contemporaneo 57, 72.
[301] Art. 4(1) Proposta in combinato disposto con l'art. 5(3) Proposta.

o che possono minare i diritti fondamentali, la sicurezza e la difesa nazionali, lo Stato di emissione deve cercare di ottenere chiarimenti prima di emettere l'ordine, aprendo eventualmente delle consultazioni anche con lo Stato di esecuzione.[302] Se viene confermato il dubbio, l'autorità di emissione deve tenere conto delle circostanze come se fossero presenti nel proprio diritto interno, evitando di adottare l'ordine o adattandolo alle caratteristiche del caso concreto. Se il potere di revocare il privilegio o l'immunità spetta a un'autorità dello Stato di esecuzione, l'autorità di emissione può chiedere all'autorità di esecuzione di contattare l'autorità competente per chiederle di esercitare immediatamente il suo potere. Se il potere di revocare il privilegio o l'immunità spetta a un'autorità di un altro Stato membro o di un paese terzo o a un'organizzazione internazionale, l'autorità di emissione può chiedere all'autorità interessata di esercitare tale potere.

Rispetto agli ordini di produzione aventi ad oggetto dati relativi al contenuto, all'Art. 7a viene previsto che qualora l'autorità di emissione abbia ragionevoli motivi per ritenere che la persona i cui dati sono ricercati non risieda nel proprio territorio, questa possa trasmette una copia dell'ordine contestualmente sia al *service provider* che all'autorità competente dello Stato di esecuzione. La doppia notifica ha lo scopo di permette all'autorità notificata di informare quanto prima, e comunque non oltre 10 giorni, l'autorità di emissione di qualsiasi circostanza relativa ad un'eventuale presenza di immunità, privilegi o lesioni di diritti e interessi fondamentali o violazione delle norme sulla libertà di stampa, così che l'autorità di emissione possa tenere in considerazione tali circostanze come se fossero previste dal proprio diritto nazionale e valutare se adattare ritirare l'ordine. Se il potere di revocare il privilegio o l'immunità spetta a un'autorità dello Stato di esecuzione o ad un'autorità di un altro Stato membro o di un paese terzo o a un'organizzazione internazionale, l'autorità di emissione può chiedere all'autorità interessata di esercitare tale potere. Al fine di non ritardare il procedimento, la notifica non ha tuttavia effetto sospensivo sugli obblighi derivanti dall'ordine per il *provider*.

Sotto questo profilo, la posizione del Parlamento diverge in modo significativo dalla posizione assunta dalla Commissione e dal Consiglio. La prima propone un ruolo solo marginale delle autorità dello Stato di esecuzione e il Consiglio stabilisce una doppia notifica solo se sussistono le specifiche condizioni previste all'Art. 7a orientamento generale. Diversamente, la relazione del Parlamento propone invece che ai fini dell'acquisizione di informazioni elettroniche nei

[302] Vedi artt. 5(7) e (8) orientamento generale.

procedimenti penali, l'ordine europeo di produzione e l'ordine europeo di conservazione siano rivolti direttamente e simultaneamente non più solo al *service provider* ma anche all'autorità di esecuzione.[303] Tale meccanismo di doppia notifica è con o senza effetto sospensivo a seconda della categoria di dati oggetto dell'ordine. Viene poi previsto che tali ordini siano tramessi attraverso un sistema europeo comune di scambio, creato dalla Commissione, con canali sicuri per la gestione delle comunicazioni transfrontaliere autorizzate, l'autenticazione e la trasmissione degli ordini e dei dati richiesti tra le autorità competenti e i prestatori di servizi.[304]

Come è possibile evincere dal testo di compromesso, se da una parte viene abbondata l'ambiziosa proposta della Commissione, dall'altra non vengono adottate nella loro totalità le novità introdotte dal Parlamento, ridimensionando la necessità di doppia notifica solo ad alcune ipotesi.

Rispetto agli ordini di produzione aventi ad oggetto dati sugli abbonati e per i "dati richiesti al solo scopo di identificare l'utente" possono essere emessi da un giudice o un pubblico ministero e per qualsiasi tipo di reato e per l'esecuzione di pene detentive o di un ordine di custodia cautelare fino a quattro mesi.[305]

Per quanto concerne gli ordini di produzione aventi ad oggetto dati sul traffico, ad esclusione dei "dati richiesti al solo scopo di identificare l'utente", o dati sul contenuto, questi possono essere emessi solo da un giudice e per una serie di reati elencati dal Regolamento.[306] Questi devono inoltre essere notificati non solo al *service provider* ma anche all'autorità dello Stato di esecuzione, a meno che sussistano ragionevoli motivi per credere, al momento dell'emissione, che (i) il reato è stato commesso, sta per essere commesso o è probabile che venga commesso nello Stato di emissione e (ii) la persona di cui si cercano i dati risiede nello Stato di emissione.[307] Tale notifica ha effetto sospensivo a meno che non sussistano delle condizioni di emergenza, come definiti dal Regolamento. Dunque, il *service provider* dovrà aspettare di eseguire l'ordine fino a quando l'autorità di esecuzione non deciderà entro dieci giorni dal

---

[303] Artt. 8a, 9 e 10 Relazione.
[304] Art. 7a Relazione.
[305] Art. 4(1) in combinato disposto con l'art. 5(3) testo di compromesso.
[306] Art. 4(2) in combinato disposto con l'art. 5(4) testo di compromesso. Tali ordini possono essere emessi per reati punibili nello Stato di emissione con una pena detentiva massima di almeno tre anni; per determinate tipologie di reati se commesse in tutto o in parte attraverso un sistema informatico; per alcune fattispecie di reato previste dalla Direttiva sulla lotta contro il terrorismo; per l'esecuzione di una pena detentiva o di ordine di custodia cautelare di almeno quattro mesi inflitta per i suddetti reati.
[307] Art. 7a testo di compromesso.

ricevimento dell'ordine, come analizzato in seguito, di sollevare uno o più dei motivi di rifiuto tassativamente previsti dal Regolamento.

2.3.4. Le modalità di esecuzione e i motivi di rifiuto

Rispetto alle modalità di esecuzione dell'ordine di produzione, ciò che viene fatto circolare è un certificato relativo all'ordine.[308] Una volta che tale certificato sia giunto al rappresentante designato dal *service provider*, questi è tenuto ad eseguire l'ordine secondo delle rigide scansioni temporali stabilite dall'art. 9: ciò deve avvenire, in linea di principio, al più tardi entro dieci giorni da quando la misura è ricevuta. Se è richiesta una doppia notifica ai sensi dell'art. 7a, il s*ervice provider* deve assicurare che i dati siano trasmessi all'autorità di emissione alla fine dei dieci giorni dal ricevuto ordine.

In casi di emergenza il destinatario trasmette i dati richiesti senza indebito ritardo, al più tardi entro otto ore dal ricevimento dell'ordine. Se l'ordine è soggetto a una notifica ai sensi dell0articolo 7a, l'autorità di esecuzione può, senza indugio e al più tardi entro 96 ore dal ricevimento della notifica, notificare all'autorità di emissione e al *provider*, sulla base di uno dei motivi di rifiuto, che si oppone all'utilizzo dei dati o che i dati possono essere utilizzati solo a condizioni da essa specificate. Nei casi in cui l'autorità di esecuzione sollevi un motivo di rifiuto, se i dati sono già stati trasmessi dal destinatario all'autorità di emissione, quest'ultima cancella o limita in altro modo l'uso dei dati o, in caso di condizioni, rispetta tali condizioni nell'utilizzo dei dati.

Rispetto alle modalità esecutive degli ordini di conservazione viene precisato all'Art. 10 che, una volta ricevuto tale certificato, il *service provider* deve, senza indebito ritardo, preservare i dati richiesti. La conservazione dei dati cessa dopo 60 giorni, a meno che l'autorità di emissione confermi che è stata avviata una successiva richiesta di produzione. Il termine di 60 giorni può essere prorogato per un termine aggiuntivo di 30 giorni.

Alla luce di tali modalità esecutive, è chiaro quale sia plus valore offerto dal Regolamento: la possibilità di contrastare la volatilità e fragilità della prova digitale, prevedendo tempi di trasmissione molto stretti. Al contrario, la DOEI, la quale è comunque più rapida rispetto agli strumenti di mutua assistenza giudiziaria con Stati terzi, prevede tempi di consegna del materiale probatorio più lunghi.

---

[308] Art. 8 testo di compromesso.

Circa le modalità di esecuzione occorre infine segnalare un'interessante aggiunta introdotte dal Consiglio, che tuttavia, sorprendentemente, non ha trovato spazio nel testo di compromesso. Rispetto all'esecuzione di ordini di conservazione, viene introdotta un'espressa previsione per mezzo della quale i dati devono essere trasmessi all'autorità di emissione "secondo modalità sicure e affidabili che consentano di stabilire l'autenticità e l'integrità" degli stessi.[309] Una tale modifica prendeva in considerazione la garanzia di affidabilità e inalterabilità dei dati acquisiti, imposta dagli Artt. 16 e 19 Convenzione di Budapest.

L'autorità di esecuzione può decidere di sollevare i motivi di rifiuto, previsti dal Regolamento. Alla luce del carattere vincolante della misura, la Proposta della Commissione prevedeva che qualora il *service provider* ritenesse di non poter adempiere all'ordine di produzione poiché, dalle sole informazioni ivi contenute, risultava che esso contenesse manifeste violazioni della Carta di Nizza o fosse manifestamente arbitrario, il *provider* era tenuto a contattare l'autorità di esecuzione competente del proprio Stato membro.[310] Quest'ultima avrebbe potuto chiedere all'autorità di emissione chiarimenti circa l'ordine, utilizzando anche i canali della Rete giudiziaria europea o dell'Eurojust. Inoltre, la Commissione identificava questa ipotesi come uno dei motivi di rifiuto degli ordini, previsti tassativamente dalla Proposta, che potevano essere presentati dal *provider*.[311]

Dunque, secondo la proposta della Commissione, i *service providers* dovevano assumere la responsabilità di valutare non solo la sussistenza di possibili motivi di rifiuto ma in particolare anche la conformità degli ordini alla Carta, un ruolo che solitamente spetta agli Stati membri e alle istituzioni dell'UE. Tale disposizione è stata tuttavia aspramente criticata da parte sia del Consiglio che del Parlamento e dalle organizzazioni per i diritti civili, ma anche dagli stessi *service providers*, i quali i sono mostrati fin da subito molto riluttanti ad entrare in una valutazione della legalità/diritti fondamentali dell'ordine alla luce di una mancanza di risorse adeguate e dell'assunzione di profili di responsabilità inediti nei confronti della propria clientela.

[309] Art. 9 orientamento generale.
[310] Art. 9(5) Proposta.
[311] Art. 14(4)(f) Proposta.

Non sorprende quindi che sia l'orientamento generale del Consiglio che la relazione del Parlamento, anche se in gradi differenti, si siano mostrati contrari a tale scelta della Commissione.

Rispetto ai motivi di rifiuto proposti dalla Commissione all'Art. 14(4), il Consiglio mantiene la possibilità per il *service provider* di esercitare un elenco tassativo di motivi di rifiuto, eliminando tuttavia dalla lista della Commissione la clausola sui diritti fondamentali. L'eliminazione di tale motivo limita il ruolo del *provider* come custode dei diritti fondamentali, che la versione della Commissione avrebbe voluto invece affidargli. Diversamente, la relazione del Parlamento prevede che solo l'autorità di esecuzione possa rifiutare un ordine, e in particolare solo gli ordini di produzione. Questa può confermare l'ordine o respingerlo sulla base di motivi tassativi indicati dal regolamento al nuovo art. 10 bis al primo paragrafo, a cui se ne aggiungono altri al secondo paragrafo dedicato agli ordini di produzione aventi ad oggetto dati relativi al traffico o al contenuto. Tali motivi sono simili a quelli nella DOEI e concernono soli motivi di legittimità, mentre quelli di merito, inerenti cioè la necessità e la proporzionalità dell'ordine, possono essere contestati solo nello Stato di emissione. Tra i motivi di legittimità spicca quello relativo all'incompatibilità dell'ordine di produzione con gli obblighi dello Stato membro in conformità dell'art. 6 TUE e della Carta. Il ruolo del *service provider* viene invece confinato alla mera possibilità che qualora non possa ottemperare, per una serie di ragioni indicate dal Regolamento, agli obblighi contenuti negli ordini, questi dovrà contattare sia l'autorità di emissione che di esecuzione e tale notifica può o meno avere effetto sospensivo sulla base dei motivi di impedimento comunicati.

Il testo di compromesso se da una parte nega ai service *providers* la possibilità, come accennato in precedenza, di sollevare motivi di rifiuto, prevede che qualora sussistano le condizioni per una doppia notifica di cui all'Art. 7a, l'autorità di esecuzione ha il potere di decidere, entro 10 giorni dal ricevimento dell'ordine, se sollevare un motivo di rifiuto tassativamente previsti dal Regolamento. Tra questi ultimi vengono comprese le situazioni eccezionali in cui, vi sono motivi sostanziali per ritenere, sulla base di prove specifiche e oggettive, che l'esecuzione dell'ordinanza comporterebbe, nelle particolari circostanze del caso, una manifesta violazione di un diritto fondamentale dall'art. 6 TUE e dalla Carta. Viene dunque preservato tale motivo di rifiuto presente nella relazione del Parlamento, ma la sua formulazione appare più stringente. In particolare, la decisione di qualificare la violazione come "manifesta" sembra far riferimento

al recente filone giurisprudenziale in materia di Mandato di Arresto Europeo ("**MAE**") e protezione dei diritti fondamentali.[312]

Per quanto riguarda i *service providers*, diversamente da quanto previsto nella Proposta della Commissione, il testo di compromesso non concede loro la possibilità di opporsi all'esecuzione di un ordine di produzione, ma solo di segnalare all'autorità di emissione, e se è prevista la doppia notifica, ai sensi dell'Art. 7a, anche alle autorità dello Stato di esecuzione, alcune questioni specifiche relative all'ordine.[313] Il *service provider* può sollevare questioni relative alla sua incompletezza, alla possibilità che contenga errori manifesti o informazioni insufficienti, e alla sussistenza di impossibilità de facto di eseguirlo non attribuibili al *service provider*. Inoltre, quest'ultimo può anche giustificare il fatto di non fornire i dati, di non fornirli in modo esaustivo o di non fornirli entro i termini previsti per altri motivi.

In aggiunta, qualora il *service provider* ritenga, sulla base delle sole informazioni contenute nell'ordine di produzione o di conservazione, che l'esecuzione di quest'ultimo possa interferire con le immunità o i privilegi, o con le norme sulla determinazione o la limitazione della responsabilità penale che riguardano la libertà di stampa o la libertà di espressione in altri mezzi di comunicazione nello Stato di esecuzione, il *service provider* informa le autorità competenti dello Stato di emissione e dello Stato di esecuzione.[314] Una simile operazione potrebbe rivelarsi piuttosto difficoltosa nella pratica, alla luce delle poche informazioni che ai sensi del Regolamento devono essere contenute nel certificato. Inoltre, come evidenziato, il fatto che il testo di compromesso lasci comunque, in sostanza, alla discrezionalità dei *providers*, la scelta di non eseguire l'ordine nel momento in cui, secondo una loro valutazione, ci siano buone ragioni per metterlo in discussione, trasforma *de facto* i *service providers* in dei "custodi dei diritti fondamentali degli individui", un compito solitamente riservato alle autorità pubbliche, ma oggi sempre più spesso trasferito a soggetti privati.[315] Rispetto all'ordine di conservazione, l'autorità di emissione, tenendo conto delle informazioni comunicate dal *provider*, decide, di propria iniziativa o su richiesta dello Stato di esecuzione, se ritirare, adattare o mantenere

[312] Vedi casi C-404/15 and C-659/15 PPU, Aranyosi e Căldăraru [2016] ECLI:EU:C:2016:198; C-216/18 PPU, *LM* [2018] ECLI:EU:C:2018:586.
[313] Art. 9 testo di compromesso.
[314] Art. 9(2a) testo di compromesso.
[315] Stanisław Tosza, 'The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?' (2023) 2 EDPL 163, 170.

l'ordine.[316] In relazione all'ordine di produzione, se non viene effettuata alcuna notifica ai sensi dell'articolo 7a, l'autorità di emissione tiene conto delle informazioni ottenute e decide, di propria iniziativa o su richiesta dell'autorità di esecuzione, se ritirare, adattare o mantenere l'ordinanza. Quando viene effettuata una notifica ai sensi dell'articolo 7a, l'autorità di emissione tiene conto delle informazioni ottenute e decide se ritirare, adattare o mantenere l'ordine.

2.3.5. I regimi sanzionatori e le procedure di *enforcement*

L'inottemperanza agli obblighi previsti dagli ordini ai sensi del Regolamento può provocare due tipi di conseguenze, l'applicazione di sanzioni e il dispiego di procedure di esecuzione.

Per quanto concerne le sanzioni, il testo di compromesso lascia agli Stati membri il compito di stabilire sanzioni pecuniarie che siano effettive, dissuasive e proporzionate nei confronti di chi violi gli obblighi di esecuzione degli ordini previsti dal Regolamento,[317] con conseguente diversità di regimi applicabili in materia di misure sanzionatorie in caso di inottemperanza.[318] Come fortemente voluto dal Consiglio, viene specificato nel testo di compromesso all'Art. 13 che gli Stati membri assicurino che possano essere imposte sanzioni pecuniarie fino al 2% del fatturato mondiale annuo del *service provider*.

Tuttavia, tale precisazione risulta t di dubbia utilità e applicazione. Da una parte, l'indicazione di una somma massima della sanzione parametrata al fatturato mondiale non elimina i potenziali rischi di *forum shopping*, in quanto le legislazioni nazionali rimangono libere di imporre sanzioni proprie nel limite del citato 2%.[319] Dall'altra, non è dato comprendere sulla base di quali criteri quantificare il fatturato "mondiale" del *provider*, anche in considerazione delle complesse strutture societarie in cui questo opera.[320]

All'art. 14 testo di compromesso viene prevista, invece, una complessa procedura esecutiva contro i *service providers* che non hanno ottemperato agli ordini, senza fornire motivazioni accettate dall'autorità di emissione e qualora l'autorità di esecuzione non abbia invocato alcun motivo di rifiuto. In tali ipotesi, vengono chiamate in causa le autorità giudiziarie dello Stato di

---

[316] Art. 10(3a) testo di compromesso.
[317] Art. 13 testo di compromesso.
[318] Raffaella Pezzuto, 'Accesso Transnazionale alla Prova Elettronica mel Procedimento Penale: la Nuova Iniziativa Legislativa della Commissione Europea al Vaglio del Consiglio dell'Unione' (2019) 1 Diritto Penale Contemporaneo 57, 61.
[319] Oscar Calavita, 'La Proposta di Regolamento sugli Ordini di Produzione e Conservazione Europei: Commissione, Consiglio e Parlamento a Confronto' (2021) La Legislazione Penale 1, 34.
[320] Ibid.

esecuzione, le quali sono tenute a riconoscere gli ordini e ad obbligare il *provider* ad ottemperare agli obblighi di produzione o conservazione, salvo che sussista uno o più dei motivi di opposizione, elencati tassativamente dal testo al quarto e al quinto comma, per gli ordini rispettivamente di produzione e conservazione. Nel caso in cui il destinatario non adempia agli obblighi derivanti da un'ordinanza riconosciuta la cui esecutività sia stata confermata dall'autorità di esecuzione, quest'ultima impone una sanzione pecuniaria in conformità all'articolo 13. Contro la decisione di imporre una sanzione pecuniaria deve essere garantito un ricorso giurisdizionale effettivo.

2.3.6. La salvaguardia dei diritti fondamentali

Pur costituendo un importante passo in avanti in una disciplina complessa e in continua evoluzione come quella dell'accesso *cross-border* alle prove digitali, il meccanismo creato dagli ordini di produzione e conservazione solleva gravi interferenze rispetto alla salvaguardia dei diritti fondamentali dei vari soggetti coinvolti.[321] Le disposizioni proposte nel Regolamento possono potenzialmente incidere su una serie di diritti fondamentali: (i) i diritti alla protezione dei dati personali, al rispetto ad una vita privata, alla libertà di espressione, alla difesa e ad un ricorso effettivo di fronte ad un giudice imparziale in capo alle persone fisiche a cui dati è previsto l'accesso; (ii) i diritti alla libertà di impresa e ad un ricorso effettivo in capo ai *service providers*; (iii) i diritti alla libertà e sicurezza di tutti i cittadini.[322]

Alla luce di tali potenziali interferenze, occorre sottolineare, in primo luogo, che poiché gli ordini possono essere emessi nell'ambito di un procedimento penale, tutte le garanzie procedurali di diritto penale sono applicabili, tra cui, in particolare, il diritto a un equo processo sancito dall'art. 6 CEDU e dagli artt. 47 e 48 della Carta e la legislazione pertinente dell'UE in materia di diritti procedurali nei procedimenti penali, vale a dire le c.d. Direttive di Stoccolma.[323] Come precisato dal considerando 2 testo di compromesso, da una parte le misure per ottenere e conservare le prove elettroniche sono sempre più importanti per consentire indagini e azioni penali in tutta l'Unione. Dall'altra è necessario bilanciare l'efficacia dei meccanismi per l'acquisizione di prove elettroniche, essenziali per combattere la criminalità,

---

[321] Christos Karagiannis, 'Digital evidence "hidden in the Cloud": Is "possession" still a relevant notion?' (2023) 23 ERA Forum 301, 310.
[322] 'Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale' COM(2018) 225 final, 10.
[323] Ibid.

con i diritti e i principi fondamentali riconosciuti dall'art. 6 TUE e dalla Carta, in particolare i principi di necessità e proporzionalità, del giusto processo, della protezione della vita privata e dei dati personali e della riservatezza delle comunicazioni. Tale necessità di bilanciamento viene poi tradotta all'art. 1(2), che prevede che il Regolamento non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dalla Carta e dall'art. 6 TUE.

Un particolare bilanciamento tra diritti fondamentali dell'indagato/imputato e le esigenze di contrasto al crimine e di efficiente cooperazione *cross-border* era contenuto all'art. 11 della Proposta della Commissione: la norma prescrive al *service provider* di prendere le misure necessarie al fine di garantire la riservatezza degli ordini e dei relativi dati prodotti o conservati e, se richiesto dall'autorità di emissione, di astenersi dall'informare la persona i cui dati sono stati richiesti, per non ostacolare lo svolgimento del relativo procedimento penale. Qualora l'autorità di emissione avesse richiesto tale obbligo riservatezza, quest'ultima aveva il dovere di informare senza indebito ritardo la persona i cui dati sono stati richiesti in merito alla produzione dei dati e in merito ai mezzi di ricorso esperibili. Tuttavia, la comunicazione di tali informazioni poteva essere posticipata per il tempo necessario e proporzionato per non ostacolare il relativo procedimento penale. Sotto questo profilo, la relazione del Parlamento si è limitata a specificare che l'obbligo di riservatezza imposto al *service provider* dall'autorità di emissione deve essere imposto per il tempo necessario e proporzionato al fine di non ostacolare il pertinente procedimento penale o per tutelare i diritti fondamentali di un'altra persona, e tenendo, tuttavia, in considerazione l'impatto della misura sui diritti fondamentali della persona i cui dati sono richiesti.

Su queste norme si è invece particolarmente soffermata l'attenzione del Consiglio in sede di negoziato, modificando i rispettivi ruoli dell'autorità di emissione e del *service provider*.[324] Il nuovo testo proposto dal Consiglio prevede un generale divieto in capo al *service provider* di informare la persona i cui dati siano stati richiesti o preservati, a meno che non sia la stessa autorità di emissione a chiedere esplicitamente al *service provider* di informare il soggetto interessato. Qualora tale richiesta venga effettuata, l'autorità di emissione dovrà fornire indicazioni al *provider* circa i rimedi che possono essere da questo esperiti contro la misura adottata. Nel caso in cui non venga invece effettuata la richiesta, l'autorità di emissione deve

[324] Art. 11 orientamento generale.

provvedere ad informare la persona i cui dati siano stati richiesti o preservati, provvedendo a fornire anche le informazioni necessarie per esperire i rimedi previsti contro l'ordine. L'autorità di emissione può ritardare questo adempimento solo nella misura in cui ciò risponda a criteri di necessità e proporzionalità nell'ambito del procedimento penale che ha originato l'ordine di acquisizione o conservazione della prova elettronica. Unica eccezione prevista all'obbligo di informazione in capo all'autorità emittente è prevista per il caso di ordini che abbiano ad oggetto dati relativi agli abbonati o agli accessi, qualora venga ritenuto che l'informazione della persona interessata possa ledere i diritti fondamentali o gli interessi legittimi di un terzo, che devono essere considerati prioritari rispetto alla tutela del soggetto a cui i dati appartengono.

Il testo di compromesso sembra aver adottato un approccio più simile a quello del Consiglio. Ai sensi del nuovo art. 11, è l'autorità di emissione a dover informare il soggetto interessato, ma solo in caso di ordini di produzione, senza indebito ritardo. Tuttavia, l'autorità di emissione può, conformemente alla legislazione nazionale, ritardare, limitare o omettere di informare il soggetto, nella misura e per il tempo in cui sono soddisfatte le condizioni di cui all'art. 13(3) della Direttiva in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte della polizia e dalle autorità di giustizia penale.[325] In tal caso, l'autorità di emissione deve indicare nel fascicolo i motivi del ritardo, della limitazione o dell'omissione. Una breve giustificazione deve essere aggiunta anche nel certificato. I *service providers* adottano le necessarie misure operative e tecniche all'avanguardia per garantire la riservatezza, la segretezza e l'integrità dei dati,

All'art. 17 testo di compromesso vengono previsti i rimedi esperibili contro gli ordini di produzione da parte dell'indagato/imputato e terzi i cui dati sono stati ricercati attraverso tali misure. Fatti salvi ulteriori rimedi giuridici offerti dal diritto nazionale, le persone i cui dati sono stati ricercati tramite un ordine di produzione europeo hanno diritto a rimedi efficaci contro lo stesso. Se la persona in questione è un indagato/imputato, questi ha diritto a mezzi di ricorso efficaci durante il procedimento penale in cui i dati sono stati utilizzati, fatti salvi i rimedi disponibili ai sensi della Direttiva in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte della polizia e dalle autorità di giustizia penale

[325] 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 [2016] OJ L 119/89.

e dal Regolamento Generale sulla Protezione dei Dati.[326] Il diritto a un ricorso effettivo è esercitato dinanzi a un'autorità giudiziaria dello Stato di emissione in conformità al suo diritto nazionale e comprende la possibilità di contestare la legittimità della misura, comprese la sua necessità e proporzionalità, fatte salve le garanzie dei diritti fondamentali nello Stato di esecuzione. Al rimedio si applicano gli stessi termini o altre condizioni previsti in casi analoghi a livello nazionale in modo da garantire l'effettivo esercizio di tali rimedi per i soggetti interessati.

Infine, fatte salve le norme procedurali nazionali, lo Stato di emissione e tutti gli altri Stati membri in cui siano state trasmesse le prove digitali devono assicurare che nei relativi procedimenti penali nazionali siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'ordine europeo di produzione. Si tratta di una disposizione che è possibile trovare anche agli artt. 12(2) e 10(2), rispettivamente, delle Direttive 2013/48/UE sul diritto di avvalersi di un difensore, di informare un terzo al momento della privazione della libertà personale e di comunicare con terzi e con le autorità consolari e 2016/343/UE sulla presunzione d'innocenza.

Sotto questo profilo, la proposta della Commissione presentava tuttavia una portata molto più innovativa: l'ultimo paragrafo dell'art. 17 Proposta doveva essere letto in combinato disposto al considerando 54, ove veniva stabilito, *inter alia*, che l'esercizio del rimedio effettivo da parte dell'indagato o imputato potesse incidere "sull'ammissibilità delle prove ottenute con detti mezzi o, a seconda del caso, sul peso di tali prove nell'ambito del procedimento". La Commissione aveva quindi cercato di adottare una previsione più coraggiosa in materia di rimedi rispetto a quanto previsto nelle Direttive di Stoccolma.[327] Nel considerando della proposta di Regolamento in questione, viene finalmente ammesso in modo esplicito che la violazione delle norme europee può influire sull'ammissibilità o sulla valutazione delle prove raccolte di fronte al giudice nazionale. Occorre inoltre notare come nella relazione del Parlamento si fosse compiuto un ulteriore passo in avanti in tal senso: per la prima volta venivano introdotte delle norme in materia di ammissibilità delle informazioni elettroniche

[326] 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 [2016] OJ L 119/1.
[327] Mitja Gialuz e Jacopo Della Torre, 'Lotta alla Criminalità nel Cyberspazio: la Commissione presenta due Proposte per facilitare la Circolazione delle Prove Elettroniche nei Processi Penali' (2018) 5 Diritto Penale Contemporaneo 277, 288.

come prove, prevedendo che se ottenute in violazione del Regolamento, tali informazioni non sono ammissibili come prove dinanzi ad un organo giurisdizionale, prevedendo che l'inammissibilità si applichi anche qualora le informazioni elettroniche siano state ottenute prima che sia stato invocato uno dei motivi di non riconoscimento elencati dal regolamento.

Tuttavia, tali proposte sono state eliminate nel testo di compromesso. Pertanto, nonostante la Commissione avesse identificato come problematico il modo in cui gli Stati membri governassero l'ammissibilità delle prove digitali nei procedimenti penali transfrontalieri,[328] non sono state incluse disposizioni per garantire l'affidabilità e la contestabilità dell'utilizzo delle prove digitali raccolte attraverso ordini di produzione europei.[329] Ciò non stupisce in quanto, come analizzato in seguito, gli Stati membri hanno da sempre mostrato una forte opposizione all'idea di armonizzare al livello comunitario norme in materia di ammissibilità, fondando tale dissenso sui limiti imposti dai principi di proporzionalità e sussidiarietà.

Rispetto al diritto alla difesa dell'indagato/imputato, viene fatta salva nel testo di compromesso l'aggiunta del Parlamento di permettere all'imputato o indagato, anche per mezzo del proprio difensore, di richiedere l'emissione di un ordine di produzione o conservazione conformemente alla procedura nazionale.[330] Così come previsto dalla DOEI, viene dunque dato spazio alle indagini difensive, le quali tuttavia pare non possano essere effettuate dal difensore autonomamente in assenza dell'intervento dell'autorità pubblica. Tale limite potrebbe ridurre la facoltà riconosciuta alla difesa ad un mero potere di sollecitazione dell'autorità nazionale competente.[331]

Infine, due importanti novità vengono introdotte dal Consiglio. La prima è relativa all'introduzione di una previsione sul rispetto del principio del *ne bis in idem* internazionale in situazioni di contemporanea pendenza di due procedimenti penali per la medesima vicenda. Tale aggiunta viene confermata anche nel testo di compromesso.[332] La seconda novità riguarda

---

[328] Si veda Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace (15072/1/16 Brussels, 7 December 2016), 10.
[329] Radina Stoykova 'The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations' (2023) 49 Computer Law & Security Review 1, 2.
[330] Art. 1(1a) testo di compromesso.
[331] Oscar Calavita, 'La Proposta di Regolamento sugli Ordini di Produzione e Conservazione Europei: Commissione, Consiglio e Parlamento a Confronto' (2021) La Legislazione Penale 1, 39.
[332] Si veda art. 10a(1)(c) testo di compromesso in cui il non rispetto del principio viene espressamente previsto come motivo di rifiuto; al considerando 35 testo di compromesso viene specificato che l'ordine non dovrebbe essere emesso qualora sussista un dubbio di violazione del principio.

l'introduzione del principio di specialità, assente non solo nella proposta della Commissione ma anche, sorprendentemente, nella DOEI. Tale principio poneva un importante limite: il divieto per le prove elettroniche di poter essere utilizzate ai fini di procedimenti diversi da quelli per i quali sono state ottenute in conformità al presente regolamento o di venire tramesse ad un altro Stato membro. Due eccezioni venivano poi previste dal Consiglio, vale dire l'utilizzo di tali prove in procedimenti per i quali avrebbe potuto essere emesso un ordine di produzione europeo nel rispetto delle condizioni di emissione previste dal Regolamento, o al fine di prevenire una minaccia grave e immediata alla sicurezza pubblica dello Stato di emissione o ai suoi interessi essenziali. Infine, il trasferimento ad un paese terzo o ad un'organizzazione internazionale era sottoposto alle condizioni previste nella Direttiva in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte della polizia e dalle autorità di giustizia penale.

Tali norme avrebbero rappresentante un'importante garanzia per la persona i cui dati sono stati raccolti tramite un ordine di produzione. Tuttavia, il principio di specialità non è stato adottato dal testo di compromesso. La *ratio* dietro tale scelta potrebbe essere dovuta all'assenza di tale previsione nella DOEI. Infatti, qualora tale differenza fosse stata mantenuta, in caso di dubbio e per evitare rischi, e tenendo conto che potrebbe esserci un interesse a trasmettere prove in futuro per utilizzarle in altri procedimenti nazionali, gli Stati membri potrebbero decidere di optare per l'utilizzo di un OEI, al posto di un Ordine di Produzione Europeo, proprio perché più costrittivo, prevedendo espressamente il principio di specialità.[333] In altre parole, avere regole diverse per misure con obiettivi affini avrebbe potuto portare ad una parziale perdita di interesse nell'utilizzo del nuovo strumento per la raccolta di prove elettroniche, il che contrasterebbe con l'obiettivo del legislatore di creare un nuovo modo, più diretto e facilitato, di ottenere prove digitali.[334]

In conclusione, è possibile affermare che pur venendo stabilite alcune salvaguardie in tema di protezione dei diritti fondamentali, ampio spazio viene lasciato alle rispettive discipline nazionali. Alla luce delle significative interferenze che le misure investigative previste possono arrecare ai diritti fondamentali dei soggetti coinvolti, la soluzione adottata dal legislatore europeo presenta numerose perplessità. Da una parte, come analizzato più approfonditamente

[333] Júlio Barbosa e Silva, 'The speciality rule in cross-border evidence gathering and in the European Investigation Order—let's clear the air' (2019) 19 ERA Forum 485, 500.
[334] Ibid.

in seguito, gli standard nazionali di protezione giuridica dei diritti fondamentali nel contesto dell'accesso alle prove elettroniche variano in modo significativo da uno Stato membro all'altro.[335] Dall'altra, il ruolo giocato dalla presunzione di fiducia reciproca governante la cooperazione giudiziaria in materia penale nello SLSG risulta particolarmente delicato in una cornice normativa che consente agli Stati membri di ottenere direttamente informazioni da soggetti privati, come i *service providers*, con un controllo piuttosto marginalizzato da parte dello Stato di esecuzione.[336]

2.3.7. Il conflitto con leggi di paesi terzi

La Commissione aveva individuato nella sua Proposta un possibile ostacolo al funzionamento dell'ordine di produzione: il *service provider* aveva il potere di non eseguire l'ordine qualora tale adempimento fosse in conflitto con le norme di uno Stato terzo, che ponevano un divieto circa la divulgazione dei dati richiesti, e che il *service provider* era tenuto a rispettare.[337] Al fine di superare l'ostacolo della sussistenza di due obblighi contrastanti in capo al *provider*, nella Proposta era stata prevista una procedura specifica, differenziata a seconda che il divieto di consegna fosse relativo alla tutela di diritti fondamentali dell'individuo o di interessi fondamentali del paese terzo (art. 15 Proposta) o riguardasse interessi di altra natura (art. 16 Proposta). Considerando che molti *service provider* hanno la loro sede principale al di fuori dello dell'Unione, si pensi ad esempio a *Google* o *Facebook*, tale norma rivestiva un'importanza fondamentale nell'economia del Regolamento.[338] Tuttavia, la soluzione proposta di cui all'art. 15 aveva destato molte perplessità nel corso del negoziato, in quanto attribuiva al *service provider* un inedito ruolo di garante degli interessi politici di un paese terzo, conferendogli *de facto* il potere di bloccare temporaneamente l'esecuzione di un ordine sulla base di valutazioni totalmente discrezionali. In aggiunta, la decisione finale era in ogni caso

---

[335] Michele Simonato, 'Defence Rights and the use of Information Technology in Criminal Procedure' (2014) 85 Revue Internationale de Droit Pénal 261, 281. Sotto questo profilo, la Direttiva 2016/280, più volte menzionata dal testo di compromesso, adotta alcune norme comuni in materia di diritti procedurali concessi agli imputati i cui dati elettronici vengono usati come prova in un procedimento penale, tuttavia, molti aspetti sono ancora lasciati alla discrezionalità degli Stati membri.

[336] Nathalie A. Smuha, 'Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency' (2018) 8(1) European Criminal Law Review 83, 95.

[337] Raffaella Pezzuto, 'Accesso Transnazionale alla Prova Elettronica mel Procedimento Penale: la Nuova Iniziativa Legislativa della Commissione Europea al Vaglio del Consiglio dell'Unione' (2019) 1 Diritto Penale Contemporaneo 57, 81.

[338] Mitja Gialuz e Jacopo Della Torre, 'Lotta alla Criminalità nel Cyberspazio: la Commissione presenta due Proposte per facilitare la Circolazione delle Prove Elettroniche nei Processi Penali' (2018) 5 Diritto Penale Contemporaneo 277, 288.

subordinata alla volontà del paese terzo, imponendo una procedura macchinosa e lenta, incompatibile la natura volatile del dato elettronico e quindi in contrasto con la stessa *ratio* del Regolamento.

Pertanto, l'art. 15 è stato totalmente eliminato dal Consiglio in sede di orientamento generale, mentre è stato mantenuto l'art. 16, che tuttavia ha subito importanti emendamenti.[339] In particolare, nel testo di compromesso viene previsto che qualora il *service provider* ritenga che l'adempimento dell'ordine di produzione europeo sia in conflitto con le leggi applicabili di un paese terzo, questi debba informare, entro 10 giorni da quando ha ricevuto l'ordine, l'autorità di emissione e l'autorità di esecuzione dei motivi di non esecuzione. L'obiezione motivata deve contenere tutti i dettagli pertinenti sulla legge del paese terzo, sulla sua applicabilità al caso in questione e sulla natura dell'obbligo in conflitto. Non può basarsi sul fatto che disposizioni analoghe riguardanti le condizioni, le formalità e le procedure di emissione dell'ordine non esistono nella legge applicabile del paese terzo, né sulla sola circostanza che i dati sono conservati in un paese terzo. In primo luogo, l'autorità di emissione riesamina l'ordine di produzione sulla base dell'obiezione motivata e di qualsiasi contributo fornito dallo Stato di esecuzione, e qualora intenda mantenere l'ordine di produzione, questa richiede poi un riesame da parte del tribunale competente del proprio Stato membro, con effetto sospensivo circa l'esecuzione dell'ordine.

Il giudice incaricato deve valutare, tenendo conto di tutte le circostanze specifiche del caso, se il diritto del paese terzo si applica al caso in questione e, in caso affermativo, se effettivamente esistono obblighi in conflitto. A tal fine, ha la facoltà di richiedere informazioni all'autorità competente del paese terzo, purché ciò non comporti pregiudizi per le indagini in corso. Nel caso in cui il giudice giunga alla conclusione che sussiste un contrasto, dovrà valutare se emettere o meno l'ordine. In particolare, nel porre in essere tale decisione deve attribuire importanza all'interesse tutelato dalla legge del paese terzo, inclusa la necessità di proteggere diritti fondamentali o altri interessi, come la sicurezza nazionale del paese terzo, che possano ostacolare la consegna dei dati. Inoltre, il giudice deve considerare il grado di connessione del procedimento penale con la giurisdizione del paese di nazionalità, residenza o dimora del soggetto cui i dati appartengono o delle vittime del reato, nonché con la giurisdizione del luogo

[339] Raffaella Pezzuto, 'Accesso Transnazionale alla Prova Elettronica mel Procedimento Penale: la Nuova Iniziativa Legislativa della Commissione Europea al Vaglio del Consiglio dell'Unione' (2019) 1 Diritto Penale Contemporaneo 57, 82.

in cui il reato è stato commesso. Qualora l'autorità giurisdizionale giunga alla decisione di confermare l'ordine di acquisizione precedentemente emesso, deve informare sia l'autorità di emissione che il *service provider*. In questo caso, quest'ultimo è obbligato a dare esecuzione all'ordine, dal momento che è stato eliminato il carattere obbligatorio e vincolante della consultazione con lo stato terzo, come inizialmente proposto dalla Commissione.

L'apertura dei negoziati UE-USA: differenze tra l'e-evidence package e il Cloud Act. Cenni.

Nel giugno 2019 il Consiglio ha autorizzato la Commissione ad aprire i negoziati, a nome dell'UE, circa un accordo sull'accesso transfrontaliero alle prove elettroniche con gli Stati Uniti, al fine di facilitare la cooperazione e garantire solide garanzie a tutela dei diritti fondamentali.[340] Sotto questo profilo, occorre sottolineare non solo che gli Stati Uniti ospitano la maggior parte dei *service providers*,[341] ma anche che questi hanno recentemente adottato in materia il *CLOUD Act* ("*Clarifying Lawful Overseas Use of Data Act*").[342] Quest'ultimo permette la conclusione di accordi bilaterali, che costituiscono la base per il trasferimento di prove elettroniche tra gli Stati Uniti e i paesi terzi autorizzati, che soddisfano i criteri stabiliti dal legislatore statunitense.[343] In linea di principio, la legislazione statunitense vietava infatti ai *service providers* di condividere i dati sui contenuti con le autorità di polizia e giudiziarie straniere al di fuori delle formali procedure di mutua assistenza,[344] le quali, come ribadito in precedenza, mal si conciliano con la natura volatile e fragile della prova digitale. Il *CLOUD Act* elimina tale divieto, a condizione che gli Stati Uniti firmino un accordo con lo Stato in questione basato sulla valutazione dello Stato di diritto e della protezione della *privacy* di quello Stato.[345] In questo senso appare di fondamentale importanza avere un unico accordo UE-USA, invece di un mosaico frammentato di accordi diversi tra gli Stati Uniti e i singoli Stati

---

[340] Consiglio dell'Unione europea, 'Un migliore accesso alle prove elettroniche per combattere la criminalità' <https://www.consilium.europa.eu/it/policies/e-evidence/> ultimo accesso 29 settembre 2023.
[341] Ibid.
[342] *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text> ultimo accesso 29 settembre 2023.
[343] Marcin Rojszczak, 'e-Evidence Cooperation in Criminal Matters from an EU Perspective' (2022) 85(4) The Modern Law Review, 997, 999.
[344] Per maggiori informazioni si veda 'Electronic Communications and Privacy Act' (1986) <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=The%20ECPA%2C%20as%20amended%2C%20protects,conversations%2C%20and%20data%20stored%20electronically> ultimo accesso 29 settembre 2023.
[345] Stanislaw Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161, 170.

membri.[346] L'adozione di una normativa europea è dunque essenziale in tal senso. Allo stesso tempo, occorre tuttavia considerare che il modello di cooperazione del *CLOUD Act* stabilisce un diverso equilibrio, rispetto al Regolamento adottato, tra i poteri di indagine e i diritti fondamentali di chi vi è sottoposto, contenendo, in particolare, garanzie procedurali per le persone i cui dati vengono trasferiti che differiscono in modo significativo da quelle previste dal legislatore UE.[347]

2.3.8. Il rapporto con il Secondo Protocollo Addizionale alla Convenzione di Budapest

Al momento della presentazione del pacchetto, al livello internazionale erano già state avviate le negoziazioni sul precedentemente analizzato Secondo Protocollo Addizionale alla Convenzione di Budapest, volto a realizzare obiettivi affini a quelli prefissati dalla Commissione. Dal momento che solo gli Stati possono esserne parti, l'UE ha recentemente autorizzato gli Stati membri a firmare e ratificare il Protocollo.[348] Per gli Stati membri tale misura costituirà uno strumento importante, che andrà integrare il quadro normativo creato dall'"*e-evidence package*".[349] Tuttavia, pur essendo rivestendo un ruolo essenziale in materia, un nuovo insieme di norme a livello internazionale non rappresenta comunque una soluzione sufficiente per affrontare gli ostacoli posti dalla raccolta della prova digitale nei contesti *cross-border* dell'Unione.

Ciò alla luce del fatto che, in primo luogo, il Secondo Protocollo non ha la stessa portata del pacchetto proposto dalla Commissione, non essendo fondato sul medesimo livello di *mutual trust* tra le Parti contraenti, esistente invece tra gli Stati membri dell'Unione. A differenza del Regolamento, come analizzato in precedenza, le disposizioni del Protocollo lasciano una notevole discrezionalità allo Stato richiedente nel determinare le modalità di esecuzione delle richieste destinate ai *service providers* nazionali, creando un quadro normativo comune più flessibile, costituito da numerose norme bilaterali per la raccolta delle prove elettroniche.[350]

---

[346] Ibid.
[347] Marcin Rojszczak, 'e-Evidence Cooperation in Criminal Matters from an EU Perspective' (2022) 85(4) The Modern Law Review 997, 999.
[348] Consiglio dell'Unione europea, 'Accesso alle prove elettroniche: il Consiglio autorizza gli Stati membri a ratificare un accordo internazionale' <https://www.consilium.europa.eu/it/press/press-releases/2023/02/14/access-to-e-evidence-council-authorises-member-states-to-ratify-international-agreement/> ultimo accesso 29 settembre 2023.
[349] Marcin Rojszczak, 'e-Evidence Cooperation in Criminal Matters from an EU Perspective' (2022) 85(4) The Modern Law Review 997, 1016.
[350] Ibid.

Allo stesso tempo, il Secondo Protocollo, presentando la differente natura di trattato internazionale, non può offrire gli stessi meccanismi di *enforcement* rispetto ad una misura adottata dal legislatore UE.

3. La *data retention saga*: tra esigenze di prevenzione, indagine, accertamento e perseguimento dei reati e salvaguardia dei diritti fondamentali

L'avvento dell'era digitale ha fatto sorgere, *inter alia*, l'esigenza di impiegare strumenti che, al fine di verificare e reprimere qualsiasi forma di attività criminosa perpetrata attraverso la rete, superano il confine tracciato dal sistema delle intercettazioni, già noto alle legislazioni degli Stati membri e alle corti nazionali ed europee, spingendosi in un'area più complessa, in cui sorge una necessità ancora più impellente di bilanciare l'esigenza di prevenire e reprimere atti illeciti con la tutela dei diritti fondamentali, vale a dire l'area della *data retention*.[351] Come accennato in precedenza, con il termine "*data retention*" si fa riferimento alla conservazione dei dati relativi al traffico e all'ubicazione, i c.d. metadati, da parte di *service providers* al fine di un successivo ed eventuale accesso da parte delle autorità investigative e giudiziarie.[352]

Appare chiaro che, se queste operazioni non sono giustificate da specifiche ragioni di indagine o da un chiaro collegamento con una minaccia alla sicurezza, c'è il rischio che tali metodologie si trasformino in un'intrusione evidente nei diritti alla riservatezza e alla protezione dei dati, ma anche nell'esercizio delle libertà fondamentali in una società democratica. Pertanto, è essenziale, in uno Stato di diritto, trovare un equilibrio tra l'utilizzo di queste metodologie investigative avanzate e il rispetto dei diritti fondamentali. [353]

Sotto questo profilo, l'UE ha presto riconosciuto l'importanza di ottenere queste tipologie di dati per le autorità investigative e giudiziarie, al fine di combattere efficacemente le minacce poste nell'era digitale da attività criminali come il terrorismo o la criminalità informatica. Già

---

[351]Alessandra Cardone, 'Il sistema del Data Retention come strumento investigativo' (2021) Giurisprudenza Penale Web, 1.

[352] Per un'analisi approfondita del tema della *data retention* e delle libertà fondamentali incise da tale fenomeno, Stefano Marcolini, 'L'istituto della data retention dopo la sentenza della Corte di Giustizia del 2014' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica),1579-1582.

[353] Giovanna Naddeo, 'Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di Giustizia UE' (2022) 2 Freedom, Security and Justice: European Legal Studies 188, 190.

agli inizi degli anni 2000, a seguito degli attentati terroristici di Madrid e Londra verificatesi rispettivamente nel 2004 e nel 2005, l'UE e i suoi Stati membri iniziano infatti ad adottare politiche volte ad inasprire la risposta sanzionatoria e a consentire indagini più efficienti contro le più gravi forme di criminalità organizzata.[354] Tali iniziative culminano poi, nel marzo del 2006, nell'adozione da parte del legislatore europeo di una direttiva "riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione", anche nota come "Direttiva sulla *data retention*".[355] In particolare, tale strumento muoveva dalla premessa che gli Stati membri si erano già dotati di discipline nazionali volte ad imporre ai *service providers* obblighi di conservazione dei dati relativi al traffico e all'ubicazione generati dall'uso di servizi di comunicazione elettronica, a fini di prevenzione, indagine, accertamento e perseguimento dei reati, trattandosi di un mezzo di contrasto alla criminalità rivelatosi nel tempo assai efficace.[356] Alla luce di tale constatazione, il legislatore EU si era dunque "limitato" a prevedere un generale obbligo di conservazione di dati, per un arco temporale da sei a ventiquattro mesi, per finalità di accertamento e perseguimento di reati qualificati come "gravi" da ciascuno Stato membro in accordo con la propria legislazione nazionale.[357] Come evidenziato dalla dottrina, il vizio della Direttiva in esame era quindi quello di essere eccessivamente "snella": dopo aver dichiarato nei Considerando che le legislazioni nazionali in materia di *data retention* erano diverse ed andavano armonizzate, lo strumento adottato falliva in tale obiettivo armonizzatore, rinviando circolarmente, per ogni aspetto concreto, proprio alle legislazioni nazionali da riavvicinare.[358] Allo stesso tempo, occorre notare come l'entrata in vigore del trattato di Lisbona nel 2009 ha avuto un impatto significativo sull'interpretazione delle disposizioni europee in

---

[354] Stefano Marcolini, 'La giurisprudenza della Corte di giustizia dell'Unione europea sulla data retention: il baluardo dei diritti fondamentali in Europa' in Stefano Marcolini e Roberto Flor, *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato* (Giappichelli 2022), 5.

[355] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE [2006] OJ L 105/54.

[356] Stefano Marcolini, 'La giurisprudenza della Corte di giustizia dell'Unione europea sulla data retention: il baluardo dei diritti fondamentali in Europa' in Stefano Marcolini e Roberto Flor, *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato* (Giappichelli 2022), 6.

[357] Casi C-293/12 e C-594/12, *Digital Rights Ireland* [2014] ECLI:EU:C:2014:238, para 60.

[358] Stefano Marcolini, 'La giurisprudenza della Corte di giustizia dell'Unione europea sulla data retention: il baluardo dei diritti fondamentali in Europa' in Stefano Marcolini e Roberto Flor, *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato* (Giappichelli 2022), 11.

materia di *data retention*: mentre la struttura dei tre pilastri viene abolita per creare un'unica Unione, e la Carta acquisiva lo stesso valore giuridico dei Trattati, gli Stati membri decidono di specificare la portata della loro clausola di identità nazionale, includendo l'area della "sicurezza nazionale" nelle varie materie oggetto di loro competenza esclusiva, ai sensi dell'Art. 4(2) TUE.

Come sottolineato dalla Commissione proprio in occasione della valutazione dell'applicazione della Direttiva,[359] se tali regimi di conservazione dei dati costituiscono un'arma indispensabile alla lotta alla criminalità, questi non possono che essere progettati, in uno Stato di diritto, in modo da garantire adeguate tutele per i diritti fondamentali, come garantiti dalla Carta. In particolare, l'equilibrio tra l'efficacia delle indagini e la protezione dei diritti fondamentali, tra i quali il diritto da una vita privata (Art. 7 Carta), alla protezione dei dati personali (Art. 8 Carta), alla libertà di espressione (Art. 11 Carta) e alla presunzione di innocenza (Art. 48(1) Carta), deve essere attentamente considerato nel momento in cui vengono formulati tali obblighi al livello sia europeo che nazionale.

Proprio l'assenza di un tale equilibrio porta prima le diverse Corti costituzionali a dichiarare invalide le leggi nazionali di attuazione della Direttiva,[360] e poi la CGUE a dichiarare invalido tale strumento nella storica sentenza *Digital Rights Ireland.*[361] Con questa decisione, i giudici di Lussemburgo affrontano per la prima volta la delicata questione concernente il bilanciamento fra esigenze di repressione ed accertamento dei reati e tutela dei diritti fondamentali dell'individuo, annullando quindi la Direttiva 2006/24/CE proprio perché contraria agli Artt. 7, 8 e 11 della Carta. In particolare, la CGUE sottolinea come l'obbligo di una conservazione generalizzata imposto dalla normativa comunitaria costituisca, di per sé, un'ingerenza grave nei diritti dei singoli individui. Pertanto, qualunque interferenza con la vita privata del cittadino avrebbe dovuto essere giustificata alla luce del principio di proporzionalità ex art. 52 Carta.[362] Sulla base di tali premesse, e in mancanza di un qualunque riferimento nella Direttiva a parametri oggettivi che consentissero di delimitare l'accesso ai dati sul traffico, la Corte ha

[359] Commissione dell'Unione Europea, 'Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24)' COM(2011) 225.
[360] In particolare, in Repubblica Ceca, Germania e Romania le rispettive Corti costituzionali avevano dichiarato incostituzionali le leggi nazionali di attuazione della stessa Direttiva.
[361] Casi C-293/12 e C-594/12, *Digital Rights Ireland* [2014] ECLI:EU:C:2014:238.
[362] Alessandro Malacarne e Gaia Tessitore, 'La ricostruzione della normativa in tema di data retention e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?' 3 Archivo penale 1, 25.

finito per rilevare il contrasto con principio di riservatezza, la cui tutela, come affermato dai giudici europei, passa anzitutto da una rigorosa interpretazione del canone di proporzionalità.[363]

La sentenza *Digital Rights Ireland* ha quindi aperto la strada ad una serie di pronunce da parte della CGUE, caratterizzate da una costante ricerca di bilanciamento tra i vari interessi contrapposti al fine di tracciare i limiti ai relativi obblighi imposti in materia di *data retention* per un'efficiente prevenzione e lotta al crimine nello SLSG. In particolare, il filo conduttore di tale orientamento giurisprudenziale è stato e continua ad essere l'interpretazione dell'Art. 15 della Direttiva 2002/58/CE, anche nota come Direttiva *e-Privacy*.[364] A seguito, infatti, dell'annullamento della Direttiva sulla *data retention,* il suddetto Art. 15 ha riacquisito un'indubbia centralità in quanto, allo stato, costituisce l'unica disposizione in materia di *data retention* nell'ordinamento giuridico dell'UE. Nel dettaglio, tale disposizione accorda agli Stati membri la possibilità di adottare misure legislative che deroghino al divieto generale di *retention,* qualora tali misure costituiscano "una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia (i) della sicurezza nazionale, (ii) della difesa, (iii) della sicurezza pubblica; e (iv) della prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica".[365] Da una parte tale articolo presenta il medesimo rischio dell'annullata Direttiva sulla *data retention,* ossia di un eccessivo rinvio alle discipline nazionali. Dall'altra, proprio al fine di rimediare a tale carattere eccessivamente generale, la CGUE, in attesa di un intervento legislativo al livello europeo,[366] ha nel tempo creato, proprio a partire dall'interpretazione dell'art. 15, un vero e proprio "statuto" in materia di *data retention,*[367] fornendo una preziosa e

---

[363] *Digital Rights Ireland*, para 65.

[364] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche OJ L 201/37 ("**Direttiva e-Privacy**").

[365] Giovanna Naddeo, 'Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di Giustizia UE' (2022) 2 Freedom, Security and Justice: European Legal Studies 188, 190.

[366] La proposta di regolamento che intende abrogare la Direttiva e-Privacy è attualmente in fase di negoziazione tra Consiglio e Parlamento europeo. Si veda 'Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE' COM(2017) 10 final.

[367] Stefano Marcolini, 'La giurisprudenza della Corte di giustizia dell'Unione europea sulla data retention: il baluardo dei diritti fondamentali in Europa' in Stefano Marcolini e Roberto Flor, *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato* (Giappichelli 2022), 18.

alquanto dettagliata guida in materia ai legislatori nazionali, aprendo un vero e proprio dialogo con le varie corti supreme e costituzionali degli Stati membri.

3.1. *Bulk data retention* e principio di proporzionalità al vaglio della CGUE

Fallito con *Digital Rights Ireland* il tentativo di armonizzazione la materia della *data retention* per scopi securitari, gli Stati membri, restii a rinunciare alle potenzialità dello strumento della conservazione generalizzata, sono tornati ad adottare o meglio hanno mantenuto, sulla base dell'art. 15 Direttiva *e-Privacy*, - e nonostante i principi emersi dalla sentenza *Digital Rights Ireland* - regimi di *bulk data retention* al livello nazionale. Tuttavia, queste normative hanno fatto emergere profondi timori nelle organizzazioni per i diritti civili, sempre più consapevoli, anche grazie alle note rivelazioni di Snowden, della pervasiva ingerenza nella sfera privata rappresentata dalla predisposizione di un obbligo diffuso di conservazione dei metadati, capace di consentire, una vera e propria una profilazione degli utenti, delle loro preferenze, frequentazioni e abitudini.[368]

Tali dubbi rispetto alla legittimità e conformità al diritto dell'UE di tali strumenti, seppur finalizzati alla garanzia della sicurezza, sono sfociati in due rinvii pregiudiziali, noti rispettivamente come i casi *Tele2*[369] e *Ministerio Fiscal*[370]. In entrambe queste decisioni i giudici di Lussemburgo si sono confrontati con l'interpretazione dell'art. 15, riconoscendo la mancata proporzionalità di una forma di *bulk data retention* e identificando in una "*targeted retention*", vale dire limitata a specifiche aree geografiche, gruppi sociali o periodi di tempo, l'unica forma legittima di *data retention*.

La CGUE ha adottato un approccio para-legislativo, fornendo un *vademecum* di criteri per guidare i legislatori nazionali nella creazione di obblighi di conservazione dei metadati. Tra questi criteri rientrano (i) la definizione di norme chiare e precise, (ii) requisiti e garanzie per

[368] Giulia Formici, 'La data retention saga al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture' (2021) *DPCE Online* 1361, 1362-63.
[369] Casi C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* [2016] ECLI:EU:C:2016:970.
[370] Caso C-207/16, *Ministerio Fiscal* [2016] ECLI:EU:C:2018:788.

evitare abusi, (iii) la relazione tra l'ingerenza nella sfera privata e la minaccia alla sicurezza, (iv) nonché la gravità del reato in questione.[371]

In particolare, la vicenda giudiziaria immediatamente successiva a *Digital Rights Ireland*, culminata nella sentenza nota come "*Tele2*", si occupa della questione, rimasta aperta, dei rapporti intercorrenti tra le discipline nazionali sulla *data retention* ed il diritto UE.[372] La questione principale sottoposta all'attenzione della CGUE mira a chiarire dopo l'annullamento della Direttiva 2006/24/CE, quale ruolo abbia preservato la *data retention* nel sistema UE. Nel caso *Digital Rights Ireland* i giudici remittenti avevano sottoposto alla CGUE non solo la questione circa l'invalidità della Direttiva sulla *data retention*, ma anche delle loro rispettive discipline nazionali. Tuttavia, nella pronuncia, la CGUE si era limitata a scrutinare, negandola, la validità dell'atto UE, mentre è mancato totalmente un giudizio sull'assetto delle discipline nazionali, che ha costituito invece proprio il fulcro della successiva giurisprudenza della CGUE, alla luce dell'interpretazione della richiamata disposizione di cui all'Art. 15 della Direttiva *e-Privacy*.

Due in particolare sono i quesiti che sono state sottoposti all'attenzione della Corte in *Tele2*. In primo luogo, veniva chiesto alla CGUE di chiarire se l'art. 15, letto alla luce della Carta, impedisse agli Stati membri di prevedere misure di *retention* generalizzata e indifferenziata (la c.d. *bulk data retention*) dei dati di traffico e dei dati relativi all'ubicazione di abbonati e utenti di servizi di comunicazione elettronica.[373] In secondo luogo, si domandava, in via accessoria, alla Corte se tale disposizione impedisse agli Stati membri di prevedere un accesso ai dati personali da parte delle autorità nazionali competenti, senza che tale accesso fosse limitato "alle sole finalità di lotta contro la criminalità grave" e senza sottoporlo ad un controllo *ex ante* da parte dell'autorità giudiziaria o amministrativa.[374]

Venendo al merito della prima questione, in via preliminare, la Corte conferma che il regime di d*ata retention* in esame rientra nell'ambito di applicazione della Direttiva *e-Privacy* e deve

---

[371] Eurojust, Data retention regimes in Europe in light of the CJEU ruling of 21 December in Joined Cases C-203/15 and C-698/15 (2017) <https://data.consilium.europa.eu/doc/document/ST-10098-2017-INIT/en/pdf> ultimo accesso 29 settembre 2023.
[372] Trattasi, di due rinvii pregiudiziali poi riuniti: il primo è stato sollevato in un giudizio svedese contro l'autorità nazionale in materia di poste e telecomunicazioni (C-203/15); il secondo in un giudizio inglese, promosso da tre cittadini contro il Ministero dell'Interno britannico (C-698/15).
[373] *Tele2*, para 62.
[374] Ibid, para 114.

quindi rispettare la normativa ivi contenuta, e in particolare il dettato di cui all'art. 15.[375] Successivamente, la CGUE fonda il proprio ragionamento sulla premessa che le norme di cui all'art. 15 abbiano carattere eccezionale e che dunque debbano essere interpretate restrittivamente.[376] Assunta tale prospettiva, la Corte sviluppa tale premessa, osservando, in primo luogo, come l'elenco degli obiettivi che consentono agli Stati membri di imporre regimi di *bulk retention*, vale a dire "la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica", abbia carattere esaustivo.[377]

In secondo luogo, viene sottolineato come la stessa disposizione preveda che tali regimi siano conformi ai principi generali del diritto dell'UE, tra cui i diritti fondamentali. Sotto quest'ultimo profilo, la CGUE decide quindi di elaborare dei criteri partendo dall'Art. 52 Carta, che riconosce che ogni limitazione all'esercizio dei diritti e delle libertà ivi contemplate deve essere prevista dalla legge e rispettare il loro contenuto essenziale e che le restrizioni necessarie ed effettivamente rispondenti ad obiettivi di interesse generale o alla tutela dei diritti altrui, invece, possono essere giustificate nel rispetto del principio di proporzionalità.[378] Così la CGUE fornisce un *vademecum* sulle condizioni che legittimano l'applicazione di queste misure, traducendo i limiti stabiliti dalla stessa Carta alle specifiche caratteristiche dei regimi nazionali di *bulk retention*.[379]

Innanzitutto, occorre che la normativa nazionale definisca, mediante regole chiare e precise, la portata e l'applicazione delle misure di conservazione, fissandone i requisiti anche al fine di permettere agli interessati di averne contezza e di poter proteggere i propri dati. Successivamente, rispetto alle condizioni sostanziali che la normativa nazionale deve soddisfare, la CGUE afferma che, per quanto esse possano variare in funzione delle misure adottate, la conservazione deve rispondere a criteri oggettivi, in base a un rapporto tra dati da conservare e obiettivo perseguito. Da ultimo, la CGUE specifica che analoghe cautele devono trovare riscontro in merito alla determinazione dei destinatari potenziali delle misure e delle situazioni in cui esse ricevono applicazione, in base a criteri oggettivi, cioè, che circoscrivano

[375] Ibid, para 78.
[376] Ibid, para 89.
[377] Ibid, paras 90-96.
[378] Ibid.
[379] Ibid, paras 97-112.

le situazioni idonee a rivelare la connessione con atti di criminalità grave o con un rischio grave per la sicurezza pubblica.

Per quanto concerne la seconda questione,[380] la CGUE si sofferma nuovamente sul principio di proporzionalità, argomentando come l'accesso ai dati garantito alle autorità nazionali competenti debba avvenire entro i limiti dello stretto necessario e in presenza di norme chiare e precise che ne identifichino i presupposti. Al fine di garantire il rispetto di tale principio, l'accesso delle autorità nazionali ai dati conservati dovrebbe essere subordinato, eccetto il ricorrere di casi d'urgenza, a un controllo preventivo effettuato da un organo giurisdizionale o amministrativo sulla base di una richiesta motivata dall'autorità procedente. Parimenti, enfasi viene data alla necessità che le autorità informino gli interessati dell'adozione delle misure, a partire dal momento in cui la divulgazione di tale informazione non è suscettibile di compromettere le indagini. Da ultimo, la conservazione da parte dei fornitori di servizi di comunicazione elettronica richiede l'utilizzo di misure tecniche e organizzative appropriate che consentano di prevenire abusi e alterazioni all'integrità e alla riservatezza dei dati.

Nel 2018, viene invece pronunciata la sentenza *Ministerio Fiscal* in cui la CGUE chiarisce la nozione di "gravità" del reato capace di giustificare l'accesso ai dati.[381] I giudici risolvono la questione richiamando il rapporto consequenziale tra obiettivo perseguito dalle autorità e gravità dell'ingerenza, già affermato nella pronuncia *Tele2*, secondo cui, sulla base del principio di proporzionalità, solo la lotta alla criminalità connotata dal carattere di gravità legittima un'ingerenza nei diritti alla riservatezza e alla protezione dei dati.[382]

A proposito la Corte evidenzia che, per stabilire quale criterio debba essere utilizzato per determinare la gravità di un reato, è necessario un vaglio preventivo circa la gravità dell'ingerenza.[383] Muovendo infatti dall'assunto che l'accesso alle informazioni che non consentono di conoscere la data, l'ora, la durata e i destinatari delle comunicazioni effettuate, né i luoghi in cui tali conversazioni sono avvenute, vale a dire il solo accesso ai dati sugli abbonati e non anche ai dati sul traffico e sull'ubicazione, debba ritenersi inidoneo a disvelare le abitudini di vita di un determinato soggetto, la CGUE ha reso legittime tutte quelle forme di conservazione dei metadati che si giustificano con l'obiettivo di prevenzione di "reati in

[380] Ibid, paras 114-125.
[381] *Ministerio Fiscal*, para 48.
[382] Ibid, para 54-55.
[383] Ibid, para 55.

generale", senza che trovi applicazione il requisito precedentemente individuato della "gravità" del crimine commesso.[384] Pertanto, qualora l'accesso delle autorità pubbliche a dati personali per ragioni connesse al contrasto della criminalità non comporti un'ingerenza grave nei diritti fondamentali alla riservatezza e alla protezione dei dati, non viene richiesta, ai fini della legittimità dell'accesso e dell'obiettivo perseguito mediante esso, la sussistenza di un reato grave, in applicazione del principio di proporzionalità.[385] Tale iter argomentativo ha portato la Corte ad esimersi dal definire i criteri determinanti la gravità del reato, che non risultavano più necessari avendo riscontrato, nel caso di specie, un'ingerenza non grave.

Con *Ministerio Fiscal*, la CGUE, da una parte, non ha quindi colto l'occasione per armonizzare il concetto di "gravi reati", la cui definizione rimane per il momento nella discrezionalità degli Stati membri.[386] Dall'altra, la scelta limitare l'operatività della clausola della gravità dei reati sulla base di una valutazione discrezionale da parte del giudice da effettuare caso per caso, regime per regime, non sembra essere del tutto compatibile con la riserva di legge imposta tanto dalla Carta all'Art. 52 che dalla CEDU all'Art. 8.[387]

3.2. La *Quadrature du Net* e *Privacy International*: un confronto tra la CGUE e la Corte EDU in tema di *bulk retention* e *bulk interception*

Il rispetto delle limitazioni imposte da *Tele2* si sono presto rivelate di difficile compatibilità con le caratteristiche presentate dalla maggior parte dei regimi imposti dagli Stati membri in materia di *data retention*. In un clima storico di forti tensioni legate alla lotta al terrorismo e alla criminalità organizzata, gli Stati membri erano stati privati di un prezioso strumento per salvaguardare la propria sicurezza nazionale. Come reazione a tale sentenza vengono, dunque,

---

[384] Alessandro Malacarne e Gaia Tessitore, 'La ricostruzione della normativa in tema di data retention e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?' 3 Archivo penale 1, 25.
[385] *Ministerio Fiscal*, paras 60-61.
[386] Sul punto è opportuno segnalare che un rinvio pregiudiziale è stato sollevato in materia: si veda Case C-241/22 Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice <https://curia.europa.eu/juris/showPdf.jsf?text=&docid=261123&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2345814> ultimo accesso 29 settembre 2023.
[387] Veronica Tondi, 'La disciplina italiana in materia di data retention a seguito della sentenza della corte di giustizia UE: il tribunale di Milano nega il contrasto con il diritto sovranazionale' Sistema penale (7 maggio 2021) < https://www.sistemapenale.it/it/scheda/tribunale-milano-22-aprile-2021-data-retention-corte-giustizia?out=print> ultimo accesso 29 settembre 2023.

avviati quattro procedimenti distinti contro le legislazioni nazionali del Regno Unito, della Francia e del Belgio in merito alla legittimità di un obbligo di *retention* generale e indiscriminato imposto ai *service providers*, che vengono riunite dalla CGUE nelle due note sentenze *La Quadrature du Net*[388] ("***LQDN**"*) e *Privacy International*[389] ("***PI**"*), pronunciate dalla Corte di Lussemburgo intorno allo stesso periodo in cui la Grande Camera della Corte EDU ha emesso la sentenza *BBW,* precedentemente analizzata.

Complessivamente, le sentenze di *BBW* , *LQDN* e *PI* sono state accolte in Europa con un certo entusiasmo, venendo definite da diverse organizzazioni per i diritti civili come una "vittoria storica" nella battaglia tra esigenze sicurezza e rispetto dei diritti fondamentali.[390] Sotto questo profilo, è interessante andare a valutare se la protezione garantita dalle due Corti europee sia effettivamente simile e comparabile.

Come punto di partenza, sia in *LQDN* che in *PI*, la CGUE è perentoria nel riaffermare, come regola generale, il divieto, ai sensi del diritto dell'UE, di leggi nazionali che impongano regimi di *data retention* "generale e indiscriminata" dei dati da parte dei *service providers.* È vero che nella sentenza *LQDN*, la CGUE aggiunge un altro tassello al complesso schema di limiti e condizioni consentendo, con le dovute garanzie, la conservazione generale e indiscriminata dei dati relativi al traffico e all'ubicazione in caso di "gravi minacce alla sicurezza nazionale".[391] Tuttavia, tale concessione viene stabilita affermando contestualmente e in maniera cristallina che il carattere eccezionale di tali ipotesi deve essere preservato, e che queste ultime non devono sostituire la regola generale di divieto, ribadita anche in *PI*.

Diversamente, la Corte EDU nella causa *BBW* concorda con la Camera sul fatto che, ai sensi della CEDU, l'intercettazione di massa non è di per sé inammissibile e ribadisce l'ampio margine di apprezzamento di cui godono i governi quando si tratta di scelte politiche in materia di sicurezza nazionale.[392] Dunque, fin dalle prime righe della sua valutazione la Corte EDU si dimostra più indulgente nell'accettare i regimi di intercettazione massiva come inevitabili, basandosi sul semplice presupposto che oggi tali sistemi hanno un ruolo chiave per "identificare

---

[388] Caso C-511/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791.
[389] Caso C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2021] ECLI:EU:C:2020:790.
[390] Si veda, per esempio, 'Mass Surveillance and Snoopers' Charter Human Rights Groups win landmark Mass Surveillance ruling' (25 Maggio 2021 LIBERTY) <https://www.libertyhumanrights.org.uk/issue/human-rights-groups-win-landmark-mass-surveillance-ruling/> ultimo accesso 29 settembre 2023.
[391] *LQDN*, paras 135-137.
[392] *BBW*, paras 322-323.

le nuove minacce" dell'era digitale. Di conseguenza, il nucleo della valutazione si sposta sulla conformità degli Stati contraenti alle c.d. "*end-to-end safeguards"* elaborate dalla Corte EDU.

Da una parte, il risultato dei ragionamenti di entrambe le Corti è similare, vale a dire quello di consentire una "*bulk data retention* o *interception"* al fine di perseguire obiettivi di sicurezza nazionale, pur limitando tale concessione con adeguate garanzie procedurali.[393] Dunque, invece di vietare regimi intrusivi che appaiono, a causa della loro stessa natura indiscriminata, di per sé sproporzionati, o perlomeno di affrontare la questione con argomentazioni sostanziali, la tendenza comune ad entrambe le Corti europee è quella di autorizzare tali sistemi, partendo dal presupposto che il rispetto di una lista di garanzie tecniche e procedurali potrà ripristinare un equilibrio, che tuttavia è stato scardinato proprio *ab origine*. Dall'altra, le diverse premesse poste dalle due Corti rivestono un'importante peso sull'onere della prova che i governi devono sostenere per dimostrare il rispetto di tali garanzie tecniche e procedurali.[394] In aggiunta, occorre notare che la Corte EDU nella causa *BBW* descriva l''intercettazione di massa "come un processo graduale" in cui il grado di interferenza con l'Art. 8 CEDU aumenta progressivamente.[395] In particolare, questa ritiene che sia l'intercettazione e la conservazione iniziale delle comunicazioni e dei relativi dati di comunicazione, che l'applicazione di selettori non costituiscano una "interferenza particolarmente significativa" con il diritto ad una vita privata e familiare,[396] specificando successivamente che la salvaguardia dell'autorizzazione in relazione a tali selettori può essere limitata a identificare a grandi linee solo i tipi o le categorie di selettori da utilizzare.[397] Al contrario, la CGUE non distingue il livello di protezione in base alla fase del trattamento che sta valutando, ma piuttosto considera ogni fase come un'interferenza diversa e separata rispetto ai diritti fondamentali in gioco. Inoltre, mentre l'accesso generalizzato al contenuto dei dati delle comunicazioni è stato considerato dalla Corte di Lussemburgo come una violazione dell'essenza del diritto ad una vita privata e familiare, la Corte EDU, sorprendentemente, non sembra affrontare la questione.

---

[393] Juraj Sajfert, 'The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?' (8 giugno 2021 European Law Blog) <https://europeanlawblog.eu/2021/06/08/big-brother-watch-and-centrum-for-rattvisa-judgments-of-the-grand-chamber-of-the-european-court-of-human-rights-altamont-of-privacy/> ultimo accesso 29 settembre 2023.
[394] Maria Tzanou e , Spyridoula Karyda, 'Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?'<http://dx.doi.org/10.2139/ssrn.3970756> ultimo accesso 29 settembre 2023.
[395] *BBW*, para 325.
[396] *BBW*, para 330.
[397] *BBW*, para 354.

Tenendo conto di tali divergenze, è possibile evidenziare che la CGUE offra, almeno in linea di principio, una maggiore protezione dei diritti fondamentali. Da un lato, la CGUE in *LQDN* continua a classificare l'obiettivo della salvaguardia della sicurezza nazionale come essenziale per la prevenzione e la repressione di attività in grado di minacciare direttamente la società, la popolazione o lo Stato stesso e quindi in grado di giustificare misure che comportano interferenze più gravi con i diritti fondamentali rispetto a quelle che potrebbero essere giustificate da altri obiettivi.[398] Tuttavia, ciò non sembra portare, come nel caso della Corte EDU con le misure di *bulk interception*, ad un'inevitabile accettazione dei regimi nazionali di *data retention* generale e indiscriminata. In altre parole, la sensazione dei cittadini dell'UE di essere costantemente sotto sorveglianza, che viola nella sua essenza il godimento del diritto alla vita privata, rimane ancora, secondo la CGUE, una conseguenza diretta dell'applicazione di sistemi di *retention* indiscriminati e generali, i quali devono quindi, di regola, essere vietati.

Da tutte le considerazioni sin qui mosse, può affermarsi come, senza dubbio, le sentenze *PI* e *LQDN* abbiano il merito di aver risposto a molti quesiti rimasti a lungo aperti a seguito della sentenza *Tele2*.

Una parte della dottrina considera che la direzione principale confermata dalla CGUE resta quella di un rafforzamento della tutela dei diritti fondamentali anche di fronte ad esigenze securitarie, sottolineando come l'ammissibilità circa una *bulk data retention* per scopi di sicurezza nazionale, si traduca semplicemente in una volontà di distanziarsi da una lettura in termini di *trade-off* degli elementi del binomio "sicurezza-diritti fondamentali", che vede cioè nella garanzia dell'uno una inevitabile rinuncia dell'altro.[399]

Altra dottrina sostiene invece che, la *LQDN* rappresenti un passo indietro rispetto al precedente approccio progressivo della CGUE contro i sistemi di sorveglianza di massa.[400] La CGUE ha elaborato una guida pragmatica per gli Stati membri rispetto alle salvaguardie e condizioni a cui tale forma di *retention* dovrebbe essere soggetta.[401] Tuttavia, ciò che sembra mancare è

---

[398] *LQDN*, paras 135-137.

[399] Giulia Formici. 'La data retention saga al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture' (2021) *DPCE Online* 1361, 1373.

[400] Monika Zalnieriute, 'A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence' (4 giugno 2021 Blog of the European Journal of International Law) <https://www.ejiltalk.org/a-dangerous-convergence-the-inevitability-of-mass-surveillance-in-european-jurisprudence/> ultimo accesso 29 settembre 2023.

[401] Maria Tzanou, 'Public Surveillance before the European Courts' (6 aprile 2022 VerfBlog) <https://verfassungsblog.de/os6-courts-surveillance/> ultimo accesso 29 settembre 2023.

un'elaborazione circa le condizioni per l'operatività *ab origine* dell'eccezione. Non sembra infatti particolarmente convincente la gerarchia implicita, che presuppone che l'idea astratta di sicurezza nazionale sia qualcosa di distinto e in qualche modo più significativo della lotta contro i reati gravi, nella misura in cui la prima, a differenza della seconda, possa andare oltre il limite di *Tele2* della *targeted retention*. Non solo i due concetti, se tradotti nella realtà – si pensi ad esempio ai reati di terrorismo e criminalità organizzata – non sembrano così diversi, ma come sottolineato in precedenza, non è ancora possibile trovare una definizione armonizzata di nessuno dei due concetti al livello europeo.

3.3. Il requisito aggiuntivo imposto dalla CGUE: il controllo *ex ante* da parte di un giudice o di un ente amministrativo indipendente

Nella successiva giurisprudenza della CGUE è possibile trovare una specificazione anche circa il secondo quesito posto da *Tele2*. Come accennato, la CGUE in tale occasione aveva affermato che alla luce del fatto che l'accesso ai dati sul traffico e l'ubicazione da parte delle autorità nazionali competenti interferisce in modo significativo con il diritto ad una vita privata e alla protezione dei dati (rispettivamente garantiti agli Artt. 7 e 8 Carta), un provvedimento che autorizzi tale accesso deve essere concesso al solo fine di contrastare i reati gravi, deve rispettare il principio di proporzionalità e deve essere accompagnato da specifiche garanzie procedurali per il soggetto interessato.[402] Pertanto, per garantire che tali condizioni previste dai legislatori nazionali siano effettivamente rispettate e valutate caso per caso, la CGUE ha stabilito in *Tele2*, come requisito aggiuntivo, che un controllo *ex ante* debba essere effettuato con una decisione motivata di un giudice o di un ente amministrativo indipendente.[403]

In *Prokuratuur*,[404] la Corte di giustizia ha poi stabilito un chiaro significativo legame tra l'accesso ai dati sul traffico e l'ubicazione e l'interferenza che tale attività crea in materia di diritti fondamentali, da un lato, e la necessità, dall'altro, che venga coinvolta un'autorità giudiziaria al fine di garantire il diritto ad una tutela giurisdizionale effettiva del titolare dei suddetti dati.

---

[402] Si veda art. 15(1) Direttiva e-Privacy.
[403] *Tele2 Sverige*, para 120.
[404] Caso C-746/18 *Prokuratuur - Conditions d'accès aux données relatives aux communications électroniques* [2021] ECLI:EU:C:2021:152.

Rispetto al requisito dell'indipendenza dell'autorità giudiziaria, la CGUE si era già espressa nel 2018 con l'importante sentenza nota come *Associação Sindical dos Juízes Portugueses*.[405] La Corte in tale occasione aveva fondato il proprio ragionamento partendo dal presupposto che in uno Stato di diritto, come l'UE, dovrebbe essere garantito a tutti i singoli "il diritto di contestare in sede giurisdizionale la legittimità di qualsiasi decisione o di qualsiasi altro provvedimento nazionale relativo all'applicazione nei loro confronti di un atto dell'Unione".[406] Non solo alla stessa CGUE, ma anche alle corti nazionali, è quindi affidato il compito di garantire un'effettiva tutela giurisdizionale.[407] Per garantire tale protezione, è essenziale che tali corti siano indipendenti, vale a dire che non solo debbano agire in piena autonomia senza essere soggette a gerarchie o subordinate a ordini e istruzioni, ma devono anche essere libere da qualsiasi pressione o intervento esterno che possa influenzare la loro decisione.[408]

Come sottolineato dall'Avvocato Generale Pitruzzella,[409] la Corte in *Prokuratuur* ha adottato lo stesso approccio fattuale per definire il concetto di indipendenza rispetto al giudice o all'ente amministrativo indipendente incaricato di effettuare il controllo *ex ante*, elaborando dunque tale concetto alla luce dell'obiettivo specifico che un simile controllo mira a perseguire.[410]

Prendendo in considerazione che un accesso a tali categorie di dati permette "di trarre precise conclusioni sulla vita privata delle persone interessate",[411] l'autorità incaricata di autorizzare *ex ante* tale misura deve "essere in grado di garantire un giusto equilibrio" tra gli interessi pubblici di combattere il crimine e la protezione dei diritti fondamentali del soggetto interessato, che subiscono una significativa limitazione.[412] Dunque l'autorità preposta a tale controllo deve (i) non essere stata coinvolta nella conduzione delle relative indagini e (ii) deve avere una posizione neutrale *vis-à-vis* le parti del procedimento penale.[413] In altre parole, la valutazione della CGUE mira a verificare se la posizione e i compiti assegnati all'autorità siano tali "possa ingenerare dubbi legittimi, nelle persone interessate, riguardo all'impermeabilità dei

---

[405] Caso C-64/16, *Associação Sindical dos Juízes Portugueses contro Tribunal de Contas* [2018] ECLI:EU:C:2018:117.
[406] *Associação Sindical dos Juízes Portugueses*, para 31.
[407] Ibid, para 33.
[408] Ibid, para 44.
[409] Caso C-746/18 *Prokuratuur - Conditions d'accès aux données relatives aux communications électroniques* [2020] ECLI:EU:C:2020:18 Opinione dell'AG Pitruzzella.
[410] *Prokuratuur*, para 54.
[411] *Prokuratuur* para 35.
[412] *Prokuratuur* para 52.
[413] *Prokuratuur* para 54.

procuratori rispetto ad elementi esterni e alla loro neutralità con riferimento agli interessi che si contrappongono", tanto da pregiudicare il diritto in capo a tali persone ad un controllo obiettivo, affidabile ed efficace.[414]

Considerando che tra i suoi compiti, l'ufficio di un pubblico ministero "è tenuto a raccogliere le prove, a valutarne la rilevanza e a trarre conclusioni riguardo alla colpevolezza dell'interessato", il suo ruolo non è compatibile con la neutralità richiesta affinché il controllo *ex ante* garantisca la proporzionalità dell'accesso ai dati.[415] Ciò vale anche qualora la legislazione nazionale conferisca alla suddetta autorità i poteri necessari al fine di verificare sia "gli elementi a carico e quelli a discarico, a garantire la legittimità del procedimento istruttorio e ad agire unicamente in base alla legge ed al suo convincimento".[416] Analogamente, come successivamente specificato in *Commissioner of the Garda An Síochána,* un funzionario di polizia, anche se assistito da un'unità di polizia che gode di "una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale", non possiede comunque lo status di imparzialità e indipendenza dalle autorità investigative, necessario per condurre un controllo obiettivo sulla proporzionalità.[417]

Alla luce della recente giurisprudenza della CGUE appena esaminata, è possibile sostenere che la CGUE ha iniziato a riconoscere le caratteristiche distintive delle prove digitali, fornendo tutele procedurali piuttosto rigide, come una previa autorizzazione giudiziaria da parte di un'autorità che possa garantire un elevato livello di indipendenza, al fine di controbilanciare misure altamente intrusive necessarie per tali prove, come l'accesso a dati sul traffico e sull'ubicazione al fine di combattere "reati gravi".

4. La giurisprudenza della Corte di Giustizia sull'ammissibilità della prova digitale in contesti domestici e *cross-border*

Con l'avvento dell'era digitale, è diventato essenziale garantire l'ammissibilità in uno Stato membro di una prova digitale raccolta in un altro Stato membro: l'attuale frammentato mosaico di norme nazionali porta ad una situazione di incertezza giuridica che, in combinazione con le caratteristiche distintive della prova digitale, non solo rappresenta un potenziale ostacolo al

[414] *Prokuratuur* Opinione dell'AG Pitruzzella, para 106-107.
[415] Ibid, para 124.
[416] *Prokuratuur*, para 56.
[417] Caso C-140/20, *G.D. c Commissioner of An Garda Síochána e altri* [2022] ECLI:EU:C:2022:258, para 111.

raggiungimento di un'efficiente cooperazione transfrontaliera, ma può anche interferire con i diritti fondamentali, in particolare con il diritto alla difesa e il diritto a un'effettiva tutela giurisdizionale, garantiti rispettivamente dagli Artt. 48(2) e 47 Carta.

A tal proposito, nel 2009 è stata introdotta una base giuridica, l'Art. 82(1)(a) TFUE, per armonizzare, nei limiti di quanto necessario per rafforzare l'esercizio del principio del mutuo riconoscimento tra Stati membri, le norme sull'ammissibilità delle prove nei procedimenti penali transfrontalieri. Alla luce di questa nuova competenza attribuita al legislatore europeo, la Commissione ha pubblicato un "*Green Book*", introducendo l'idea di adottare un nuovo strumento unico basato sul principio del mutuo riconoscimento e applicabile a tutti i diversi tipi di prove.[418] Questo strumento mirava a creare un regime che disciplinasse sia l'accesso *cross-border* alle prove che la loro successiva ammissibilità di fronte al giudice nazionale. Secondo la Commissione, la mancanza di norme comuni in materia comportava infatti il rischio che eventuali norme adottate al livello europeo sull'acquisizione *cross-border* di prove funzionassero poi efficacemente solo tra Stati membri con norme nazionali simili sotto il profilo dell'ammissibilità. A tal fine, la Commissione concludeva il documento chiedendo il parere degli Stati membri al fine di verificare se essi avrebbero accolto con favore un eventuale introduzione di norme comuni per la raccolta e ammissibilità delle prove. Tuttavia, gli Stati membri manifestarono fin da subito la loro riluttanza a cedere la propria sovranità in materia di ammissibilità delle prove, basando le loro rivendicazioni sui principi di proporzionalità e sussidiarietà.[419] Non sorprendentemente, nel 2014 non viene infatti colta l'opportunità di introdurre degli standard comuni in tema di ammissibilità della prova quando viene introdotto lo strumento dell'OEI.[420]

Occorre, tuttavia, sottolineare come nel corso degli anni i procedimenti penali digitali transfrontalieri si siano evoluti, non solo aumentando nel numero in modo significativo, ma anche creando nuove sfide in una duplice prospettiva. Dottrina, difensori e organizzazioni non governative evidenziano l'impatto della raccolta della prova digitale in contesti domestici e *cross-border* sui diritti fondamentali. Le istituzioni e le agenzie dell'UE sembrano invece dare

---

[418] Commission of the European Communities, 'GREEN PAPER on obtaining evidence in criminal matters from one Member State to another and securing its admissibility' COM(2009) 624 final.
[419] Balázs Garamvölgyi *et al*, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 eucrim 201, 201.
[420] Martyna Kusak, 'Mutual admissibility of evidence and the European investigation order: aspirations lost in reality' (2019) *ERA Forum* 19.

priorità al raggiungimento di un risultato investigativo efficiente.[421] Nonostante, infatti, sia la Proposta della Commissione che la relazione del Parlamento contenessero delle norme in tema di ammissibilità, non è stato possibile, come evidenziato in precedenza, trovare alcun riferimento in materia nel testo di compromesso per adottare gli Ordini europei di produzione e conservazione. D'altronde, questa opposizione ad armonizzare norme in materia di ammissibilità va inquadrata oggi anche nell'attuale clima di "*mutual distrust*" che sembra regnare tra i governi nazionali sulla conformità di altri sistemi penali nazionali ad adeguate garanzie procedurali e più in generale ai principi dello Stato di diritto.[422] Di conseguenza, alcuni Stati membri ritengono che l'armonizzazione delle norme procedurali penali finirebbe per ridurre gli standard nazionali di protezione delle prove digitali. Questa mancanza di fiducia è amplificata dalla connotazione politica dell'area in questione, dal momento che un vivace dibattito pubblico è solitamente legato sia al ruolo delle prove digitali nei procedimenti penali che alle tipologie di reati spesso oggetto di grandi indagini digitali transfrontaliere, come il terrorismo, la frode o la criminalità organizzata.

Nonostante l'assenza di uno strumento legislativo al livello europeo e malgrado le norme sull'ammissibilità della prova digitale siano quindi regolate dalla legislazione nazionale, la CGUE ha emesso diverse sentenze in cui è stata affrontata la questione dell'ammissibilità e dell'esclusione delle prove digitali raccolte in un contesto domestico, fornendo un'improntante guida per le corti nazionali. Allo stesso tempo, è interessante notare che la CGUE non si sia ancora pronunciata sulla questione quando le prove sono invece raccolte in un contesto transfrontaliero. Tuttavia, di recente è stato posto di fronte alla CGUE una questione pregiudiziale sull'utilizzo come prova nei procedimenti nazionali dei dati digitali raccolti e condivisi nel contesto di un'ampia indagine transfrontaliera.[423]

---

[421] Si veda, ad esempio, Eurojust, 'PRESS RELEASE. Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe' <https://www.eurojust.europa.eu/news/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe> accesso 29 settembre 2023.
[422] Marion Ho-Dac, 'The Principle of Mutual Trust in EU law in the Face of a Crisis of Values' (EAPIL Blog 22 febbraio 2021)<https://eapil.org/2021/02/22/the-principle-of-mutual-trust-in-eu-law-in-the-face-of-a-crisis-of-values/> ultimo accesso 29 settembre 2023.
[423] Decisione del 19 ottobre 2022 – LG Berlin (525 KLs) 279 Js 30/22 (8/22).

4.1. Contesto domestico

Nella giurisprudenza della CGUE sull'ammissibilità ed esclusione delle prove digitali raccolte in un contesto domestico, si possono individuare due linee interpretative, a seconda che il dictum delle sentenze si limiti a consentire alle corti nazionali di ammettere o escludere le prove digitali o se venga imposto dalla CGUE un vero e proprio obbligo in tal senso. Rispetto al primo approccio, questo elaborato esamina i casi *WebMindLicenses*[424] e *Dzivev*[425], concernenti l'ammissibilità di prove digitali raccolte in procedimenti penali in materia di IVA. Per il secondo approccio, vengono invece analizzati i casi *La Quadrature du Net e altri* (*LQDN*) e *Prokuratuur* che, come analizzato in precedenza, riguardano il trattamento dei dati personali nel settore delle comunicazioni elettroniche come previsto dalla Direttiva *e-Privacy*. Le quattro sentenze analizzano il legame tra la questione dell'ammissibilità delle prove digitali e l'osservanza, nell'ambito dell'attuazione del diritto UE,[426] degli Artt. 7, 47 e 48 Carta.

4.1.1. L'esclusione della prova digitale come "possibile rimedio"

Nella decisione *WebMindLicenses*, la CGUE ha riconosciuto che il rispetto della Carta funge da limite all'autonomia procedurale di cui godono gli Stati membri in materia di ammissibilità. Nell'esaminare la raccolta di dati e il loro utilizzo come prove digitali, i giudici nazionali devono assicurarsi che siano rispettate una serie di garanzie prescritte dalla Carta, rimanendo tuttavia liberi di decidere quale rimedio procedurale adottare in caso di una loro violazione. Per giungere a tale conclusione, la Corte fornisce un'importante guida per i giudici nazionale affinché i diritti fondamentali e le garanzie procedurali, previsti dalla Carta, possano dirsi rispettati durante un procedimento penale che preveda la raccolta e l'utilizzo di prove digitali.

In primo luogo, ai sensi dell'Art. 7 Carta, "ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni".

A causa del carattere altamente complesso e tecnico delle indagini digitali, quando si raccolgono i dati non è spesso possibile fare una selezione a priori di ciò che sarà utile per le indagini. Questo porta alla raccolta di una grande quantità di dati che potrebbero o meno essere poi utilizzati come prove, ma che in ogni caso potrebbero giocare un ruolo circa la decisione se

[424] Caso C-419/14, *WebMindLicenses* [2015] ECLI:EU:C:2015:832.
[425] Caso C-310/16, *Dzivev and Others* [2019] ECLI:EU:C:2019:30.
[426] Art. 51(1) Carta.

archiviare o meno un caso. [427] Ad esempio, le autorità investigative in tutto il territorio dell'Unione hanno iniziato ad impiegare il c.d. "*Trojan*", un tipo di *malware* inserito segretamente nei dispositivi elettronici di chi è sottoposto a indagine e che consente di controllare tutte le attività svolte tramite il dispositivo, nonché di videoregistrare tutto ciò che si trova nelle vicinanze dello stesso.[428] Simili strumenti di indagine hanno il potere di interferire significativamente con la vita privata non solo di chi è sottoposto a indagine, ma anche di coloro che entrano in contatto con lui quotidianamente.

Data la natura relativa, le misure investigative digitali nazionali che interferiscono con il diritto ad una vita privata (Art. 7 Carta) sono ammissibili, ma solo se vengono soddisfatte le condizioni di cui all'art. 52(1) Carta. Tali interferenze devono essere previste dalla legge e rispettare l'essenza del diritto ad una vita privata. Inoltre, le limitazioni devono essere giustificate da un obiettivo di interesse generale riconosciuto dall'Unione o dalla necessità di proteggere i diritti e le libertà altrui. Infine, deve essere rispettato il principio di proporzionalità. Sotto questo profilo, la CGUE sottolinea come, nel valutare la necessità di tali misure, in assenza di una preventiva autorizzazione giudiziaria, le corti nazionali debbano valutare se alla persona affetta da tali misure sia stato garantito un controllo giudiziario ex *post*. In altre parole, il soggetto interessato deve essere messo nella condizione di esercitare efficacemente il suo diritto di difesa per contestare sia la "legalità che la necessità" della misura.[429]

In secondo luogo, la Corte stabilisce un legame con il diritto alla difesa, in quanto principio generale del diritto dell'UE.[430] Quando le persone sono affette da una decisione che rientra nel campo di applicazione del diritto UE, devono essere messe in condizione di far conoscere effettivamente di contestare le informazioni su cui le autorità intendono basare la propria decisione, avendo accesso alle prove e avendo diritto di essere ascoltati in merito.[431]

In terzo luogo, affinché sia garantito il diritto ad un ricorso effettivo (Art. 47(1) Carta), l'autorità giurisdizionale che ha il dovere di controllare la legittimità di una decisione di attuazione del diritto UE deve essere in grado di verificare se gli elementi di prova su cui si fonda tale

---

[427] Radina Stoykova 'The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations' (2023) 49 Computer Law & Security Review 1, 2.
[428] Monica Alessia Senor, 'Come funzionano i trojan di Stato? Analisi delle nuove norme e indicazioni operative' <https://www.altalex.com/documents/news/2018/01/22/come-funzionano-i-trojan-di-stato> ultimo accesso 29 settembre 2023.
[429] *WebMindLicenses*, para 78.
[430] *WebMindLicenses*, para 84.
[431] Ibid.

decisione siano stati ottenuti e utilizzati in violazione dei diritti garantiti dal diritto UE e, in particolare, dalla Carta. [432]

Nella sentenza *Dzivev*, la CGUE ha osservato che se la raccolta di prove digitali nei procedimenti penali non è stata conforme a quanto prescritto dalla Carta, i giudici nazionali possono, ma non devono, escludere, sulla base di quanto previsto dalla propria legislazione nazionale, le prove digitali illegalmente raccolte. Le corti nazionali possono prevedere un simile rimedio anche se ''utilizzo di tali prove avrebbe aumentato le possibilità per le autorità nazionali di sanzionare violazioni di obblighi imposti dal diritto dell'Unione.[433]

Il ragionamento della Corte parte dalla premessa che gli Stati membri godono di autonomia procedurale circa l'adempimento degli obblighi imposti dal diritto dell'UE. [434] Tuttavia, tale margine di discrezionalità non esime le corti nazionali dall'osservanza dei diritti fondamentali e garanzie procedurali come previsti dalla Carta, che devono essere rispettati non solo durante il procedimento penale, ma anche durante la fase delle indagini preliminari, dal momento in cui la persona interessata diventa un indagato.[435] Poiché le misure investigative digitali interferiscono con il diritto ad una vita privata (Art. 7 Carta), devono rispettare le condizioni poste dall'art. 52(1). A questo proposito, le prove digitali raccolte, come nel caso in esame, attraverso l'intercettazione di telecomunicazioni autorizzata da un tribunale privo di giurisdizione, non soddisfano tale requisito. [436] Se la legislazione nazionale prescrive come rimedio a tale violazione, come nel caso in esame, l'esclusione delle prove raccolte, la CGUE consente alle corti nazionali di applicare tale norma.[437]

4.1.2. L'esclusione della prova digitale come "rimedio obbligatorio"

Per quanto riguarda la seconda serie di sentenze, vale la pena ricordare che né in *LQDN* né in *Prokuratuur* la questione dell'ammissibilità della prova digitale è stata affrontata direttamente, ma la CGUE ha considerato il problema come implicitamente richiamato dai giudici nazionali nei loro rispettivi rinvii.[438] In entrambe le sentenze, la CGUE parte dalla premessa che, in linea di principio, l'ammissibilità e l'esclusione delle prove è una questione di diritto nazionale.

---

[432] *WebMindLicenses*, para 87.
[433] *Dzivev*, para 41.
[434] *Dzivev*, para 24.
[435] *Dzivev*, para 33.
[436] *Dzivev*, para 38.
[437] *Dzivev*, para 39.
[438] *LQDN*, para 221; *Prokuratuur*, para 41.

Secondo il principio dell'autonomia procedurale, spetta al legislatore nazionale stabilire le norme procedurali, comprese quelle probatorie, per garantire i diritti derivanti dal diritto dell'UE.[439]

Tuttavia, tale autonomia è limitata nella misura in cui vengono rispettati sia il principio di equivalenza che il principio di effettività. Il primo richiede che le norme procedurali sulle prove ottenute in violazione del diritto dell'UE non siano "meno favorevoli" di quelle che regolano situazioni nazionali "equivalenti".[440] Tale valutazione spetta al giudice nazionale. A sua volta, il principio di effettività garantisce che l'esercizio dei diritti conferiti dal diritto dell'UE non sia reso praticamente impossibile o eccessivamente difficile. A questo proposito, la CGUE precisa che l'esclusione delle prove non è l'unico rimedio per perseguire l'obiettivo di evitare che le prove raccolte illegalmente arrechino indebitamente pregiudizio all'imputato. Ad esempio, la ponderazione del suo valore probatorio o un ridimensionamento della pena al momento della decisione possono essere soluzioni alternative.[441] Tuttavia, come risulta da precedente orientamento giurisprudenziale della CGUE, le corti nazionali devono considerare il rischio di violazione del principio del contraddittorio, che ostacola il diritto ad un processo equo, quando viene presa una decisione di esclusione di prove raccolte in violazione delle prescrizioni imposte dal diritto dell'UE. Secondo la CGUE, tale violazione viene riscontrata e le prove devono essere quindi escluse in presenza di tre criteri. In particolare, una corte nazionale che ritenga che (i) una parte non sia in grado di dedurre efficacemente in merito a un mezzo di prova, (ii) che rientra in un settore che esula dalla competenza dei giudici e (iii) può influenzare in modo preponderante la valutazione dei fatti, deve constatare una violazione del diritto a un processo equo ed escludere tale mezzo di prova.[442]

Prima di analizzare le tre condizioni stabilite dalla CGUE, è necessario esaminare come la Corte EDU abbia influenzato il ragionamento della CGUE in queste due sentenze. Entrambe le Corti europee hanno riconosciuto che violazioni di diritti fondamentali e garanzie procedurali durante la raccolta delle prove, o in relazione ad una loro eventuale condivisione in un contesto transfrontaliero, possono ostacolare il rispetto del diritto ad un equo procedimento fino al punto

[439] *LQDN*, paras 222-223; *Prokuratuur*, para 41-42.
[440] *LQDN*, paras 223-224; *Prokuratuur*, para 42.
[441] *LQDN*, paras 223-225; *Prokuratuur*, para 43.
[442] *LQDN*, paras 226-227; *Prokuratuur*, para 44.

che le prove devono essere escluse.[443] La stessa conseguenza può verificarsi anche quando le prove sono raccolte legalmente ma vengono poi utilizzate in un processo in assenza di adeguate garanzie procedurali.[444] Tuttavia, a differenza della CGUE, la Corte EDU ha lasciato un margine di discrezionalità ai giudici nazionali: pur dovendo esaminare il modo in cui le prove sono state ottenute e utilizzate nel procedimento penale, questi rimangono liberi di decidere se l'esclusione di tali prove sia il rimedio per garantire l'equità del procedimento "nel suo complesso".[445] L'unica eccezione, in cui la Corte di Strasburgo ha richiesto l'esclusione obbligatoria, è quando le prove sono state ottenute in violazione di diritti umani assoluti, come il divieto di tortura e di trattamenti inumani garantito dall'Art. 3 CEDU.[446] Pertanto, rispetto all'approccio della Corte EDU, la Corte di Lussemburgo ha deciso di compiere un passo avanti sulla questione, stabilendo un chiaro e indissolubile legame tra il diritto a una tutela giurisdizionale effettiva e l'esclusione della prova, nonostante l'ambito di applicazione di questo rimedio sia stato piuttosto circoscritto dalla Corte.

Le tre condizioni necessarie perché si applichi l'esclusione obbligatoria sono brevemente menzionate e non ulteriormente elaborate dalla CGUE in nessuna delle due sentenze. Ciò sorprende non solo per il potenziale delle dictum delle due decisioni, il cui ragionamento potrebbe essere applicato in futuro a casi al di fuori dello specifico ambito in cui i due giudizi sono state pronunciati. Ma soprattutto, la CGUE fa un esplicito e reiterato riferimento nel suo ragionamento ad un caso precedente, ovvero la sentenza *Steffensen*,[447] il cui contesto differisce significativamente da quello caratterizzante sia *LQDN* che *Prokuratuur*. Questa sentenza non riguardava l'utilizzo di prove digitali in procedimenti penali, ma piuttosto quello di prove scientifiche in procedimenti amministrativi. Inoltre, si tratta di una decisione risalente a quasi 20 anni fa, in un'epoca in cui il processo di integrazione europea e la Carta non svolgevano lo stesso ruolo che hanno oggi. La CGUE aveva affermato in tale occasione che le norme probatorie nazionali dovevano essere conformi ai requisiti imposti dal rispetto dei diritti fondamentali e in particolare al diritto a un processo equo garantito dall'art. 6 CEDU, che, tra

---

[443] John Vervaele, 'Lawful and fair use of evidence from a European Human Rights Perspective' in Fabio Giuffrida and Katalin Ligeti (eds) *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings* (University of Luxembourg 2019), 94.
[444] Ibid.
[445] *A.M. c Italia*, App no 40020/03 (Corte EDU 31 luglio 2012), paras 24-25; *Echeverri Rodriguez*, App no 43286/98 (Corte EDU 27 giugno 2000), 8.
[446] *Ibrahim e altri c Regno Unito*, App nos 50541/08, 50571/08, 50573/08 e 40351/09 (Corte EDU 13 settembre 2016), para 254.
[447] Caso C-276/01, *Joachim Steffensen* [2003] ECLI:EU:C:2003:228.

l'altro, prevede la tutela del principio del contraddittorio.[448] Per elaborare sulle condizioni che avrebbero potuto causare una violazione di tale principio e quindi portare all'esclusione obbligatoria della prova, la CGUE aveva fatto a sua volta riferimento alla sentenza *Mantovanelli*, emessa nel 1997 dalla Corte EDU..[449] In questa decisione, i ricorrenti avevano sostenuto che il principio del contraddittorio fosse stato violato in un procedimento amministrativo, dal momento che non potevano commentare efficacemente su una perizia medica, che era stata considerata dalla Corte come una prova appartenente ad un settore tecnico in cui l'opinione dell'esperto aveva solitamente un valore probatorio decisivo.[450] Date le caratteristiche delle sentenze a cui la CGUE fa riferimento, l'applicazione *mutatis mutandis* di queste condizioni a *LQDN* e *Prokuratuur* non sembra convincente, soprattutto considerando la mancanza di ulteriori approfondimenti da parte della Corte. Sotto questo profilo, nonostante la motivazione piuttosto sintetica, è importante comunque valutare brevemente i due principali criteri stabiliti dalla CGUE alla luce delle caratteristiche distintive della prova digitale e del suo utilizzo nei procedimenti penali.

Per quanto concerne l'impossibilità di una parta di dedurre efficacemente in merito a un mezzo di prova, nei procedimenti penali alle parti viene normalmente garantita la possibilità di contestare le prove, alla luce del principio del contradditorio.[451] Tuttavia, a causa delle particolari caratteristiche della prova digitale, tale condizione potrebbe essere difficile da realizzare. Infatti, affinché il diritto di contestare in merito ad un mezzo di prova sia esercitato "efficacemente", l'imputato deve essere messo nelle condizioni di acquisire una conoscenza sufficiente del caso. Pertanto, entra in gioco l'esercizio del diritto alla *digital discovery*, che come analizzato in precedenza, risulta difficile da garantire quando vengono raccolte enormi quantità di dati con tecniche investigative complesse, che spesso le autorità investigative non sono disposte a divulgare.

Rispetto invece alla necessità che la prova rientri in un settore che esula dalla competenza dei giudici, esaminare le tecniche investigative digitali e verificare l'integrità e affidabilità dei dati raccolti richiede un elevato livello di conoscenza nel campo della *digital forensic*. Di conseguenza, un perito viene tipicamente nominato per accedere ed esaminare le prove digitali

[448] *Steffensen*, paras 71-72.
[449] *Steffensen*, para 77.
[450] *Mantovanelli c Francia*, App no 21497/93 (Corte EDU 18 marzo 1997), para 30.
[451] Ibid.

secondo gli standard della *digital forensics* e il suo parere avrà probabilmente un peso significativo nella valutazione da parte del giudice delle questioni relative all'area di competenza in questione. Pertanto, si potrebbe sostenere che le prove digitali appartengano ad un'area di competenza di cui il giudice non ha "alcuna conoscenza", nel senso che richiedono che il giudice si affidi all'opinione di un esperto e ad una sua perizia tecnica, come spesso accade per le prove che appartengono all'ambito scientifico. Una simile interpretazione di questa condizione sembra essere confermata dalla giurisprudenza precedente citata dalla CGEU nella sentenza *LQDN*.[452]

In conclusione, la massima che può essere dedotta da entrambi i giudizi in esame è che se una parte non ha goduto di una tutela giurisdizionale effettiva, valutata alla luce dei tre criteri citati, la prova deve essere esclusa. Tuttavia, la CGUE ha perso l'opportunità di approfondire il modo in cui le caratteristiche distintive delle prove digitali ottenute ingiustamente o illegalmente hanno un impatto sul diritto alla difesa, così come viene esercitato nel contesto specifico dei procedimenti penali, in cui devono essere presi in considerazione i diversi ruoli e poteri assegnati alla difesa e all'accusa. Inoltre, la CGUE non ha elaborato circa la ragione per cui l'esclusione delle prove debba essere l'unico rimedio applicabile dalle corti nazionali rispetto ad una simile interferenza.[453]

4.2. Contesto transfrontaliero

La CGUE ha emesso alcune sentenze sull'ammissibilità delle prove digitali in un contesto nazionale, in cui è stato stabilito un collegamento con il diritto a una tutela giurisdizionale effettiva. In assenza di un filone giurisprudenziale della CGUE, è importante valutare come tale collegamento opererebbe in un contesto transfrontaliero, tenendo conto delle caratteristiche della cooperazione giudiziaria *cross-border* all'interno dello SLSG. A tal fine, come già accennato, i due principi fondamentali che regolano tale cooperazione tra gli Stati membri sono il principio del mutuo riconoscimento e il principio della fiducia reciproca. Il primo, che implica che nello SLSG la decisione dell'autorità giudiziaria di uno Stato membro deve essere eseguita

[452] Si veda *LQDN*, para 226 e le sentenze ivi citate.
[453] Michele Panzavolta ed Elise Maes, 'Exclusion of evidence in times of mass surveillance. In search of a principled approach to exclusion of illegally obtained evidence in criminal cases in the European Union' (2022) 26(3) The International Journal of Evidence & Proof 199, 205.

al di là dei suoi confini giuridici territoriali, implica il secondo.[454] Una delle conseguenze del principio di fiducia reciproca è che gli Stati membri non possono controllare se gli altri Stati rispettino i diritti fondamentali come garantiti dalla Carta, in quanto devono presumere che un tale livello di protezione venga garantito.[455] Tuttavia, tale presunzione è di natura relativa, il che significa che è possibile una sua confutazione in presenza di "circostanze eccezionali".[456]

Dal momento che non è stata fornita al livello legislativo o giurisprudenziale una definizione univoca per stabilire quando le circostanze possano essere considerate "eccezionali" così da consentire un controllo reciproco del rispetto dei diritti fondamentali, la CGUE ha elaborato su tale requisito, nell'ambito di un importante strumento di riconoscimento reciproco, vale a dire il MAE.[457] A tal proposito, la CGUE ha riconosciuto per la prima volta, nella sentenza pilastro *Aranyosi e Căldăraru*,[458] che si verificano circostanze eccezionali, e di conseguenza la presunzione di fiducia può essere confutata, se sussiste un rischio reale per la persona interessata di essere sottoposta a pene o trattamenti inumani e degradanti, il cui divieto assoluto è sancito dall'art. 4 Carta, a causa delle condizioni di detenzione nello Stato membro di emissione.[459] Successivamente, nella sentenza *LM*, è stato chiesto alla CGUE se anche un rischio reale di violazione del diritto a un processo equo, a causa della mancanza di indipendenza dell'autorità emittente, potesse far scattare la clausola delle "circostanze eccezionali".[460] Un simile dubbio scaturiva dalla constatazione che, a differenza dell'art. 4 Carta, l'art. 47(2) Carta, non abbia natura assoluta. La Corte ha pronunciato in senso favorevole basando il suo ragionamento sul ruolo essenziale svolto dall'indipendenza della magistratura, come garanzia fondamentale del diritto a un processo equo, in una società democratica fondata sullo Stato di diritto.[461]

Più recentemente, la CGUE si è pronunciata sul rapporto tra mutuo riconoscimento, fiducia reciproca e cooperazione giudiziaria anche nel contesto dell'OEI. L'interpretazione della DOEI

---

[454] Valsamis Mitsilegas, 'Mutual recognition, mutual trust and fundamental rights after Lisbon' in Valsamis Mitsilegas *et al* (eds) *Research Handbook on EU Criminal Law* (Edward Elgar Publishing Limited 2016), 150-151.
[455] *Opinione 2/13*, paras 191-92.
[456] Ibid.
[457] Decisione Quadro del Consiglio del 13 giugno 2002 relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (2002/584/GAI) OJ L 190/1.
[458] Casi C-404/15 e C-659/15 PPU, *Aranyosi e Căldăraru* [2016] ECLI:EU:C:2016:198.
[459] Ibid, para 183.
[460] *LM*, para 34.
[461] *LM*, paras 48-55.

ha infatti presto dato origine a un numero crescente di sentenze della CGUE, che ha dunque colto l'occasione per approfondire le conseguenze dell'inosservanza dei diritti fondamentali garantiti dalla Carta. In particolare, in *Gavanozov II*, il giudice del rinvio aveva sollevato due principali questioni preliminari in relazione all'art. 14(1) DOEI, ai sensi del quale gli Stati membri devono garantire che contro le misure investigative indicate nell'OEI possano essere esperiti rimedi equivalenti a quelli disponibili in un caso nazionale analogo, e all'interpretazione di questa disposizione alla luce dell'art. 47 Carta. In primo luogo, la CGUE ha riconosciuto che se l'esecuzione di un OEI può interferire con i diritti fondamentali del soggetto interessato, come le perquisizioni e i sequestri digitali oggetto dell'ordine nel caso di specie, l'interessato deve essere in grado di esercitare il proprio diritto ad un ricorso effettivo contro tale ordine, come garantito dall'art. 47(1) Carta. Affinché tale diritto possa essere esercitato in modo effettivo, spetta allo Stato membro di emissione garantire che le persone interessate dalle misure investigative oggetto dell'OEI dispongano di un mezzo di ricorso dinanzi ad un organo giurisdizionale nazionale che consenta loro di contestare la necessità e la regolarità di tale OEI, quantomeno rispetto alle ragioni di merito per cui è stato emesso l'OEI.[462] In secondo luogo, la CGUE è giunta alla conclusione che qualora lo Stato membro emittente non preveda alcun rimedio per poter impugnare tali aspetti dell'OEI, tale mancanza impedisca l'attivazione del meccanismo di riconoscimento reciproco per tale Stato membro. In altre parole, quando in uno Stato membro si verifica una violazione sistematica del diritto ad un ricorso effettivo garantito dall'Art. 47(1) Carta, tale violazione esclude la possibilità che il riconoscimento reciproco venga attuato e vada beneficio di tale Stato membro.[463]

Facendo un confronto con la giurisprudenza sul MAE, si può affermare che con questa sentenza la CGUE ha fatto un passo avanti per quanto riguarda il ruolo della fiducia reciproca e la protezione dei diritti fondamentali. Sia in *Aranyosi e Căldăraru* che in *LM*, la Corte ha identificato il mancato rispetto dei diritti fondamentali come un ostacolo al riconoscimento reciproco, innescando una confutazione della presunzione di fiducia reciproca. In *Gavanozov II*, la Corte è giunta all'ulteriore conclusione che il rispetto dei diritti fondamentali garantiti dalla Carta, e in particolare del diritto ad una tutela giurisdizionale effettiva (Art. 47 Carta), è

[462] Caso C-852/19, *Gavanozov II* [2021] ECLI:EU:C:2021:902, para 41.
[463] Ibid para 56.

un prerequisito necessario affinché lo Stato membro possa essere considerato parte dello SLSG e del suo sistema di riconoscimento reciproco.

Alla luce di tale filone giurisprudenziale sul rapporto tra la presunzione di fiducia reciproca e presunte violazioni dei diritti fondamentali, e in assenza di norme comuni al livello UE in materia di ammissibilità delle prove, si può sostenere che, quando si tratta di utilizzare in un procedimento penale nazionale prove digitali acquisite in un altro Stato membro, il principio della fiducia reciproca e del mutuo riconoscimento non dovrebbero precludere la possibilità per le corti nazionali competenti di verificare che il suddetto procedimento penale nazionale sia compatibile con la Carta.[464] In particolare, i giudici nazionali dovrebbero essere autorizzati a verificare se l'utilizzo di prove digitali raccolte in un altro Stato membro violerebbe il diritto ad un processo equo, alla luce dei criteri elaborati dalla CGUE in *LQDN* e *Prokuratuur*. Tuttavia, tale valutazione può essere difficile da porre in essere nella pratica, poiché, soprattutto quando si tratta di prove digitali, il giudice potrebbe non avere accesso alle informazioni necessarie per stabilire l'equità dell'intero procedimento, compreso il modo in cui i dati sono stati raccolti.[465]

D'altra parte, quando una corte nazionale deve verificare se la raccolta, la condivisione transnazionale e il successivo uso di prove digitali sono stati conformi alla Carta, entrano in gioco sia il principio della fiducia reciproca sia le caratteristiche distintive delle indagini digitali. Il rischio è che le autorità nazionali competenti acquisiscano prove, illegalmente o non equamente raccolte in un altro Stato membro, con il risultato di "riciclarle", dietro una presunzione di fiducia reciproca. Inoltre, sebbene esista una fiducia reciproca tra le autorità nazionali, la funzione della difesa non è quella di "fidarsi", ma di verificare la legalità delle indagini e di assicurare che i diritti dell'indagato o imputato siano salvaguardati.[466] Tuttavia, a causa di esigenze di "segretezza" ai fini della difesa e sicurezza nazionali e alla luce della maggiore complessità operativa delle indagini transfrontaliere, il diritto della difesa di impugnare efficacemente e tempestivamente le prove digitali è ancora più difficile da garantire nella pratica.

---

[464] Aart de Vries and Rob Widdershoven 'Constitutional Principles and Composite Punitive Enforcement in the EU' in Michiel Luchtman *et al* (eds) *EU Enforcement Authorities - Punitive Law Enforcement in a Composite Legal Order* (Hart Publishing 2023), 61.
[465] Ibid.
[466] Lorena Bachmaier Winter, 'Transnational Criminal Proceedings, Witness Evidence and Confrontation: Lessons from the ECtHR's Case Law' (2013) 9(4) Utrecht Law Review 127, 140.

PARTE SECONDA

LA DIMENSIONE NAZIONALE

Capitolo 3

La prova digitale nel procedimento penale italiano alla luce degli insegnamenti sovranazionali

SOMMARIO:

1. Introduzione

Di fronte alle nuove sfide emerse dall'avvento della prova digitale nel procedimento penale, i vari sistemi giuridici nazionali in Europa hanno adottato disparate soluzioni, perseguendo l'obiettivo di bilanciare le esigenze investigative con i valori costituzionali e le garanzie individuali.[467] Alcune giurisdizioni hanno risposto con l'introduzione di una disciplina *ad hoc* che regolasse le nuove sfide emerse dall'incontro tra il progresso tecnologico con il procedimento penale, mentre altri sistemi hanno cercato di adattare le tradizionali regole procedurali attraverso un'interpretazione di tipo sistematico-evolutivo. Altri ancora hanno adottato una combinazione delle due strategie.

Tuttavia, come fin qui evidenziato, la carenza di una risposta efficace ed uniforme tra gli Stati membri, insieme alla natura *borderless* della prova digitale, hanno messo in luce un'impellente necessità di costruire un quadro giuridico europeo condiviso, avente la capacità di influenzare e guidare la normativa e la giurisprudenza nazionali in materia.[468] In tal senso, la prospettiva sovranazionale ha significatamene inciso, seppur spesso con qualche ritardo, sul contesto del procedimento penale italiano, sotto un profilo sia legislativo che giurisprudenziale.

Questo Capitolo illustra come il panorama normativo italiano in materia sia stato modificato in risposta alle disposizioni e alla giurisprudenza sovranazionali, esaminate nei due Capitoli precedenti.

[467] Burkhard Schafer e Stephen Mason, 'The characteristics of electronic evidence' in Stephen Mason e Daniel Seng (eds) *Electronic evidence* (quarta edizione, OBserving Law – IALS Open Book Service for Law 2017), 18.
[468] Sara Conti, 'La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia' (2015) 24 Informatica e diritto 153, 153-154.

2. L'acquisizione e l'ammissibilità della prova digitale entro i confini nazionali: la legge 48/2008 di ratifica della Convenzione di Budapest

Sotto il profilo procedurale penale, la legge 48/2008,[469] di ratifica della Convenzione di Budapest, ha segnato un importante passo verso l'adeguamento della normativa italiana alle novità della realtà digitale e agli standard europei in materia, introducendo per la prima volta una disciplina specifica in tema di acquisizione, conservazione ed utilizzo della prova digitale. Adottando il nuovo approccio stabilito dalla Convenzione di Budapest in risposta al ruolo cruciale assunto dalla prova digitale anche nelle indagini aventi ad oggetto i c.d. reati comuni, la legge 48/2008 si svincola dal ristretto campo della "criminalità informatica", superando la datata premessa che la prova digitale costituisca strumento di rilevanza esclusivamente per l'accertamento dei reati informatici.[470] Allo stesso tempo, la *ratio* sottesa alla riforma del 2008 lungi dall'essere legata esclusivamente ad un'esigenza di mero adempimento degli impegni internazionali assunti.[471] L'obbligo pattizio ha piuttosto creato l'occasione per poter rispondere al livello legislativo ad una serie di criticità emerse nella pratica e da tempo sottolineate in dottrina. In particolare, la legge 48/2008 registra il tentativo di innovare le norme nazionali in materia, con una duplice finalità.[472] Da una parte, il legislatore ha voluto fornire una soluzione alternativa agli sforzi ermeneutici di adattare i tradizionali mezzi di ricerca della prova all'inedita natura della prova digitale. Dall'altra, si è voluto creare un punto di contatto tra l'impianto codicistico e quell'insieme di norme tecniche appartenenti alla disciplina della *digital forensic*,[473] fino a quel momento lasciata al dominio assoluto dei tecnici del settore.[474]

Nonostante le promettenti premesse, sotto numerosi profili la riforma del 2008 rappresenta un'occasione mancata per il legislatore nazionale. Come approfondito nei paragrafi seguenti,

---

[469] Legge 18 marzo 2008, n. 48.
[470] Alessia Ester Ricci, 'Digital evidence, sapere tecnico-scientifico e verità giudiziale', in Carlotta Conti (ed), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi* (Giuffrè, Milano, 2011) 343.
[471] Luca Luparia, 'La ratifica della Convenzione Cybercrime del Consiglio d'Europa' (2008) 6 Criminalità informatica 696, 717.
[472] Ibid.
[473] Come evidenziato in, Maria Angela Biasiotti *et al* (eds), *Trattamento e scambio della prova digitale in Europa*, (Edizioni scientifiche italiane 2016): tale disciplina fa parte delle scienze forensi e si occupa "dell'applicazione di metodi scientifici e di tecniche di investigazione dei reati ed in particolare dell'acquisizione, conservazione, analisi e presentazione di prove contenute in un crescente numero di dispositivi elettronici e digitali".
[474] Luca Luparia, 'La ratifica della Convenzione Cybercrime del Consiglio d'Europa' (2008) 6 Criminalità informatica 696, 717.

la novella si fa merito di aver "canonizzato" i mezzi di ricerca della prova digitale, fino a quel momento considerati atipici, fornendo una regolamentazione specifica che ha posto l'accento sull'esigenza di integrità e genuinità della prova digitale.[475] Tuttavia, invece di creare strumenti *ex novo* che rispondessero alle caratteristiche inedite della prova digitale, il legislatore ha optato per la soluzione di emendare i vecchi istituti,[476] ponendo in essere un'operazione di pedissequa traduzione del dettato sovranazionale ed evitando di toccare invece i temi più controversi e discussi in materia.[477] La scelta di ridurre al minimo la portata innovatrice dell'intervento, probabilmente influenzata dall'allora caduta dell'esecutivo e repentina chiusura dell'attività parlamentare,[478] ha comportato una duplice conseguenza. Da una parte, la decisione di conservare la tradizionale distinzione tra accertamento, ispezione, sequestro e perquisizione, ha creato nuove difficoltà interpretative legate all'inquadramento di una determinata attività operativa nell'una o nelle altre fattispecie previste dal codice, con evidenti conseguenze in termini di disciplina e garanzie applicabili.[479] Dall'altra, la riforma ha interessato solo i mezzi di ricerca della prova digitale c.d. *offline*, caratterizzati dal cogliere il dato digitale nella sua staticità, vale a dire conservato in un server o supporto informatico.[480] Rispetto ai mezzi di ricerca della prova c.d. *online*, non conoscibili dall'indagato e che colgono il dato digitale nel suo fluire, questi non hanno ricevuto particolare attenzione da parte del legislatore sovranazionale, e pertanto non saranno oggetto di ulteriore analisi ai fini di questo elaborato.

2.1. Le nozioni di dato, sistema e documento informatico

Come già evidenziato al Capitolo 1, la Convenzione di Budapest non fornisce una definizione di prova digitale, operando invece una distinzione tra i concetti di "sistema informatico" e "dato informatico". Il primo viene definito come una o più apparecchiature interconnesse e collegate, che compiono, in base ad un programma, l'elaborazione automatica di dati.[481] Il "dato informatico" s'identifica invece in "una qualunque presentazione di fatti, informazioni o

[475] Paolo Tonini e Carlotta Conti (eds), *Manuale di Procedura Penale* (Giuffrè editore 2021), 372.
[476] Si vedano gli artt. 8,9 e 10 legge 48/2008.
[477] Luca Luparia, 'La ratifica della Convenzione Cybercrime del Consiglio d'Europa' (2008) 6 Criminalità informatica 696, 718.
[478] Ibid.
[479] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016), 7.
[480] Ibid.
[481] Art.1(a) Convenzione di Budapest.

concetti in forma suscettibile di essere utilizzata in un sistema computerizzato".[482] Una simile precisazione tra "contenitore" e "contenuto" lungi dall'avere una rilevanza meramente formale, producendo, importanti conseguenze anche sul piano sostanziale in tema di individuazione ed attuazione di tutta una serie di garanzie per la persona i cui diritti subiscono delle limitazioni. Per tale ragione, è importante chiarire, in via preliminare, come il legislatore e la giurisprudenza abbiano recepito e adattato tale distinzione al livello nazionale.

Se ad oggi è pacificamente riconosciuto nel nostro ordinamento il valore autonomo al livello probatorio del dato digitale, indipendentemente dai supporti in cui tale elemento è incorporato, non sempre la distinzione è stata chiara al livello sia legislativo che giurisprudenziale.[483] Sul piano normativo, prima dell'entrata in vigore della legge 48/2008, coesistevano due differenti definizioni di "documento informatico". Il primo riferimento risale al 1993,[484] in cui è stata fornita una nozione di "documento informatico", quale "supporto" contente dati. Nel 2005, il codice dell'amministrazione digitale ha identificato il "documento informatico" nella "rappresentazione" informatica di un fatto.[485] Le due nozioni sono rimaste in vigore contemporaneamente fino alla legge 48/2008, che ha abrogato la disposizione del 1993, prediligendo la nozione di "rappresentazione". Allo stesso tempo, il legislatore del 2008, consapevole dell'immaterialità delle prove digitali, ha ampliato l'oggetto delle norme in materia di mezzi di ricerca della prova attraverso l'inserimento di espressioni che rimandano ad operazioni connesse a "dati, informazioni e programmi informatici" incorporati su "supporti informatici"; e ancora, nel descrive l'ipotesi di sequestro presso i *service providers*, ha distinto l'atto di sequestro dalla materialità della cosa, prevedendo la prelevazione dei dati indipendentemente dalle sorti del dispositivo in cui siano contenuti. Simili emendamenti hanno mostrato di aver recepito la differenza tra "dato-contenuto" e "supporto-contenitore", il quale di per sé risulta spesso irrilevante al livello probatorio. Nonostante un simile passo in avanti sul piano legislativo sovranazionale e domestico, come in seguito analizzato in materia di sequestri digitali, le corti nazionali hanno invece per lungo tempo continuato a negare un valore probatorio autonomo al dato digitale, superando solo recentemente un simile orientamento.

---

[482] Art. 1(b) Convenzione di Budapest.
[483] Paolo Tonini, 'L'evoluzione delle categorie tradizionali: il documento informatico' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1506-1507.
[484] Art. 491-bis codice penale., inserito dalla Legge 23 dicembre 1993 n. 547.
[485] Art. 1.1 lett. p), Decreto legislativo 7 marzo 2005, n. 82.

2.2. L'introduzione delle *best practices* nelle indagini informatiche

In ottemperanza al dettato della Convenzione di Budapest, la legge 48/2008 ha stabilito in tema di perquisizioni, ispezioni e sequestri di sistemi o supporti informatici una serie di importanti garanzie.[486] L'introduzione di disposizioni che non si limitino a prevedere solo la possibilità di perquisire, ispezionare o sequestrare dati e sistemi informatici, ma che indichino anche "in che modo" tali misure investigative debbano essere poste in essere, evidenzia una chiara intenzione legislativa.[487] Tale novità traduce la volontà di introdurre nell'ambito delle indagini informatiche le c.d. *best practices*, vale a dire tecniche e procedure volte a preservare l'integrità e la genuinità del dato digitale.[488] Al fine di raggiungere un simile risultato è necessario porre in essere una catena di custodia (la c.d. *chain of custody*), vale a dire documentare ogni passaggio del procedimento di acquisizione e di analisi dei dati, attraverso l'osservazione di specifiche accortezze tecniche.[489] L'istituto della catena di custodia, di importazione statunitense, non ha tuttavia conosciuto una vera e propria codificazione nell'ordinamento italiano, rimettendo nelle mani della giurisprudenza e della dottrina l'arduo compito di ricostruire in via ermeneutica il sistema.[490]

In primo luogo, il legislatore nazionale con la legge 48/2008 ha frammentato i passaggi necessari al fine di garantire una catena di custodia in varie disposizioni codicistiche, fornendo determinate garanzie solo per alcuni mezzi di ricerca della prova digitale.[491] In particolare, quando vengono poste in essere ispezioni o perquisizioni disposte dall'autorità giudiziaria (artt. 244.2 e 247.1-bis codice di procedura penale ("**cpp**")) o perquisizioni e sopralluoghi da parte della polizia giudiziaria (artt. 352.1-bis e 354.2 cpp), vengono sanciti (i) il dovere di conservare inalterato il dato informatico originale nella sua genuinità e (ii) il dovere di impedire l'alterazione successiva del dato originale. Se viene invece effettuato un sopralluogo da parte della polizia giudiziaria o un sequestro da parte dell'autorità giudiziaria, ma esclusivamente in relazione ai dati acquisiti dai fornitori di servizi (artt. 254-bis cpp), è necessario (i) formare una

---

[486] Paolo Tonini e Carlotta Conti (eds), *Manuale di Procedura Penale* (Giuffrè editore 2021), 372.
[487] Stefano Aterno, 'La Convenzione di Budapest del 2001 e la l. n. 48/2008' Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1554-1555.
[488] Luca Lupária e Giovanni Ziccardi, LE "MIGLIORI PRATICHE" NELLE INVESTIGAZIONI INFORMATICHE: BREVI CONSIDERAZIONI SULL'ESPERIENZA ITALIANA.
[489] Laura Bartoli e Cesare Maioli, 'La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti' (2015) 1-2 Informatica e diritto 139, 140.
[490] Paolo Tonini e Carlotta Conti (eds), *Manuale di Procedura Penale* (Giuffrè editore 2021), 373.
[491] Ibid.

copia che assicuri la conformità del dato informatico acquisito rispetto a quello originale, (ii) effettuare la copia su un supporto informatico "adeguato" e (iii) assicurare la non modificabilità della copia del documento informatico. Infine, è prevista in via facoltativa e solo per il sequestro (art. 260 cpp) la garanzia di installare sigilli informatici sui documenti acquisiti.

In secondo luogo, ad un approccio poco sistematico si aggiunge una chiara scelta legislativa di focalizzarsi più sul risultato che sul metodo: vengono infatti adottate una serie di "norme penali in bianco", che fissano degli obiettivi senza, tuttavia, fornire indicazioni circa le migliori tecniche e procedure da adottare.[492] L'attuazione nella pratica dei principi di *digital forensic* fissati dal legislatore è stata dunque affidata agli strumenti di *soft law*, che per la loro maggiore flessibilità risultano più adatti a rispondere ad un duplice ordine di limitazioni in materia.[493] Da una parte, le migliori procedure devono mutare di pari passo con la tecnologia, sia rispetto al suo rapido progresso che alle caratteristiche dell'*habitat* tecnologico caratterizzante la *scena criminis*.[494] Dall'altra, è necessario considerare una "variabile soggettiva", legata alla diversità degli operatori e degli obiettivi investigatori.[495]

Sotto questo profilo, come evidenziato nei Capitoli precedenti, al livello europeo, sono state adottate importanti linee guida che costituiscono la "traduzione operativa", anche se priva di valore giuridico e vincolatività, delle generiche garanzie adottate al livello legislativo.[496] L'adozione di simili protocolli investigativi riveste sicuramente un ruolo fondamentale nel guidare la polizia e le autorità giudiziarie nelle indagini e per la difesa al fine di una partecipazione più "consapevole" al contradditorio in fase investigativa o processuale. Ma, *in primis*, l'adozione di protocolli che traducano gli obiettivi legislativi in linee guida sono d'ausilio per l'organo giudicante al fine di verificare, in un'ottica di libera valutazione della prova ex art. 192 cpp, il percorso di acquisizione del dato digitale, effettuando un controllo su tutta una serie di aspetti caratterizzanti la qualità dell'indagine come, ad esempio, la reputazione

---

[492] Carlotta Conti, 'La prova informatica e il mancato rispetto delle *best practices*: lineamenti sistematici sulle conseguenze processuali' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1537.
[493] Laura Bartoli and Giulia Lasagni, 'The Handling of Digital Evidence in Italy' in Michele Caianiello and Alberto Camon (eds) *Digital Forensic Evidence Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Wolters Kluwer 2021), 92.
[494] Alessandra Testaguzza 'Il sequestro di dati e sistemi' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1646.
[495] Ibid.
[496] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016), 36.

scientifica del programmatore di un certo tipo di *software* o la qualifica e le performance dell'operatore di polizia giudiziaria.[497] A titolo esemplificativo, in Germania vengono adoperate al livello nazionale per le indagini informatiche le *IT FORENSIK BSI GUIDELINES.*[498] Queste linee guida hanno stabilito una metodologia completa per garantire la sicurezza dei dati raccolti come prova, che può quindi essere facilmente aggiornata con i nuovi sviluppi tecnologici.[499] Tuttavia, se si guarda all'ordinamento italiano nessuno strumento di *soft law* si è affermato al livello nazionale così da concretizzare i principi introdotti nel 2008 in linee guida e protocolli riconosciuti in tutte le aule penali di tribunale.[500] In particolare, ad un'iniziale lacuna normativa in materia, si è poi registrato un susseguirsi di autonome iniziative promosse dai diversi organismi investigativi,[501] che hanno portato all'adozione di numerosi *standard* in materia, ma divergenti tra di loro.

2.3. La ricerca della prova digitale: le ispezioni e le perquisizioni informatiche

Un primo gruppo di disposizioni introdotte dalla legge 48/2008 è dedicato all'individuazione degli elementi probatori utili. Tradizionalmente, ex art. 244 cpp l'attività di *inspicere* si sostanzia nel limitarsi ad esaminare situazioni legate alla persona, al luogo o alle cose, al fine di trarre e accertare tracce o altri effetti materiali del reato;[502] diversamente, l'attività di *perquirere* ex art. 247 cpp si caratterizza per una ricerca attiva, avente la finalità di rinvenire ed assicurare il corpo del reato o delle cose ad esso pertinenti, le quali si presumono nascoste in un determinato luogo.[503] La novella ha emendato entrambi gli istituti: il nuovo secondo comma

---

[497] Luca Lupária e Giovanni Ziccardi, LE "MIGLIORI PRATICHE" NELLE INVESTIGAZIONI INFORMATICHE: BREVI CONSIDERAZIONI SULL'ESPERIENZA ITALIANA.

[498] Le linee guida sono disponibili solo in versione originale al seguente link: Bundesamt für Sicherheit in der Informationstechnik 'Leitfaden, IT-Forensik" Version 1.0.1 (März 2011)' <bsi.bund.de/SharedDocs/Downloads/DE/BSI/CyberSicherheit/Themen/Leitfaden_ITForensik.pdf?__blob=publicationFile&v=2.> ultimo accesso 29 settembre 2023.

[499]Sabine Gless e Thomas Wahl, 'The Handling of Digital Evidence in Germany' in Michele Caianiello and Alberto Camon (eds) *Digital Forensic Evidence Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Wolters Kluwer 2021), 64.

[500] Laura Bartoli and Giulia Lasagni, 'The Handling of Digital Evidence in Italy' in Michele Caianiello and Alberto Camon (eds) *Digital Forensic Evidence Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Wolters Kluwer 2021), 92.

[501] Si vedano gli standard adottati dalla Guardia di Finanza, dall'arma dei Carabinieri e così via.

[502] Giorgio Spangher and Luca Della Ragione, *Codice di procedura penale ragionato* (Neldiritto Editore 2021), commento all'art. 244 cpp.

[503] Ibid, commento all'art. 247 cpp.

dell'art. 244 cpp prevede che l'ispezione possa essere disposta dall'autorità giudiziaria anche in relazione a "sistemi informatici o telematici", mentre ex art. 247.1-bis cpp può essere disposta perquisizione dall'autorità giudiziaria anche se si ha "fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza (…)". In aggiunta, ex art. 352 cpp, il legislatore del 2008 ha previsto che in casi di flagranza di reato o se sussistono altre condizioni indicate nel codice, anche gli ufficiali di polizia giudiziaria hanno il potere di perquisire sistemi informatici o telematici, anche se protetti da misure di sicurezza, qualora sussista "fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi".

Sebbene il legislatore abbia deciso di emendare i vecchi istituti, mantenendo una distinzione tra le due operazioni, è opportuno segnalare come, nel contesto informatico, il confine tra le attività di ispezione e perquisizione tendano ad affievolirsi, quasi fino a diventare impercettibili.[504] Del resto il *discrimen* tra ricerca c.d. attiva e mera osservazione viene meno se anche la semplice osservazione di un *file* implica comunque l'accesso al dispositivo di memorizzazione, almeno per verificarne la presenza e, potenzialmente, per visualizzarne il contenuto.[505] La difficoltà pratica di distinguere tra le due operazioni di ispezionare e perquisire nell'ambiente virtuale ha portato all'affermarsi di due orientamenti in dottrina al fine di tracciare una più chiara linea di demarcazione tra i due istituti. Secondo parte della dottrina, l'attività ispettiva nel contesto informatico si sostanzierebbe nell'osservazione solo di *files* non protetti da *password*, mentre si parlerebbe di perquisizione ogniqualvolta la lettura di un *file* richieda procedure di autenticazione specifiche.[506] Altri studiosi sottolineano invece come l'attività ispettiva in ambiente informatico dovrebbe limitarsi ad osservare il sistema informatico, descrivendolo nei suoi particolari, rivelando, ad esempio, la presenza di periferiche collegate o la presenza di *software* in funzione.[507] Una simile attività troverebbe oggi una sua utilità alla luce della nuova complessità caratterizzante la *scena criminis* informatica, non più rappresentata solamente dal

[504] Stefano Aterno, 'Modifiche al titolo III del libro terzo del codice di procedura penale' in Giuseppe Corasaniti e Giovanna Corrias Lucente (eds) *Cybercrime, responsabilità degli enti, prova digitale* (CEDAM 2009), 203 e ss.
[505] Cesare Maioli e Elisa Sanguedulce, 'I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008' (Altalex 7 maggio 2012) < https://www.altalex.com/documents/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008> ultimo accesso 29 settembre 2023.
[506] Ibid.
[507] Ibid.

personal computer, ma anche da altri dispostivi quali *smartphones* o *tablet*, spesso interconnessi tra loro.[508]

In ogni caso, anche una mera esplorazione a fini ispettivi di un sistema informatico per individuare dati e tracce pertinenti al reato inevitabilmente comporta l'alterazione dei dati di sistema o, almeno, la modifica dei c.d. metadati.[509] La conferma di ciò risiede nella scelta del legislatore di prevedere sia per le ispezioni che per le perquisizioni informatiche, ad opera dell'autorità o della polizia giudiziaria, un'importante garanzia: nel disporre tali mezzi di ricerca devono essere adottate misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. Da qui emergono due importanti conseguenze. In primo luogo, il legislatore del 2008 ha qualificato tanto le attività di *inspicere* che di *perquirere* i sistemi informatici come operazioni in grado di alterare in maniera irreversibile lo stato e il contenuto del dispositivo ispezionato o perquisito.[510] In secondo luogo, viene riconosciuta la natura fragile e volatile del dato digitale, che conseguentemente impone l'adozione di cautele sin dal primo contatto delle autorità o della polizia giudiziaria con il materiale informatico.[511]

2.4. La raccolta e la custodia della prova digitale: la disciplina dei sequestri informatici

Un secondo gruppo di disposizioni è dedicato alla tematica del sequestro probatorio, operazione disposta dall'autorità giudiziaria con decreto motivato volta ad assicurare il corpo del reato o le cose pertinenti al reato al procedimento per finalità probatorie.[512]

Per quanto concerne le novità introdotte in materia, in primo luogo, la novella ha introdotto ex novo una norma di cui all'art. 254-bis cpp, rubricato "Sequestro di dati informatici presso fornitori di servizi, informatici, telematici e di telecomunicazioni". La norma ha una forte portata innovatrice in quanto nel descrivere l'ipotesi di sequestro presso i *service providers* separa l'atto dalla corporeità della cosa, con l'intento non solo di riconoscere l'autonomia del

---

[508] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016), 57.
[509] Ibid.
[510] Luca Luparia, 'La ratifica della Convenzione Cybercrime del Consiglio d'Europa' (2008) 6 Criminalità informatica 696, 719.
[511] Laura Bartoli e Cesare Maioli, 'La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti' (2015) 1-2 Informatica e diritto 139, 141.
[512] Giorgio Spangher and Luca Della Ragione, *Codice di procedura penale ragionato* (Neldiritto Editore 2021), commento all'art. 253 cpp.

dato, ma anche di garantire ai *providers* la continuità dei propri servizi.[513] In particolare, la disposizione prevede che qualora l'autorità giudiziaria disponga il sequestro presso i *service providers* "dei dati da questi detenuti, compresi quelli di traffico e di ubicazione" e decida di disporne acquisizione mediante copia, deve porre in essere una serie di *best practices*: occorre un supporto adeguato, una procedura che assicuri la conformità del duplicato rispetto all'originale e la sua immodificabilità, ed infine è posto in capo al fornitore del servizio l'ordine di conservare e proteggere adeguatamente i dati originali.

In secondo luogo, la legge 48/2008 ha riformulato il primo comma dell'art. 254 cpp in materia di sequestro di corrispondenza. Questo istituto prevedeva una serie di norme speciali volte a conciliare la tutela della libertà e la segretezza della corrispondenza, garantite dall'art. 15 Cost. e dall'art. 8 CEDU, con l'esigenza di accertamento del reato. L'intervento del 2008 ha adeguato le relative disposizioni ai mutamenti intervenuti nei servizi di corrispondenza per effetto dell'avvento dell'era digitale.

In particolare, rispetto alla categoria dei fornitori di servizi di corrispondenza, presso i quali è consentito procedere a sequestro agli uffici postali e telegrafici, la novella ha inserito le categorie dei "fornitori di servizi telematici e di telecomunicazione". Al secondo comma viene emendata la riserva di giurisdizione, già stabilita dal legislatore per il sequestro di corrispondenza "tradizionale", alla luce della natura speciale della norma. Quando è un ufficiale di polizia a procedere al sequestro, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza non solo senza aprirli, ma anche senza "alterarli", evitando così di prendere conoscenza del loro contenuto. La *ratio* dietro l'inserimento di una garanzia di non alterabilità, che si aggiunge al già previsto divieto di apertura, risiede nella natura particolarmente delicata della corrispondenza elettronica: non solo questa è altamente suscettibile di subire alterazioni, ma, a differenza della corrispondenza tradizionale, non è sigillata in una busta, "viaggiando" aperta ed essendo conoscibile nel suo oggetto anche semplicemente aprendo il file che la contiene.[514]

Rispetto allo scopo di applicazione materiale del mezzo di ricerca, si aggiungono agli oggetti di corrispondenza sottoponibili a sequestro, le forme di comunicazioni elettroniche, rientrando

---

[513]Alessandra Testaguzza 'Il sequestro di dati e sistemi' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1646.
[514] Stefano Aterno, 'La Convenzione di Budapest del 2001 e la l. n. 48/2008' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1569.

nel novero della norma, in quanto materiale sequestrabile, anche la corrispondenza "in corso di spedizione", vale a dire, nel contesto informatico, le comunicazioni elettroniche, attivate dal mittente, ma ancora giacenti presso i *service providers*.[515] Sotto questo profilo, occorre sottolineare come il sequestro della posta elettronica deve essere tenuto distinto dalla captazione da remoto ed in tempo reale del flusso di dati, comprendente anche la posta elettronica stessa, realizzabile però mediante il diverso meccanismo dell'intercettazione telematica, disciplinato dall'art. 266-bis cpp.[516] Allo stesso tempo, rispetto all'acquisizione di messaggi *WhatsApp* e degli sms custoditi nella memoria di un telefono cellulare,[517] così come dei messaggi di posta elettronica memorizzati nell'*account* o nel computer del mittente ovvero in quello del destinatario, e quelli in formato di bozza,[518] la Corte di Cassazione ha precisato che non trova applicazione né l'art. 254 cpp né la disciplina in materia di intercettazioni telematiche, dal momento che tali contenuti hanno natura documentale ex art. 234 cpp.[519] Di conseguenza, in quanto documenti informatici possono essere acquisiti mediante mera riproduzione fotografica o acquisizione del supporto. Sul punto occorre tuttavia segnalare la recentissima sentenza della Corte Costituzionale che ha riconosciuto ai messaggi *WhatsApp* e agli altri messaggi elettronici sopracitati valore costituzionale di corrispondenza, rientrando quindi nella tutela di cui all'art. 15 Cost.[520]

2.5. Le modalità operative del sequestro nel contesto digitale: dalla creazione della copia-clone alla restituzione del bene sequestrato

Il rapporto esplicativo adottato dal Comitato dei ministri del Consiglio d'Europa chiarisce che il termine "sequestrare" significhi, ai sensi della Convenzione di Budapest, "prendere il mezzo fisico sul quale i dati o le informazioni sono registrati oppure fare e trattenere una copia di tali dati o le informazioni".[521] Poiché la misura di sequestro probatorio informatico si riferisce a dati immateriali memorizzati su dispositivi materiali, sulla base della disciplina codicistica le autorità competenti devono adottare ulteriori misure per assicurare i dati, ossia "mantenere

[515] Ibid.
[516] Ibid.
[517] Cass. sez II penale n. 39529 del 1° luglio 2022.
[518] Cass sez IV penale n. 40903 del 28 giugno 2016 e Cass. se. VI penale n. 12975 del 27 aprile 2020.
[519] Cass sez VI penale n. 1822 del 17 gennaio 2020.
[520] Corte Costituzionale n. 170/2023.
[521] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) ETS 185, 32.

l'integrità dei dati", o mantenere la "catena di custodia" dei dati, nel senso che i dati copiati o rimossi devono essere conservati nello stato in cui si trovavano al momento del sequestro e rimanere non alterati durante tutto l'arco temporale del procedimento penale. Da qui è possibile affermare che un importante passaggio nella catena di custodia della prova digitale è la creazione di una copia dei dati presenti sul supporto sequestrato, che sia effettuata garantendo l'integrità e la genuinità dei dati originali. Sebbene il legislatore domestico, al pari del legislatore sovranazionale, non descriva dettagliatamente tale passaggio, il riferimento nelle varie disposizioni alla "conservazione" dei dati e alla loro "non alterazione" sembra richiamare la tecnica del *legal imaging* o *bit stream image*, che permette di cristallizzare lo stato probatorio attraverso la creazione di una copia-clone dei dati conservati all'interno del supporto sequestrato.[522] Ciò permette infatti agli investigatori di cercare successivamente sulla copia i dati rilevanti per l'indagine penale, senza il rischio di alterare i dati originali. Sotto questo profilo, l'art. 8 legge 48/2008 ha modificato il primo comma di cui all'art. 260 cpp in materia di sigilli alle cose sequestrate, estendendo la possibilità di assicurare le cose sequestrate, in relazione alla natura di queste ultime, anche con sigilli di carattere elettronico o informatico, purché idonei a indicare il vincolo imposto ai fini di giustizia. La novella ha specificato poi al secondo comma che quando vengono sequestrati dati, informazioni o programmi informatici, "la copia deve essere realizzata su adeguati supporti, mediante una procedura che assicuri conformità della copia all'originale e la sua immodificabilità", potendo la custodia dell'originale essere disposta anche in luoghi dalla cancelleria o dalla segreteria. Come osservato in dottrina, si è aperta così la strada alla certificazione di conformità tra copia e originale tramite le c.d. *hash functions*.[523] Quando una funzione *hash* viene applicata ai dati digitali, il risultato è chiamato valore *hash.* La funzione *hash* viene utilizzata per certificare che un *file* o la copia di un file non sia stata modificata. *A contrario*, se il *file* è stato alterato in qualche modo, il valore dell'*hash* non sarà lo stesso.[524]

---

[522] Luca Luparia, 'La ratifica della Convenzione Cybercrime del Consiglio d'Europa' (2008) 6 Criminalità informatica 696, 719.
[523] Ibid.
[524] Burkhard Schafer e Stephen Mason, 'The characteristics of electronic evidence' in Stephen Mason e Daniel Seng (eds) *Electronic evidence* (quarta edizione, OBserving Law – IALS Open Book Service for Law 2017), 296. L'*hash* è una funzione univoca che opera in modo irreversibile, in quanto non può essere invertita. Questa funzione è progettata per trasformare un testo di qualsiasi lunghezza in una stringa di lunghezza fissa e relativamente limitata. Tale stringa rappresenta una specie di "impronta digitale" del testo originale. L'impronta utilizza una tecnica crittografica che può essere associata a un singolo file, a un dischetto o all'intero contenuto di un disco rigido.

Sebbene sia la Convenzione di Budapest che la legge 48/2008 abbiano riconosciuto la differente natura del sequestro probatorio digitale rispetto al mezzo di ricerca della prova tradizionale, l'intervento "chirurgico" del legislatore del 2008 ha lasciato inalterate tutta una serie di disposizioni codicistiche dedicate ad assicurare, anche in materia di sequestri probatori, il classico bilanciamento tra esigenze investigative e protezione dei diritti fondamentali. Tale silenzio normativo si è tradotto in un lungo e travagliato sforzo giurisprudenziale nel cercare di adattare tali norme alle peculiarità del contesto digitale e in particolare all'autonomia riconosciuta, al livello legislativo, al dato digitale rispetto supporto fisico in cui viene incorporato. D'altra parte, le indicazioni codicistiche erano e continuano ad essere difficilmente adattabili alle nuove potenzialità della prova digitale.[525] Il "punto di partenza" avrebbe dovuto essere l'art. 258 cpp, che sulla falsa riga della disposizione del codice precedente, si limita a prevedere che qualora l'autorità giudiziaria decida di estrarre copia di atti e documenti sequestrati, venga attribuito il diritto di chi li deteneva legittimamente a farsene rilasciare copia autentica.[526] Ancora, ex art. 257 cpp, l'imputato, la persona a cui le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione possono richiedere un riesame, anche se privo di effetto sospensivo. Al diritto al riesame si aggiunge infine un'ulteriore garanzia, all'art. 262 cpp, in cui viene stabilito un vincolo tra le necessità probatorie e la durata sequestro: quando non è più necessario mantenere il sequestro a fini di prova, le cose sequestrate devono essere immediatamente restituite a chi ne abbia diritto, anche prima della sentenza.

Nella ricostruzione di un simile sforzo interpretativo, è possibile identificare come punto di partenza la nota sentenza *Tchmil*, [527] risalente a poco prima dell'entrata in vigore della legge 48/2008. In tale occasione, le Sezioni Unite avevano confermato un orientamento maggioritario che riconosceva piena autonomia al provvedimento acquisitivo della copia rispetto a quello del sequestro probatorio informatico, qualificando l'estrazione della copia ridotta come mera modalità esecutiva del sequestro. Di conseguenza, in virtù del principio di tassatività delle impugnazioni, l'avvenuta restituzione del bene sequestrato rendeva inammissibili, per sopravvenuta carenza di interesse, la richiesta di riesame del sequestro probatorio e l'eventuale successivo ricorso per cassazione.

---

[525] Laura Bartoli, 'Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature' (2018) 1 Archivio Penale 1, 3.
[526] Ibid.
[527] Sez. Unite sentenza n. 18253 del 7 maggio 2008.

Poco dopo la pronuncia del 2008, entrava in vigore la legge 48/2008. Nonostante l'importante cambiamento avvenuto nel panorama normativo, per lungo tempo la giurisprudenza non ha mutato il suo orientamento. Solo nel 2017,[528] le Sezioni Unite hanno infatti ribaltano il precedente del 2008, prendendo le mosse e richiamando i contenuti proprio della riforma del 2008. In particolare, la Sezione rimettente aveva respinto l'orientamento precedente, sostenendo che, sulla base del contenuto delle disposizioni della legge 48/2008, la caratteristica di "oggetto del sequestro" doveva essere riconosciuta non solo al supporto fisico, ma anche al "dato digitale", in un quanto "la sua riproduzione si risolve in un clone identico ed indistinguibile dall'originale".[529] Di conseguenza, rimanendo i dati informatici, acquisiti mediante copia integrale, sotto sequestro, permaneva, secondo la Sezione remittente, anche una volta restituito il supporto fisico, una perdita autonomamente valutabile per il titolare del dato, venendo meno la "disponibilità esclusiva dell'informazione".[530] Le Sezioni Unite accolgono tale lettura, superando (almeno in parte) il *dictum* della sentenza *Tchmil*.

In primo luogo, la Corte coglie l'occasione per delineare la nozione di sistema informatico, distinguendo tra le sue componenti *hardware* e le sue componenti *software*. Se le prime si riferiscono al complesso di elementi fisici non modificabili quali, ad esempio unità di memoria, il *monitor*, la tastiera, le secondo sono costituite dall'insieme di istruzioni, procedure e programmi necessari per il funzionamento della macchina.[531] Tale distinzione è funzionale al fine di delineare una definizione di "dato o documento informatico" in sé, distinta dalla nozione di supporto in cui il dato o documento vengono incorporati. A sostegno di tale tesi vengono richiamate non solo le nozioni di "sistema informatico", "dato informatico" e "sequestro" previste dalla Convenzione di Budapest, ma anche numerose disposizioni codicistiche modificate dalla legge 48/2008.[532]

Alla luce di tale inquadramento, la Corte afferma che "oggetto del sequestro" può essere non solo il singolo apparato fisico su cui i dati e le informazioni sono registrate, ma anche il dato informatico in esso contenuto.[533] Circa questa seconda ipotesi, la Corte sottolinea, tuttavia, un'importante, ma alquanto opaca, distinzione tra "dato informatico in sé" e dato informatico

[528] Sez. Unite sentenza n. 40963 del 20 luglio 2017.
[529] Ibid, svolgimento del processo para 3.
[530] Ibid,
[531] Ibid, motivi della decisione para 9.
[532] Ibid.
[533] Ibid, para 18.

quale "mero recipiente di informazioni".[534] Nella prima categoria rientra "il dato come cristallizzato nel clone identico all'originale e, perciò, da esso indistinguibile". Il dato-recipiente è invece un atto o un documento che si presenta sotto forma di dato informatico, rendendo possibile distinguere le copie dall'originale, il quale è "rappresentato dal documento elettronico originariamente formato ed univocamente identificabile". Di conseguenza, se oggetto del sequestro è il dato in sé, "la mera restituzione del supporto non può considerarsi come esaustiva restituzione della cosa in sequestro".[535] Diversamente, se il dato viene sequestrato come "mero recipiente" di informazioni allora si applica ancora il *dictum* della sentenza *Tchmil*, ad eccezione del caso in cui il documento "trasferisca il proprio valore anche sulla copia".[536] In tal caso, sopravvive alla restituzione fisica un interesse alla "disponibilità esclusiva del patrimonio informativo". Una distinzione quella tra dato in sé e dato-documento che risulta di difficile comprensione e che, sorprendentemente, non viene poi ulteriormente elaborata e soprattutto menzionata nella massima enunciata dalla Corte.[537] A conclusione del proprio ragionamento, le Sezioni Unite dettano infatti il seguente principio di diritto: "è ammissibile il ricorso per cassazione avverso l'ordinanza del tribunale del riesame di conferma del sequestro probatorio di un computer o di un supporto informatico, nel caso in cui ne risulti la restituzione previa estrazione di copia dei dati ivi contenuti, sempre che sia dedotto l'interesse, concreto e attuale, alla esclusiva disponibilità dei dati".[538]

A supporto di questa tesi, vengono citate alcune decisioni emanate dalla Corte EDU, con cui si è cercato di valorizzare non solo il fattore temporale come criterio per valutare la correttezza di un sequestro, ma anche il diritto alla libertà di espressione di cui all'Art. 10 CEDU, e il diritto al rispetto della vita privata e familiare ex Art. 8 CEDU.[539] Come sottolineato dalle Sezioni Unite, la giurisprudenza europea ha tenuto in considerazione l'inevitabile impatto delle attività investigative che coinvolgono dati sensibili e, in un caso specifico, ha chiaramente sottolineato, riconoscendo la legittimità del procedimento in una situazione di sequestro di commenti e file estratti da computer aziendali, la necessità di garantire un pieno contraddittorio riguardo ai

[534] Ibid.
[535] Ibid.
[536] Ibid, para 19.
[537] Laura Bartoli, 'Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature' (2018) 1 Archivio Penale 1, 12.
[538] Ibid, motivi della decisione para 21.
[539] Ibid, para 20.

documenti acquisiti, nonché la possibilità di impugnare l'atto di rimozione dinanzi a un giudice.[540]

Nonostante il richiamo alla giurisprudenza della Corte EDU, numerosi dubbi sorgono tuttavia circa la costruzione dell'interesse ad impugnare: non solo viene posto in capo al soggetto interessato una sorta di onere probatorio "rafforzato" rispetto a quanto richiesto ex art. 257 cpp, ma la Corte non fornisce ulteriori indicazioni rispetto a quando un simile interesse possa sussistere e ancor prima, in cosa consista l'interesse ad "un'esclusiva disponibilità dei dati".[541] Suddetto interesse sembra evocare i concetti di *privacy* e autodeterminazione informatica, i quali se ampiamente elaborati da diverse corti costituzionale nazionali, prima tra tutte la Corte costituzionale tedesca,[542] così come dalle due Corti europee, per quanto attiene invece l'ordinamento nazionale, non trovano un preciso collocamento nel novero dei diritti fondamentali e inviolabili della Costituzione. Se tradizionalmente il diritto alla riservatezza viene fatto rientrare, alla luce di un'interpretazione evolutiva, nel novero dei diritti della personalità di cui all'art. 2 Cost., tale soluzione mostra i suoi limiti se applicata al bilanciamento tra esigenze investigative e garanzie caratterizzante il procedimento penale.[543] A differenza di altre disposizioni costituzionali, quali ad esempio gli artt. 13, 14 e 15 Cost., l'art. 2 non contiene alcuna previsione in merito ai presupposti necessari affinché l'autorità pubblica possa limitare i diritti inviolabili ivi garantiti.

Alla luce di tali considerazioni, è possibile affermare che la decisione analizzata da una parte si fa merito di tradurre i cambiamenti normativi, apportati dalla novella del 2008, anche sul piano giurisprudenziale, riconoscendo la capacità della Convenzione di Budapest di incidere sul diritto delle prove penali al di là del circoscritto settore della criminalità informatica, ma dall'altra presenta numerose zone d'ombra che ne riducono la portata innovatrice, lasciando vecchie questioni irrisolte e aprendone di nuove.

---

[540] Ibid.
[541] Guido Todaro, 'Restituzione di bene sequestrato, estrazione di copia e interesse ad impugnare: revirement delle Sezioni Unite' (2017) 11 Diritto Penale Contemporaneo, 160.
[542] Bundesverfassungsgericht del 27 febbraio 2008 1 BvR 370/07.
[543] Guido Todaro, 'Restituzione di bene sequestrato, estrazione di copia e interesse ad impugnare: revirement delle Sezioni Unite' (2017) 11 Diritto Penale Contemporaneo, 169-170.

Un ulteriore passo in avanti nella rimeditazione dei modelli concettuali e dell'approccio investigativo tradizionale, in virtù della natura peculiare del dato informatico, viene compiuto dalla Corte di Cassazione con la sentenza 34625/2020.[544]

Con tale decisione, i giudici di legittimità affrontano un'importante criticità del sequestro probatorio digitale, legata alla capacità dei sistemi informatici di contenere un'ampia massa di dati, di diversa natura e solo potenzialmente rilevanti per le indagini. Se nelle indagini tradizionali è possibile limitare la ricerca a specifiche informazioni, questo non è, allo stato della tecnica, possibile per le indagini informatiche, in cui risulta spesso difficoltoso individuare *ex ante* l'oggetto del sequestro.[545] Di conseguenza, potrebbe rivelarsi necessario per l'autorità giudiziaria disporre un sequestro c.d. integrale, vale a dire procedere a sequestro per l'intero contenuto di un dispositivo o se non addirittura all'apprensione fisica del supporto.[546]

Se, da una parte, tale possibilità non viene, in astratto, negata dalla Corte, dall'altra, i giudici di legittimità sottolineano il ruolo giocato dal principio di proporzionalità, elevato in materia di sequestri digitali c.d. integrali a "termine necessario di raffronto tra compressione dei diritti quesiti e la giustificazione della loro limitazione".[547] Da qui, è possibile evincere un'importante influenza della giurisprudenza delle due Corti Europee, che, come possibile evincere dall'analisi precedentemente svolta, hanno da sempre riconosciuto una centralità al principio di proporzionalità in materia di prova digitale e processo penale, al fine di raggiungere quel delicato equilibrio tra esigenze investigative e protezione dei diritti fondamentali. Sotto questa prospettiva, al fine di riportare a proporzione un sequestro c.d. integrale in ragione del carattere promiscuo dei dati, viene richiesto un onere di motivazione rafforzato, che abbia ad oggetto, pena l'illegittimità del decreto di sequestro, tre diversi profili: (i) il nesso di pertinenza tra *res*, finalità probatoria e reato per cui si procede, (ii) la tipologia di operazioni tecniche da svolgere sul dato e da ultimo (iii) la durata vincolo del temporale.[548] Tuttavia, come sottolineato dalla Corte, la possibilità di "verificare nella immediatezza" la sussistenza del nesso tra *res*, di cui

---

[544] Cass. sez. VI penale n. 34265 del 22 settembre 2020.
[545] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016), 3.
[546] Cass. sez. VI penale n. 34265 del 22 settembre 2020, 11.
[547] Ibid, 7.
[548] Marco Pittiruti, 'Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus' (Sistema penale 14 gennaio 2021) <https://www.sistemapenale.it/it/scheda/cass-sez-vi-sent-22-settembre-2020-dep-2-dicembre-2020-n-34265-pres-di-stefano-rel-silvestri.> ultimo accesso 29 settembre 2023.

non si ancora piena consapevolezza, reato per cui si procede e finalità probatoria, viene limitata dal momento che per esigenze investigative non è possibile individuare *ex ante* la *res*.[549] Considerando tale limitazione circa il profilo "quantitativo", sarà quindi necessario porre in essere delle garanzie di carattere compensativo, quali la giustificazione e motivazione specifica, da parte dell'autorità giudiziaria, dei profili di carattere qualitativo e temporale del sequestro, così da evitare il rischio che il sequestro assuma un valore meramente esplorativo circa "notizie reato diverse ed ulteriori rispetto a quella per cui si procede".[550] La Corte coglie l'occasione per elaborare su tali garanzie di carattere qualitativo e temporale, fornendo un vero e proprio *vademecum* per il pubblico ministero.[551] In particolare, una volta che il sequestro c.d. esteso venga realizzato attraverso l'ablazione "fisica" delle memorie si deve, in primo luogo, effettuare una copia integrale del contenuto dei dispositivi acquisiti. Successivamente, alla luce della promiscuità dei dati, è necessario procedere all'analisi della copia al fine di ricercare ed acquisire i dati rilevanti al fine dell'accertamento del fatto di reato. Una volta compiuta l'analisi, la copia integrale dei dati, denominata dalla Cassazione "copia-mezzo" perché servente solo ed esclusivamente alla selezione dei contenuti d'interesse investigativo, deve essere anch'essa restituita. Difatti, tale copia-mezzo non costituisce di per sé un elemento pertinente al reato, essendo una raccolta di dati indiscriminati e disorganizzati, che, allo stesso tempo, potrebbe presentare il rischio di acquisizione casuale di informazioni "sensibili" o "supersensibilli", vale a dire attinenti alla sfera intima e privata del soggetto interessato.[552] Pertanto, il pubblico ministero è autorizzato a trattenere tale duplicazione completa solamente per l'arco temporale strettamente necessario al fine di compiere l'operazione di selezione, assumendo la responsabilità di predisporre una struttura organizzativa adeguata a condurre tale attività nel minor tempo possibile.[553]

---

[549] Cass. sez. VI penale n. 34265 del 22 settembre 2020, 9.
[550] Ibid, 10.
[551] Marco Pittiruti, 'Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus' (Sistema penale 14 gennaio 2021) <https://www.sistemapenale.it/it/scheda/cass-sez-vi-sent-22-settembre-2020-dep-2-dicembre-2020-n-34265-pres-di-stefano-rel-silvestri.> ultimo accesso 29 settembre 2023.
[552] Cass. sez. VI penale n. 34265 del 22 settembre 2020, 10.
[553] Marco Pittiruti, 'Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus' (Sistema penale 14 gennaio 2021) <https://www.sistemapenale.it/it/scheda/cass-sez-vi-sent-22-settembre-2020-dep-2-dicembre-2020-n-34265-pres-di-stefano-rel-silvestri.> ultimo accesso 29 settembre 2023.

2.6. Gli accertamenti e i rilievi urgenti nella *scena criminis* digitale

Da ultimo, la novella del 2008 è intervenuta anche in materia di accertamenti e rilievi urgenti. Per quanto concerne le attività ad iniziativa della polizia giudiziaria, il codice del 1988, ex art. 354 cpp, ha posto in capo agli ufficiali e agli agenti della polizia giudiziaria il compito di vigilare e preservare la *scena criminis*, nell'attesa che il pubblico ministero sopraggiunga e assuma la direzione delle indagini. Tuttavia, ai commi successivi vengono tuttavia previste delle eccezioni che consentono alla polizia giudiziaria di porre in essere accertamenti e rilievi urgenti.[554] Qualora siano richieste, per lo svolgimento di tali atti, particolari competenze tecniche, la polizia giudiziaria può avvalersi dell'ausilio di esperti. Rispetto poi al requisito di urgenza, il legislatore pone una duplice condizione affinché venga legittimato un simile intervento da parte della polizia giudiziaria: il c.d. *periculum in mora*, vale a dire la sussistenza di un pericolo di alterazione o dispersione o in ogni caso di modifica delle cose, le tracce e i luoghi pertinenti al reato e l'impossibilità di un tempestivo intervento da parte del pubblico ministero o la mancata assunzione della direzione delle indagini da parte dello stesso. Inoltre, se del caso, gli ufficiali di polizia hanno anche il potere di disporre un sequestro del corpo di reato e delle cose a questo pertinenti, il quale dovrà ex art. 352, entro le 48 ore, essere convalidato dal pubblico ministero.

Rispetto allo svolgimento di tali attività, incombe in capo alla polizia giudiziaria il dovere di documentare tutte le attività svolte, al fine di garantire la futura utilizzabilità di tali atti probatori, che se verbalizzati, entrano a far parte del fascicolo del dibattimento o attraverso le contestazioni o in quanto irripetibili. Inoltre, ex art. 356 cpp, il difensore della persona sottoposta ad indagini ha la facoltà di assistere, senza diritto di essere preventivamente avvisato, a tali atti. L'assenza di particolari garanzie trova ragion d'essere nel fatto che la polizia giudiziaria, quando agisce di propria iniziativa, ha solo il compito di conservare, anche attraverso manipolazione, gli elementi probatori, essendo invece un accertamento che comporti la modifica dell'elemento di prova prerogativa del pubblico ministero ex art. 360 cpp.[555]

Tale impianto codicistico viene tuttavia modificato dalla legge 48/2008, che aggiunge un periodo di cui al comma 2 dell'art. 354 cpp: in relazione a "dati, informazioni, programmi informatici, sistemi informatici o telematici" viene prescritto in capo alla polizia giudiziaria

[554] Paolo Tonini e Carlotta Conti (eds), *Manuale di Procedura Penale* (Giuffrè editore 2021), 535.
[555] Ibid.

l'adozione di misure tecniche e prescrizioni, e prevedere, ove possibile, alla loro immediata duplicazione su supporti adeguati, che garantiscano "la conformità della copia all'originale e la sua immodificabilità". La *ratio* risiede nella necessità di conservazione del volatile e fragile dato digitale e di prevenzione rispetto ad una sua alterazione o accesso.[556] L'introduzione di un sopralluogo informatico ad iniziativa della polizia giudiziaria far venir meno il riconoscimento in capo alla polizia giudiziaria di un potere di carattere meramente cautelativo, di tipo conservativo: nell'ambiente informatico, il primo contatto con la scena *criminis* è parimenti, se non più, cruciale rispetto alla successiva analisi forense, in quanto un errore commesso durante tale fase preliminare può compromettere l'affidabilità o addirittura l'utilizzabilità delle prove digitali acquisite una volta terminata la catena di custodia.[557]

Rispetto invece all'attività del pubblico ministero, ai sensi dell'art. 358 cpp, viene riconosciuto in capo questi il potere di compiere accertamenti su fatti e circostanze a favore della persona sottoposta alle indagini. Se tali attività richiedono, come spesso accade per la raccolta di materiale digitale, una competenza tecnica specifica, allora il pubblico ministero può avvalersi della facoltà, ex art. 359 cpp, di richiedere la collaborazione di consulenti che possono essere da lui autorizzati ad assistere ai singoli atti di indagine. Se tale accertamento può essere ripetuto, allora non entra a far parte del fascicolo del dibattimento, potendo gli esiti dell'attività essere utilizzabili come prova, attraverso la deposizione di testimone del collaboratore. Mentre ex art. 360 cpp se tali accertamenti hanno natura non ripetibile sono sottoposti ad una disciplina particolare: gli atti possono essere inseriti nel fascicolo del dibattimento ed essere valutati come prova, senza ulteriore attività processuale. In aggiunta, alla difesa viene garantita la possibilità di manifestare la volontà di ricorrere all'istituto dell'incidente probatorio. Tale richiesta potrà non essere accolta dal pubblico mistero solo qualora sussista un'incompatibilità tra i tempi di tale procedura e l'urgenza di assicurare la prova al procedimento.

Allo stesso tempo, occorre segnalare che la tradizionale distinzione tra atto ripetibile o meno, da cui discende l'applicazione di un diverso ordine di garanzie, non risulta facilmente adattabile al contesto informatico, sussistono sul tema orientamenti contrastanti.[558] Una parte della

---

[556] Stefano Aterno, 'La Convenzione di Budapest del 2001 e la l. n. 48/2008' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1554-1555.
[557] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016), 32.
[558] Stefano Aterno, 'La Convenzione di Budapest del 2001 e la l. n. 48/2008' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1572 e *ss*.

dottrina sostiene che le tecniche di acquisizione della *digital forensics* possono consentire l'acquisizione della prova digitale con modalità ripetibili, salvo alcune particolari situazioni che possono dipendere anche dalla tipologia di strumenti informatici da acquisire.[559] Altri sostengono invece che qualsiasi operazione eseguita sui dati informatici comporta una modifica irreversibile degli stessi, anche quando si utilizzano gli strumenti più avanzati di *digital forensics*.

2.7. L'ammissibilità della prova digitale: le conseguenze sanzionatorie in caso di violazione delle *best practices*

In tema di ammissibilità della prova digitale, prima dell'entrata in vigore della legge 48/2008 la sentenza di riferimento era il "caso *Vierika*": il tale occasione il Tribunale di primo grado di Bologna aveva stabilito che l'assenza o la non corretta adozione delle misure volte a salvaguardia della genuinità del dato informatico comportasse l'inutilizzabilità della prova digitale acquisita durante le indagini.[560] Una lettura che, già prima della ricezione al livello nazionale degli insegnamenti del Consiglio d'Europa, era alquanto criticata, in virtù del principio di tassatività delle ipotesi di inutilizzabilità previsto dal nostro ordinamento giuridico.[561]

La legge del 2008, nell'introdurre le *best practices* in tema di ricerca, raccolta e custodia della prova digitale, non ha, tuttavia, definito le possibili conseguenze processuali derivanti dalla mancata conformità ai relativi adempimenti. Tale lacuna normativa ha aperto un vivace dibattito in dottrina e giurisprudenza circa la categoria di sanzioni procedurali da applicare a simili violazioni.

Un orientamento minoritario in dottrina ha sostenuto la possibilità di far rientrare il mancato rispetto delle *best practices* nella categoria delle nullità, ex art. 178, lettera c) cpp. Tuttavia, tale ricostruzione è stata presto contestata, in quanto si è sostenuto che la suddetta nullità non potesse riguardare la metodologia di acquisizione e conservazione delle prove raccolte in materia informatica.[562]

---

[559] Ibid.
[560] Corte d'appello di Bologna, sez II penale n 1823 30 gennaio 2008.
[561] Francesco Cajani, 'Il vaglio dibattimentale della digital evidence' (2013) 3 Archivio penale 837, 837.
[562] Andrea Colaiocco, 'La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria' (2019) 1 Archivio Penale 1, 5.

Un'altra ricostruzione, fondandosi sul dictum del caso *Vierika*, identifica l'art. 191 cpp come la sede privilegiata per giudicare le modalità di acquisizione della prova digitale, includendo dunque le sanzioni per violazioni delle *best practices* in materia digitale nella categoria dell'inutilizzabilità. Tale orientamento si fonda sul qualificare i parametri di integrità e genuinità della prova digitale, stabiliti dalla legge 48/2008, non come dettami operativi sprovvisti di conseguenze giuridiche, bensì come veri divieti probatori impliciti presidiati dalla sanzione dell'inutilizzabilità.[563]

Tuttavia, nella sua prima pronuncia in tema di prova digitale dopo l'entrata in vigore della legge 48/2008, la Corte di Cassazione ha preferito una terza via rispetto alle tesi della nullità e dell'inutilizzabilità proposte dalla dottrina.[564] I giudici di legittimità hanno infatti evidenziato che dal momento che "la normativa richiamata dal ricorrente non individua specificatamente le misure tecniche da adottare, limitandosi a richiamare le esigenze da salvaguardare attraverso idonei accorgimenti", la violazione di tali norme rientrava nella valutazione del giudice.[565] Di recente, la Corte di Cassazione ha ribadito che le *best practices* introdotte dal legislatore nel 2008, e poi "riempite di contenuto" dagli strumenti di *soft law*, hanno esclusivamente natura "programmatica".[566] Di conseguenza, le violazioni di tali regole possono avere un ruolo nella valutazione dell'attendibilità delle prove raccolte, ma non fanno scattare la sanzione dell'inutilizzabilità di cui all'art. 191 cpp.

Del resto, il contesto informatico, in quotidiana evoluzione, non permette, per sua stessa natura, al legislatore di precisare nel dettaglio le singole procedure e tecniche da adottare. Alla luce di un silenzio normativo, colmato da non vincolanti, e spesso divergenti tra loro, fonti di *soft law*, non sorprende che al livello giurisprudenziale la scelta sia ricaduta su un orientamento che identifichi nel piano della valutazione da parte dell'organo giudicante la conseguenza da allegare qualora si contesti una violazione delle *best practices* in materia. Tuttavia, occorre sottolineare che una simile ricostruzione finisce per attribuire un eccessivo margine discrezionale in capo all'organo giudicante, facendo coincidere l'oggetto della valutazione non più con la violazione della *best practice* in sé, ma con gli effetti che questa violazione ha

[563] Francesco Cajani, 'Il vaglio dibattimentale della digital evidence' (2013) 3 Archivio penale 837, 837.
[564] Corte d'appello di Bologna, sez II penale n. 1823 30 gennaio 2008.
[565] Ibid.
[566] Cass. sez. II penale n. 35447 del 21 ottobre 2020.

sull'elemento probatorio acquisito.[567] Di conseguenza, qualora si accertasse che l'integrità e genuinità del dato non siano state compresse, tale elemento sarebbe pienamente utilizzabile come prova. In aggiunta, la mancanza di protocolli riconosciuti al livello nazionale rende in ogni caso complesso effettuare un dettagliato scrutinio, con la conseguenza che il giudice nella sua valutazione tenderà a limitarsi a prendere atto che dal momento che la legge non favorisce alcun metodo, le autorità investigative possiedono un certo margine discrezionale circa l'adozione e l'attuazione della migliore metodologia applicabile al singolo caso concreto.[568]

Sotto questa prospettiva, il contraddittorio "sulla prova" da esercitarsi in giudizio, assume un ruolo fondamentale quale strumento di contrasto alle *best practices* non applicate correttamente.[569] Qui riveste un preminente rilievo l'esposizione dei risultati dell'indagine informatica ad opera dell'esperto, che sarà veicolata attraverso l'esame e il controesame, consentendo alla difesa di verificare la competenza specifica dell'esperto, l'impiego in concreto delle *best practices* in materia e l'osservanza della catena di custodia delle prove digitali.[570] Occorre, tuttavia, che si pongano le condizioni di trasparenza circa l'operato delle autorità investigative affinché il controllo differito sulla metodica di riproduzione digitale possa agevolmente esplicarsi e dunque configurarsi un onere probatorio in capo alla parte che lamenti la non genuinità del documento digitale. *A contrario*, qualora non vi sia trasparenza nell'operato investigativo, l'inattendibilità della prova dovrebbe ritenersi intrinseca.[571]

In particolare un simile onere probatorio in capo all'accusa potrà considerarsi correttamente assolto nel momento in cui venga indicato, per l'istruttoria dibattimentale: (i) da chi sia stato individuato il dato informatico, (ii) come tale dato si presentava al momento della sua individuazione ad opera della parte, (iii) con quale modalità e dopo quanto tempo tale persona lo abbia acquisito, in che modo siano state successivamente conservate le "sue caratteristiche

---

[567] Carlotta Conti, 'La prova informatica e il mancato rispetto delle *best practices*: lineamenti sistematici sulle conseguenze processuali' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1545.
[568] Laura Bartoli and Giulia Lasagni, 'The Handling of Digital Evidence in Italy' in Michele Caianiello and Alberto Camon (eds) *Digital Forensic Evidence Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Wolters Kluwer 2021), 92.
[569] Carlotta Conti, 'La prova informatica e il mancato rispetto delle *best practices*: lineamenti sistematici sulle conseguenze processuali' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1546.
[570] Francesco Cajani, 'Il vaglio dibattimentale della digital evidence' (2013) 3 Archivio penale 837, 850.
[571] Ibid, 851.

oggettive di qualità, sicurezza, integrità", così come presenti al momento della individuazione/acquisizione.[572]

Ciò detto, la soluzione ottimale al fine di preservare l'autenticità della prova consisterebbe nel garantire un contraddittorio tecnico in fase di assunzione del dato digitale.[573] Tuttavia, tale garanzia non è compatibile con un consolidato orientamento giurisprudenziale, rispetto al quale le operazioni di sequestro tramite copia dei dati digitali rientrerebbero nella disciplina degli accertamenti tecnici ripetibili ex art. 359 cpp, da svolgere, pertanto, senza le garanzie stabilite dall'art. 360 cpp per gli accertamenti non ripetibili, quali il preavviso alla difesa in ordine al compimento delle operazioni, la possibilità di parteciparvi con un consulente tecnico e il diritto all'instaurazione dell'incidente probatorio.[574] Tuttavia, gli esperti tecnici hanno più volte sottolineato come le procedure di copia delle prove informatiche, anche quando non riguardano un oggetto esposto a deterioramento, potrebbero comportare un'alterazione irreversibile del dato digitale.[575] Se la possibilità di effettuare più duplicati potrebbe, in astratto, eliminare ogni rischio di irripetibilità dell'attività svolta, le criticità si collocano a monte, ossia al momento della "fotografia digitale" del contenuto racchiuso nel dispositivo.[576] Sotto questo profilo, nella prospettiva dell'imputato, l'intervento difensivo *ab inizio* è cruciale al fine di contestare il *modus operandi* delle autorità investigative in dibattimento. Sul punto occorre segnalare che, la Corte di Cassazione, sembra aver riconosciuto, seppur in via incidentale, la necessità di attivare rispetto all'acquisizione della prova digitale delle garanzie partecipative sin dalla fase investigativa, da tempo sollecitata dall'elaborazione scientifica consapevole del rischio di modifica del dato sottoposto ad analisi.[577] Riconoscendo la centralità del principio di proporzionalità, che si traduce nella valorizzazione di un onere di motivazione circa il sequestro digitale, la Corte censura la scelta della pubblica accusa di assegnare alla polizia giudiziaria

[572] Ibid.
[573] Alessandra Sanna, 'La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati' (2022) Discrimen, 10.
[574] Ibid.
[575] Vincenzo Lagi, 'Accertamento tecnico ripetibile. la gestione del reperto informatico' in Alberto Cadoppi *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica), 1671.
[576] Marco Pittiruti, 'Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus' (Sistema penale 14 gennaio 2021) <https://www.sistemapenale.it/it/scheda/cass-sez-vi-sent-22-settembre-2020-dep-2-dicembre-2020-n-34265-pres-di-stefano-rel-silvestri.> ultimo accesso 29 settembre 2023.
[577] Corte Cass. sez. VI penale 22 settembre 2020 n. 34265.

l'esame preliminare della strumentazione informatica, il che porta a sostenere che le attività di duplicazione del dato digitale debbano avvenire in contradditorio tra le parti.[578]

Alla luce di quanto esposto, risulta necessario un intervento legislativo che non solo identifichi delle *guidelines*, ma che individui altresì i rimedi in caso di violazioni delle stesse. In particolare, l'adozione di protocolli e guida riconosciuti al livello nazionale, seguendo l'esempio di altri Stati membri e degli strumenti di *soft law* adottati al livello europeo, potrebbe rendere più facile per la difesa, che abbia o meno partecipato al contradditorio nella fase investigativa, contestare l'affidabilità della prova digitale raccolta e per il giudice effettuare uno scrutinio circa la qualità dell'indagini investigativa svolta. Allo stesso tempo, è auspicabile un intervento legislativo volto alla stesura di una serie di regole di esclusione ad hoc che tengano conto del peculiare legame tra modalità acquisitive e prova digitale. Infine, si spera che anche gli operatori del diritto si mostrino, propensi a adottare un approccio coerente che tenga conto sia delle necessità di preservare e raccogliere dati, sia dell'importanza di proteggere la dignità individuale.[579]

3. La disciplina in materia di *data retention*: verso una compatibilità della normativa nazionale al *dictum* della giurisprudenza europea?

A seguito degli attentati di Londra del 2005 e Madrid del 2004, numerosi Stati membri, tra cui anche l'Italia, hanno adottato regimi sempre più rigorosi in materia di *data retention* al fine di rafforzare la sicurezza nazionale e prevenire futuri attacchi terroristici. Tuttavia, a seguito della dichiarazione d'invalidità della Direttiva 2002/58/CE da parte della CGUE, i legislatori nazionali hanno iniziato ad adeguare tali regimi pro-securitari al fine di raggiungere un migliore equilibrio tra esigenze di prevenzione e repressione al crimine e la protezione dei diritti fondamentali. Tuttavia, il legislatore italiano è intervenuto solo recentemente in tal senso, con il d. l. 132/2021,[580] che, pur rappresentando un'importante passo in avanti al fine di conformare la disciplina nazionale in materia di *data retention* al *dictum* della giurisprudenza europea, ha lasciato ancora diverse questioni aperte.

[578] Ibid.
[579] Alessandra Sanna, 'La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati' (2022) Discrimen, 13.
[580] Decreto-Legge 30 settembre 2021, n. 132.

3.1. I primi interventi legislativi in materia: una risposta pro-securitaria alla lotta contro il terrorismo

La norma di riferimento in materia è l'art. 132 del Codice della Privacy che, introdotta dal d. lgs. 196/2003,[581] stabiliva in capo ai *service providers* un generale obbligo di *retention* di 24 mesi dei dati informatici e telematici, per finalità di accertamento e repressione dei reati. Su tale disciplina interviene, solo a pochi mesi di distanza dall'entrata in vigore del Codice, il d. l. 354/2003,[582] prevedendo che l'acquisizione di tali dati debba essere disposta con decreto motivato del giudice, su richiesta del pubblico ministero o delle parti private. Nuovamente, con la l. 155/2005,[583] viene invece introdotto un vero e proprio "doppio binario": in primo luogo, solo per determinati reati gravi la richiesta di accesso doveva essere autorizzata dal giudice, mentre per gli altri era sufficiente un decreto motivato da parte del pubblico ministero; in secondo luogo, veniva modificato anche l'obbligo di *retention* in capo ai service providers, prescrivendo che per perseguire fattispecie di reato legate ad una matrice terroristica, "tutti i metadati dovevano essere trattenuti dagli operatori sino al 31 dicembre 2007", con un'estensione dunque dei limiti temporali stabiliti dall'art. 132.[584] Tale riforma risultava perfettamente in linea con il clima pro-securitario, respirato in quegli anni in tutta Europa a seguito degli attentati terroristici di Madrid e Londra.

Tuttavia, il legislatore nazionale è stato presto tenuto a riscrivere la norma in esame, al fine di attuare, con il d. lgs. 109/2008, la Direttiva 2006/24/CE. La riforma, da una parte, identificava il pubblico ministero quale unico soggetto incaricato ad autorizzare le richieste di acquisizione dei metadata e, dall'altra, prescriveva una conservazione generalizzata ed un accesso garantiti per la repressione di qualunque tipologia di reato. Veniva dunque eliminata la limitazione di una *data retention* generalizzata alla sola categoria dei reati "gravi", andando anche oltre a quanto prescritto Direttiva del 2006 che invece continuava a prevedere una simile distinzione.[585]

---

[581] Decreto-Legislativo 30 giugno 2003, n. 196 ("**Codice della Privacy**").
[582] Decreto-Legge 24 dicembre 2003, n. 354
[583] Legge 31 luglio 2005, n. 155.
[584] Giulia Formici, 'The three Ghosts of data retention': passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione' (2022) 1 OSSERVATORIO COSTITUZIONALE 125, 135.
[585] Ibid, 136.

A seguito della dichiarazione d'invalidità della Direttiva del 2006 ad opera della sentenza *Digital Rights Ireland* e all'affermarsi di nuovo ruolo per l'art. 15 *Direttiva c.d. e-Privacy*, molti Parlamenti nazionali avevano intrapreso riforme significative delle loro leggi interne in materia di *data retention*, spesso sollecitati dai numerosi rinvii pregiudiziali alla CGUE.[586] Tuttavia, un simile processo di revisione non è stato avviato nell'ordinamento italiano: l'art. 132 Codice della Privacy ha continuato a subire una serie di modifiche da parte del legislatore,[587] rispondenti ad una logica meramente emergenziale e derogatoria rispetto agli "ordinari" limiti temporali di *retention*, al fine di far fronte alle nuove esigenze di contrasto al terrorismo.[588] Del resto, anche su un piano giurisprudenziale, la Corte di Cassazione, con orientamento granitico, aveva sostenuto la compatibilità dell'art. 132 Codice della Privacy con l'articolo 15 Direttiva e-Privacy, come interpretato dalla CGUE. Ad avviso della Suprema Corte, il principio di proporzionalità e stretta necessarietà veniva rispettato in quanto non solo la deroga alla tutela della riservatezza delle comunicazioni prevista dalla norma era limitata nel tempo e mirava esclusivamente all'accertamento e repressione dei reati, la cui gravità poteva essere valutata caso per caso dall'autorità giudiziaria, ma la decisione era anche affidata allo scrutinio di un'autorità giudiziaria, vale a dire del pubblico ministero.[589] Alla luce di tali considerazioni, è possibile affermare che malgrado i numerosi moniti da parte della CGUE rispetto alla necessità di porre delle limitazioni alla *retention* dei dati non solo al livello temporale, ma anche oggettivo, soggettivo e geografico, al fine di raggiungere un equilibrio tra ingerenza nella sfera privata ed esigenze di prevenzione e repressione dei reati, fino alla riforma del 2021, non si è registrato al livello nazionale nessun intervento normativo o giurisprudenziale in tal senso.[590]

---

[586] Sul punto si veda l'analisi svolta al paragrafo 3 e *ss* del Capitolo 2.

[587] Nel giro di pochi anni, si sono susseguiti i seguenti interventi legislativi: il decreto-legge antiterrorismo, il Decreto milleproroghe, entrambi del 2015, ed infine con la Legge Europea 2017.

[588] Giulia Formici, 'The three Ghosts of data retention': passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione', (2022) 1 OSSERVATORIO COSTITUZIONALE 125, 138.

[589] Giovanni Petroni, 'Il caso Prokuratuur: il difficile dialogo tra le Corti e le conseguenze della sentenza della Corte di Giustizia nell'ordinamento nazionale' (Giustizia insieme 24 novembre 2021) < https://www.giustiziainsieme.it/en/diritto-ue/2026-il-caso-prokuratuur-il-difficile-dialogo-tra-le-corti-e-le-conseguenze-della-sentenza-della-corte-di-giustizia-nell-ordinamento-nazionale-di-giovanni-petroni?hitcount=0> ultimo accesso 29 settembre 2023.

[590] Giulia Formici, 'The three Ghosts of data retention': passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione' (2022) 1 OSSERVATORIO COSTITUZIONALE 125, 139.

3.2. L'intervento legislativo del 2021: la codificazione dei principi espressi dalla Corte di Giustizia in *Prokuratuur*

Come anticipato, nel 2021 arriva finalmente una risposta da parte del legislatore nazionale, innescata dal *dictum* della sentenza *Prokuratuur*. Tale decisione ha fatto emergere numerosi ed evidenti profili di compatibilità, a lungo segnalati in dottrina, tra il dettato europeo e l'articolo 132 nella versione all'epoca vigente, nella parte in cui esso: (i) rimetteva nelle mani del pubblico ministero la decisione circa l'acquisizione dei dati; (ii) non fissava alcun limite, in particolare dal punto di vista qualitativo rispetto alla gravità dei reati che potevano giustificare una simile interferenza.[591]

Come evidenziato al suo stesso preambolo, con il d. l. 132/2021, il legislatore ha deciso di intervenire d'urgenza, considerando "straordinaria necessità ed urgenza di garantire la possibilità di acquisire dati relativi al traffico telefonico e telematico per fini di indagine penale nel rispetto dei principi enunciati dalla Grande sezione della Corte di giustizia dell'Unione europea nella sentenza del 2 marzo 2021, causa C-746/18, e in particolare di circoscrivere le attività di acquisizione ai procedimenti penali aventi ad oggetto forme gravi di criminalità e di garantire che dette attività siano soggette al controllo di un'autorità giurisdizionale".

Rispetto alle principali novità introdotte al fine di conformarsi al *dictum* della Curia europea, in primo luogo, il decreto elimina il margine discrezionale lasciato alle autorità giudiziarie, fornendo una definizione di categorie di reati considerati "gravi", tanto da giustificare l'acquisizione dei dati sul traffico. Attualmente, la legge consente l'acquisizione dei tabulati solo qualora "sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi".[592] In secondo luogo, viene specificato che l'acquisizione di tali dati deve risultare rilevante per l'accertamento dei fatti di reato.[593] Da ultimo, viene stabilito che l'accesso ai dati deve essere

---

[591] Giovanni Petroni, 'Il caso Prokuratuur: il difficile dialogo tra le Corti e le conseguenze della sentenza della Corte di Giustizia nell'ordinamento nazionale' (Giustizia insieme 24 novembre 2021) < https://www.giustiziainsieme.it/en/diritto-ue/2026-il-caso-prokuratuur-il-difficile-dialogo-tra-le-corti-e-le-conseguenze-della-sentenza-della-corte-di-giustizia-nell-ordinamento-nazionale-di-giovanni-petroni?hitcount=0> ultimo accesso 29 settembre 2023.
[592] Art. 132.3 Codice della Privacy.
[593] Ibid.

effettuato da un'autorità che sia indipendente e imparziale, vale a dire terza e neutrale rispetto al procedimento: la nuova formulazione del terzo comma prevede che "i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato" su istanza del pubblico ministero o delle parti private.[594]

3.3. Le questioni rimaste aperte

Nonostante l'intervento legislativo del 2021 abbia introdotto importanti modifiche nella disciplina della *data retention*, diversi aspetti sono stati trascurati o del tutto dimenticati da parte del legislatore. In particolare, la riforma non sembra aver affrontato due tematiche centrali, vale a dire (i) l'imposizione di limiti temporali di conservazione dei dati e, più in generale, (ii) il divieto di conservazione "generalizzata e indifferenziata" degli stessi.[595]

Rispetto al primo profilo, l'art. 132 Codice della Privacy prevede che i tabulati siano conservati per un termine massimo di 24 mesi, che scende a 12 per quelli telematici, e a 30 giorni per le chiamate senza risposta, e stabilisce anche, per i reati di competenza delle procure distrettuali o per i quali la durata delle indagini preliminare è ampliata a due anni, un termine di conservazione di settantadue mesi. Sebbene quest'ultima deroga sia limitata a specifiche categorie di reati, la mancanza di possibilità da parte del *service provider* di effettuare una valutazione e una selezione preventiva basata sul tipo di reato per cui potrebbe essere richiesto l'accesso in futuro, si traduce inevitabilmente in una conservazione generalizzata di tutti i dati per un periodo di sei anni.[596] Ciò potrebbe comportare il rischio di creazione di archivi di milioni e milioni di dati potenzialmente utilizzabili come veri e propri dossier su determinati individui, con evidenti interferenze sul piano della protezione dei diritti fondamentali.[597]

Per quanto concerne il divieto di conservazione "generalizzata e indifferenziata" dei dati, alla luce del principio di proporzionalità, la CGUE ha delineato chiaramente l'importanza di un'identificazione preventiva dei soggetti coinvolti e della selezione di criteri oggettivi e non discriminatori per giustificare la conservazione mirata dei dati. Sotto questo profilo, l'art. 132 non fornisce rilevanti indicazioni.

---

[594] Ibid.
[595] Veronica Palladini, 'Data retention e privacy in rete: verso una regolazione conforme al diritto UE?' 1 Rivista Italiana di informatica e diritto 103, 107.
[596] Ibid, 108.
[597] Ibid.

Del resto, occorre sottolineare che sebbene la CGUE fornisca in materia indicazioni piuttosto dettagliate, non sembra tuttavia distinguere, *ab origine*, tra indagini preventive e repressive. Se da un lato, una linea di demarcazione tra le due finalità finisce per essere al quanto superflua se si assume, come nel caso della CGUE, una "prospettiva c.d. *privacy oriented*", sul piano delle garanzie procedurali tale differenza non può che risultare essenziale.[598]

Alla luce di tali considerazioni, la saga nazionale in materia di *data retention* non può dirsi giunta a conclusione, in quanto, già a solo pochi anni di distanza dall'ultimo intervento legislativo, potrebbe essere richiesto un ulteriore adeguamento del testo dell'art. 132 Codice Privacy, al fine conformarsi al *dictum* della CGUE, che, allo stesso tempo, risulta tutt'altro che definitivo.[599]

4. L'acquisizione e l'ammissibilità della prova digitale all'estero

Come delineato nei Capitoli precedenti, la possibilità che i dati informatici siano immagazzinati presso *server* allocati al di fuori dei confini nazionali è diventata un'ipotesi piuttosto frequente. In tal caso, le autorità investigative, interessate ad assicurare tali dati al procedimento penale nazionale, devono ricorrere agli strumenti di cooperazione giudiziaria disciplinati dall'ordinamento nazionale. Sotto questo profilo, ad oggi, l'acquisizione e custodia della prova digitale può effettuarsi tramite tre diversi strumenti: (i) la tradizionale rogatoria internazionale, la cui disciplina è stata da ultimo modificata dal d. lgs. 149/2017;[600] (ii) l'OEI introdotto dal d. lgs. 108/2017, in attuazione della DOEI, sopra esaminata; ed infine (iii) il mezzo di prova di cui all'art. 234 bis cpp, introdotto dal legislatore nel 2015, in occasione del decreto c.d. "antiterrorismo",[601] e che fino ad ora, rispetto agli altri due strumenti, ha avuto una portata applicativa piuttosto limitata, ma che recentemente è stato oggetto di diverse sentenze della Cassazione. Occorre, tuttavia, segnalare che il quadro normativo attuale è destinato a subire delle modifiche alla luce di due strumenti recentemente adottati al livello sovranazionale riguardanti l'accesso alla prova digitale presso i *service providers*. L'Italia ha infatti recentemente ratificato il Secondo Protocollo Addizionale alla Convenzione di Budapest,

---

[598] Giulia Lasagni, 'Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della privacy', (2022) La legislazione penale 1, 11.
[599] Valeria Tartara, 'La Corte di Giustizia conferma il "divieto di conservazione generalizzata e indiscriminata" dei dati relativi al traffico delle comunicazioni elettroniche per finalità preventive di contrasto alla criminalità. possibili ricadute nell'ordinamento italiano' (2022) 12 Sistema Penale 173, 204.
[600] Decreto Legislativo 3 ottobre 2017, n. 149.
[601] Decreto-Legge 18 febbraio 2015, n. 7.

mentre al livello UE, il nostro ordinamento dovrà, entro il 2026, conformarsi con il dettato del nuovo pacchetto in tema di accesso alle prove digitali *cross-border*, recentemente entrato in vigore.

4.1. La rogatoria "internazionale" in ambito digitale

Rispetto alla rogatoria c.d. attiva, vale a dire quando la richiesta viene effettuata dall'Italia ad uno Stato estero, il procedimento è disciplinato agli artt. 727 e *ss* cpp. In particolare, la procedura ordinaria prevede che la richiesta diretta alle autorità straniere, avente ad oggetto comunicazioni, notificazioni o attività di acquisizione probatoria, possa essere effettuata dal giudice o dal pubblico ministero, in ottemperanza alle rispettive attribuzioni, per poi essere trasmessa al ministro della giustizia, che provvederà all'inoltro per via diplomatica. A quest'ultimo viene attribuito un "potere di blocco" della richiesta, esercitabile con decreto, qualora sussista il rischio di compromissione della sicurezza o di altri interessi essenziali dello Stato. In aggiunta alla procedura ordinaria, il codice contempla la possibilità di inoltro diretto al rappresentante diplomatico o consolare, previa notifica al ministro, qualora quest'ultimo non proceda all'inoltro della rogatoria entro trenta giorni dalla richiesta né emetta il decreto di sospensione o se sussista una situazione di urgenza. Da ultimo, è prevista altresì la possibilità di trasmissione diretta tra le autorità giudiziarie quando sia stipulato un accordo internazionale a tal fine.

La riforma del 2017 ha modificato il regime di utilizzabilità degli atti assunti per rogatoria previsto all'art. 729 cpp, producendo importanti conseguenze per l'acquisizione e l'utilizzo della prova digitale acquisita tramite tale procedura. [602]

La novella fa salva la "regola di specialità" di cui al primo comma: l'autorità giudiziaria richiedente è vincolata al rispetto di eventuali condizioni all'utilizzabilità degli atti richiesti poste dallo lo Stato estero. La riforma emenda invece la normativa previgente nella parte in cui veniva prescritta la sanzione dell'inutilizzabilità nel processo penale interno qualora la prova venisse acquisita nello Stato estero con modalità diverse da quelle indicate dall'autorità giudiziaria italiana. Di conseguenza, ad ogni richiesta l'autorità giudiziaria poteva imporre

[602] Andrea Colaiocco, 'La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria' (2019) 1 Archivio Penale 1, 5.

condizioni utilizzabilità differenti. Rispetto all'acquisizione del dato digitale, un simile margine discrezionale non offriva alcuna garanzia circa il rispetto delle *best practices* previste dal diritto interno al fine di preservare la genuinità e integrità della prova digitale.[603]

Con l'obiettivo di stabilire un nuovo equilibrio tra esigenze investigative e certezza del diritto, il decreto del 2017 è intervenuto, specificando che gli atti compiuti in violazione delle condizioni poste dall'autorità giudiziaria sono inutilizzabili solo nei casi in cui l'inutilizzabilità è prevista dalla legge. Nel contesto informatico, questa modifica implica che solo qualora l'eventuale deviazione dello Stato estero nel processo di acquisizione dei dati digitali sia sanzionata in Italia con la sanzione dell'inutilizzabilità, allora la prova digitale raccolta sarà affetta da una simile conseguenza procedurale.[604] Diversamente, la violazione sarà una considerata una mera irregolarità. Una simile soluzione, se, da una parte, rende omogeneo il regime tra la prova digitale raccolta mediante rogatoria e quella acquista con i mezzi di ricerca della prova in territorio nazionale, dall'altra, sembra rimandare ad un'inutilizzabilità ex lege, che, come in precedenza evidenziato, in caso di violazioni delle *best practices*, non è stata prescritta dal legislatore o riconosciuta al livello giurisprudenziale.

4.2. La disciplina prevista ex art. 234 bis cpp

Come è possibile evincere dall'analisi fin qui condotta, la legge 48/2008, si è limitata ad attuare il dettato della Convenzione di Budapest sotto una prospettiva esclusivamente interna, non traducendo alcuna indicazione al livello di cooperazione giudiziaria tra le sue Parti contraenti. Una risposta legislativa in tal senso arriva solo nel 2015: in occasione del "decreto c.d. antiterrorismo", il legislatore nazionale, traendo spunto dall'art. 32 della Convenzione di Budapest, ha introdotto nel codice l'art. 234 bis cpp. La norma disciplina un nuovo mezzo di prova, prevedendo che sia sempre ammessa "l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico". In quest'ultimo caso, in ottemperanza degli obblighi pattizi, viene richiesto il consenso volontario del legittimo titolare.

L'art. 234 bis cpp, in primo luogo, stabilisce che quando i dati informatici sono facilmente accessibili attraverso una semplice navigazione in rete, come ad esempio i dati relativi ai profili pubblici sui *social network*, è possibile acquisirli per scopi investigativi senza richiedere il

[603] Ibid, 7.
[604] Ibid.

consenso dell'interessato. In secondo luogo, la norma consente di acquisire documenti e dati informatici conservati all'estero non disponibili al pubblico, quali ad esempio i metadati, subordinando tale possibilità al consenso del "legittimo titolare".

Per comprendere la motivazione del legislatore dietro la scelta di introdurre tale disposizione, è essenziale, innanzitutto, esaminare il contesto in cui questa norma è stata inclusa. L'art. 234 bis cpp è parte di un quadro normativo di lotta al terrorismo, nel quale il legislatore nazionale, attraverso l'adozione strumenti legislativi dal carattere preventivo, tenta di fronteggiare le crescenti minacce rappresentate da un uso sempre più sofisticato e complesso di strumenti tecnologici da parte delle organizzazioni terroristiche. Un'interpretazione della norma che tenga in considerazione la *ratio* della riforma in cui è stata inserita potrebbe portare a considerare l'art. 234 bis cpp come "strumento finalizzato ad un'attività di prevenzione ai fini di un'efficace intelligence".[605] Tuttavia, in questa prospettiva, se l'intenzione del legislatore fosse stata effettivamente quella della prevenzione, è legittimo interrogarsi sulla ragione del posizionamento della norma all'interno della sezione relativa ai mezzi di prova.[606]

Nel caso invece in cui la norma fosse stata introdotta con l'intento di derogare al sistema vigente di rogatorie internazionali, l'ambito di applicazione rimane eccessivamente limitato: se non esiste un accordo bilaterale tra l'Italia e lo Stato che detiene tali documenti o dati informatici, la norma in questione non sembra essere in grado di superare questa mancanza poiché ha un'applicazione unilaterale e non può influire sulle decisioni dello Stato richiesto in materia di cooperazione internazionale.[607] Inoltre, se la norma sembra aprire la strada ad una cooperazione diretta i *service providers*, occorre, tuttavia, sottolineare che il successo di una simile operazione dipende dalla decisione di accogliere o meno una simile richiesta da parte del *provider* stesso, il quale, come già evidenziato nel Capitolo 2, è mosso da interessi diversi rispetto alle esigenze delle diverse parti coinvolte nel procedimento penale. Sotto questo profilo, sarà interessare analizzare se il legislatore, al fine di recepire il dettato dei recenti strumenti adottati al livello internazionale che disciplinano la cooperazione diretta con i *service providers*, deciderà di emendare tale norma o introdurre una disciplina ad hoc, riducendo, in quest'ultimo caso, ancora di più lo scopo di applicazione dell'art. 234 bis cpp.

---

[605] Marco Torre, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016), 89.
[606] Ibid.
[607] Ibid.

4.3. L'ordine di indagine europeo

La DOEI è stata attuata nell'ordinamento interno con il d.lgs. 108/2017.[608] La procedura rogatoria ex art. 723 e ss cpp, sopra analizzata, rimane, tuttavia, in vigore nei rapporti fra l'Italia e gli Stati membri che non hanno aderito alla direttiva, vale a dire la Danimarca e l'Irlanda, così come nei rapporti fra l'Italia e gli Stati che non appartengono all'Unione.

In materia di acquisizione *cross-border* della prova digitale la DOEI, come evidenziato al Capitolo 2, detta una serie di norme dedicate al tema delle intercettazioni. Di conseguenza, anche il decreto dedica, agli artt. 23 e *ss*, un'espressa disciplina all'assistenza giudiziaria in materia di intercettazione di flussi di comunicazioni o di dati, secondo il dettato dagli artt. 30 e 31 DOEI. Il decreto riprende la distinzione stabilita nella direttiva, fondata sulla necessità o meno, ai fini di eseguire l'attività di intercettazione di comunicazioni, di ricorrere all'assistenza tecnica dell'autorità giudiziaria di un altro Stato membro nel "cui territorio si trova il dispositivo o il sistema da controllare".[609]

Come ribadito dalla Circolare ministeriale in attuazione della direttiva 2014/41/UE,[610] l'assistenza non si rende necessaria quando l'utenza soggetta all'intercettazione è associata ad un operatore nazionale di telecomunicazioni che ha stipulato accordi di *data roaming* con operatori esteri, garantendo così automaticamente il trasferimento delle comunicazioni sul territorio italiano. Inoltre, come sottolineato dalla Cassazione,[611] non è richiesta assistenza anche nei casi in cui si verifichi il c.d. "istradamento" delle comunicazioni, dal momento che tutte le operazioni di intercettazione vengono svolte all'interno territorio nazionale. In tali evenienze, ex art. 44 decreto vige solo un obbligo di informativa circa l'inizio delle operazioni di intercettazione verso l'autorità giudiziaria dello Stato membro nel "cui territorio si trova il dispositivo o il sistema da controllare".[612] Qualora si sia appreso, solo nel corso delle operazioni di intercettazione, che il dispositivo o il sistema controllato si trova nel territorio di altro Stato membro, la notifica deve essere effettuata non appena si sia appresa tale notizia. Se l'autorità

---

[608] Decreto Legislativo 21 giugno 2017, n. 108
[609] Artt. 43 e 44.
[610] Circolare 26 ottobre 2017 - Attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale – Manuale operativo (Ministero della Giustizia 26 ottobre 2017) <https://www.giustizia.it/giustizia/it/mg_1_8_1.page?facetNode_1=0_0&facetNode_2=0_0_2&facetNode_3=4_10&facetNode_4=0_0_2_3&contentId=SDC58426&previsiousPage=mg_1_8> ultimo accesso 29 settembre 2023.
[611] Ibid.
[612] Ibid.

giudiziaria dello Stato membro, ricevuta l'informazione, decida che le attività di intercettazione non possono essere eseguite o proseguite, vige un obbligo di immediata cessazione delle operazioni in corso. In quest'ultimo caso, viene fatta salva l'utilizzabilità dei risultati ottenuti dalle operazioni di intercettazione svolte fino a quel momento, purché siano rispettate le condizioni stabilite dall'autorità giudiziaria dello Stato membro informato.

L'assistenza risulta invece indispensabile "qualora si tratti di conversazioni che intercorrono su un'utenza o un sistema riferibile soltanto a un gestore estero ovvero di comunicazioni estero su estero non dirottabili (o comunque non dirottate) su nodi telefonici ubicati in Italia".[613] In tal caso, troverà applicazione la disciplina di cui all'art. 43 del decreto. In particolare, il pubblico ministero dovrà emettere un OEI contente una serie di informazioni, tra cui l'indicazione dell'autorità giudiziaria che ha disposto l'intercettazione, la sua durata e i motivi della rilevanza dell'atto. Tale norma deve essere letta in combinato disposto con l'art. 27 decreto che riproduce il dettato della direttiva di cui all'art. 6 DOEI, in cui, come esaminato al Capitolo 2, l'emissione dell'OEI viene subordinata alla condizione che l'atto istruttorio avrebbe potuto essere emesso "alle stesse condizioni in un caso interno analogo". Tuttavia, l'art. 27 del decreto si limita a prescrivere che l'OEI possa essere emesso dal pubblico ministero o dal giudice, "nell'ambito delle rispettive attribuzioni", senza sottoporre l'emissione al rispetto delle condizioni prescritte per emettere, al livello interno, il mezzo di ricerca della prova oggetto dell'OEI. Sotto questo profilo, sebbene la disciplina codicistica in tema di intercettazioni non sia stata approfondita ai fini di questo elaborato, risulta evidente da un'interpretazione letterale della disciplina, un contrasto con la riserva di giurisdizione contenuta all'art. 15 Cost. e garantita, per la disposizione al livello interno delle intercettazioni, all'art. 267.1 cpp.[614] La norma codicistica non utilizza il termine "autorità giudiziaria", impiegato per altri mezzi di ricerca della prova, come il sequestro e la perquisizione, stabilendo che solo il giudice per le indagini preliminari abbia il potere di autorizzare ex ante o, qualora il pubblico ministero non abbia atteso l'intervento giurisdizionale, di convalidare ex post le attività di intercettazione.

Tuttavia, occorre sottolineare come la lettera della norma possa essere superata in chiave ermeneutica, tenendo in considerazione non solo che il decreto deve essere letto unitamente alla direttiva, le cui prescrizioni sono dotate di efficacia diretta nella misura in cui, come nel

---

[613] Ibid.
[614] Fabiana Falato, 'La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale' (2018) Archivio Penale 1, 34.

caso dell'art. 6 DOEI, risultino sufficientemente precise ed incondizionate, ma anche quanto evidenziato dalla Circolare ministeriale in attuazione della DOEI.[615] In tale "manuale operativo" viene giustificata la scelta di individuare il pubblico ministero, e non il giudice per le indagini preliminari, come autorità emittente l'OEI avente ad oggetto operazioni di intercettazione ex art. 43 del decreto, in quanto anche per le intercettazioni disposte al livello domestico l'esecuzione è affidata all'autorità giudiziaria inquirente, anche se preventivamente autorizzata dal giudice.[616] Allo stesso tempo, il pubblico ministero, nel fornire nell'OEI l'indicazione circa l'autorità giudiziaria che ha disposto l'intercettazione, deve necessariamente richiamare il previo provvedimento autorizzativo dato dal giudice ai sensi dell'art. 267 cpp.

Rispetto al regime di ammissibilità delle prove digitali acquisite tramite OEI, il silenzio della DOEI si traduce anche nel decreto attuativo. La norma di riferimento è l'art. 33 decreto, la quale stabilisce che "l'autorità giudiziaria che ha emesso l'ordine europeo di indagine concorda con l'autorità di esecuzione le modalità di compimento dell'atto di indagine o di prova, specificamente indicando i diritti e le facoltà riconosciuti dalla legge alle parti e ai loro difensori". Tale disposizione deve essere letta in combinato disposto con l'art. 1 decreto, che sancisce il dovere di rispettare i principi dell'ordinamento costituzionale e della Carta di Nizza. Sebbene vengano prescritte tali regole procedurali, nulla viene detto in merito alle conseguenze procedurali da applicare in caso tali norme siano violate.[617] La direttiva, infatti, si limita a rinviare, in ottemperanza al principio di autonomia procedurale, tramite una clausola di equivalenza, agli strumenti di doglianza già predisposti al livello interno rispetto all'espletamento di simili attività istruttorie.

---

[615] Marcello Daniele, 'L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d. lgs. n. 108 del 2017' (2017) 7-8 Diritto Penale dell'Uomo 208, 210.

[616] Circolare 26 ottobre 2017 - Attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale – Manuale operativo (Ministero della Giustizia 26 ottobre 2017) <https://www.giustizia.it/giustizia/it/mg_1_8_1.page?facetNode_1=0_0&facetNode_2=0_0_2&facetNode_3=4_10&facetNode_4=0_0_2_3&contentId=SDC58426&previsiousPage=mg_1_8> ultimo accesso 29 settembre 2023.

[617] Fabiana Falato, 'La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale' (2018) Archivio Penale 1, 15.

Capitolo 4

I casi *EncroChat* e *Sky ECC*: le corti nazionali e le nuove piattaforme di comunicazione criptate

1. Introduzione

L'evoluzione delle tecnologie di comunicazione ha portato ad una crescente complessità nella lotta contro la criminalità. In questo contesto, diventa essenziale sviluppare nuovi strumenti investigativi ad alta tecnologia per combattere efficacemente la criminalità e penetrare nelle reti di comunicazione utilizzate per commettere reati gravi.[618] Come già evidenziato, la Convenzione di Budapest, così come l'intervento legislativo del 2008, non hanno disciplinato tali tecniche investigative, che per le loro caratteristiche non riescono a trovare esatta collocazione nell'alveo dei mezzi di ricerca digitali disciplinati dal legislatore, lasciando all'interprete l'arduo compito di adattare, alla luce dei principi nell'ordinamento nazionale, la disciplina vigente alle nuove sfide dell'era tecnologia.

In tal senso, una delle ultime novità delle investigazioni digitali è rappresentata dalle piattaforme di comunicazioni criptate, di recente utilizzate anche dalle organizzazioni criminali per condurre e pianificare i propri traffici illeciti.[619] Recentemente, due tra queste piattaforme, *EncroChat* e *Sky ECC*, sono state scoperte e disattivate all'esito di indagini *cross-border* che hanno visto coinvolti numerosi Stati membri. In particolare, nel luglio 2020, le autorità francesi e olandesi, in una dichiarazione congiunta con l'*Eurojust*, hanno reso noto che i *server* del sistema di comunicazioni criptate *EncroChat* con sede in Francia erano stati smantellati con successo. Tale operazione investigativa, guidata dalle autorità di polizia francesi in collaborazione con le autorità olandesi e l'Europol, attraverso una squadra investigativa comune, ha portato alla raccolta di milioni di messaggi intercettati, poi utilizzati come prove davanti alle corti nazionali di diversi Stati membri. Poiché le autorità francesi hanno guidato la cooperazione nell'ambito della squadra, in base all'art. 13 della Convenzione UE sulla mutua assistenza del 2000,[620] le indagini sono state condotte secondo il diritto processuale penale

[618] Donatella Curtotti *et al*, 'Piattaforme criptate e prova penale' (2023) 3 Sistema Penale 173, 175.
[619] Ibid.
[620] 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 [2000] OJ L 197/3.

francese e le prove raccolte sono state poi condivise utilizzando il quadro normativo stabilito in occasione della creazione della squadra o tramite OEI. Meno di un anno dopo, la polizia e autorità giudiziarie di Belgio, Francia e Paesi Bassi, in stretta collaborazione, con il supporto di *Europol* ed *Eurojust*, sono intervenuti per bloccare un'altra piattaforma di comunicazioni criptate utilizzata dalla criminalità organizzata su larga scala, vale a die la piattaforma *Sky ECC*, raccogliendo informazioni cruciali su oltre un centinaio di operazioni criminali in vari Stati membri dell'Unione.

In assenza di norme armonizzate, al momento di utilizzare i risultati di tali operazioni di fronte alle corti penali nazionali, diversi dubbi sono sorti dovute al fatto che ogni Stato membro ha le proprie norme in materia di acquisizione e ammissibilità delle prove elettroniche, che stabiliscono un diverso equilibrio tra le esigenze investigative e la salvaguardia dei diritti fondamentali e delle garanzie procedurali degli indagati/imputati.

Dunque, in tutta Europa, questi ultimi hanno iniziato a contestare l'utilizzo come prove dei dati raccolti in queste operazioni di fronte ai giudici nazionali, lamentando errori nelle indagini, violazioni delle norme sulla condivisione delle prove stabilite a livello transfrontaliero dalla DOEI e un arbitrario parziale accesso alle prove raccolte. In particolare, in una lettera aperta, un'associazione di penalisti, per la maggior parte coinvolti nella difesa degli utenti di *EncroChat*, provenienti da diversi Stati membri, hanno sostenuto che i messaggi ottenuti tali operazioni non dovrebbero essere ammessi come prove nei vari procedimenti penali nazionali.[621] Questi hanno criticato (i) la mancanza di trasparenza circa lo svolgimento delle indagini che rende difficoltoso per la difesa impugnare le prove raccolte sotto i profili dell'integrità, autenticità e attendibilità, ledendo dunque il diritto ad un equo processo, (ii) il fatto che probabilmente l'attività di *hacking* da parte delle autorità francesi abbia comportato un esercizio di giurisdizione extraterritoriale, violando la sovranità dei singoli Stati membri, ed infine (iii) la contestazione che tali attività possano inoltre aver coinvolto i diritti fondamentali di migliaia di singoli cittadini degli Stati membri, tra cui il diritto al rispetto della vita privata e familiare, il diritto alla libertà di espressione e il diritto alla protezione dei dati personali, senza che sia stato esercitato un adeguato controllo da parte di un'autorità giudiziaria indipendente.[622]

---

[621] Fair Trials, 'Letter of concern regarding evidence obtained from EncroChat hack' <https://www.fairtrials.org/app/uploads/2022/02/EnroChat_LetterofConcern.pdf> ultimo accesso 29 settembre 2023.
[622] Ibid.

Le criticità evidenziate hanno portato ad un crescente dibattito tra le varie Supreme Corti nazionali. In attesa di una pronuncia da parte della CGUE, è interessante, in conclusione di questo elaborato, analizzare gli orientamenti delle varie corti nazionali e le divere soluzioni adottate al fine di stabilire un complesso equilibrio tra i vari interessi caratterizzanti il ruolo della prova digitale nel processo penale, le cui criticità sono state fin qui analizzate principalmente solo nella loro singolarità.

2. La Corte di Cassazione: alla ricerca di un equilibro tra il diritto alla *discovery digitale* e l'esigenza di "segretezza"

La Corte di Cassazione, interrogata circa l'utilizzabilità dei dati ottenuti nelle operazioni *EncroChat* e *Sky ECC,* ha affrontato due diverse tematiche: (i) da un lato, è intervenuta per definire il corretto inquadramento giuridico delle modalità acquisitive, (ii) dall'altro, ha determinato le modalità attraverso cui i dati ottenuti possono essere utilizzati nel processo penale.

Rispetto al primo profilo, la Suprema Corte ha recentemente definito le piattaforme di comunicazione criptate, come *Sky ECC* ed *EncroChat*, come "piattaforme di comunicazione criptata che consentono lo scambio di comunicazioni utilizzando i cc.dd. criptofonini, ovverosia smartphone opportunamente modificati nel software (prevalentemente con il sistema Android o Blackberry) con l'unico scopo di garantirne l'inviolabilità, poiché il relativo sistema operativo è caratterizzato da particolari requisiti di sicurezza che si possono riassumere nella cifratura dei dati trasmessi e di quelli memorizzati, nella possibilità per l'utilizzatore di cancellare, quasi in tempo reale e anche da remoto, l'intera memoria del telefono inserendo un cd. panic code, o nella possibilità di segnalare la presenza di sistemi di individuazione (cd. Imsi Catcher) o di tentativi di aggressione informatica da parte di agenti esterni".[623] Si tratta di comunicazioni che avvengono sfruttando un sistema crittografico c.d. "*end to end*": le conversazioni vengono criptate mediante l'utilizzo di chiavi crittografiche che sono depositate esclusivamente sui dispositivi che colloquiano. Di conseguenza, neanche al gestore del servizio è dato conoscere il contenuto delle comunicazioni, non essendo a lui accessibili le chiavi utilizzate.[624]

[623] Cass. sez. I penale n. 6364 del 15 febbraio 2023.
[624] Cybercrime: rassegna delle novità (gennaio-marzo 2023)' (12 maggio 2023 Sistema penale) <https://www.sistemapenale.it/it/scheda/cybercrime-rassegna-delle-novita-gennaio-marzo-2023> ultimo accesso 29 settembre 2023.

Delineate le caratteristiche di tali piattaforme di comunicazione criptata, secondo i giudici di legittimità occorre distinguere tra due tipi di operazioni: (i) le operazioni di captazione e di registrazione del messaggio cifrato che vengono poste in essere quando il flusso di comunicazione è ancora "in atto", vale a dire "in transito" dal mittente al destinatario; (ii) le operazioni di decriptazione del contenuto del messaggio, finalizzate alla trasformazione di "mere stringhe informatiche" in messaggi intellegibili.[625] Le attività rientranti nella prima categoria sono assimilabili alle tradizionali intercettazioni regolate, al livello interno, agli artt. 266 bis cpp e *ss*, e poi disciplinate dal d. lgs. 108/2017 all'art. 43. Diversamente, l'acquisizione delle *chat* conservate presso il *data set EncroChat* e *Sky ECC*, raccolte e decriptate dalle autorità francesi per poi essere trasmesse, attraverso un OEI, alle autorità italiane, non può essere assimilata alle operazioni di captazione.[626] In questo caso, l'OEI risulta funzionale ad acquisire "messaggi di comunicazioni già avvenuti e conservati presso il server della società che gestisce il servizio di messaggistica ed acquisiti nell'osservanza dell'ordinamento interno francese", secondo la previsione del dettato ex art. 234 bis cpp.[627] I giudici di legittimità colgono l'occasione per specificare che il requisito, previsto dalla norma in esame, del consenso all'acquisizione da parte del "legittimo titolare" di quei documenti o dati conservati all'estero va identificato nella "persona giuridica che può legittimamente disporre del documento". Di conseguenza, "legittimo titolare" non è solo nell'interessato o il *service provider* ma anche la polizia o autorità giudiziaria, che legittimamente conservano i dati.[628]

Rispetto al secondo profilo, la Corte di Cassazione ha affrontato il tema dell'utilizzabilità dei dati raccolti nelle operazioni in esame in due importanti pronunce, giungendo ad un esito *prima facie* divergente, che trova, tuttavia, la sua giustificazione in virtù delle differenti premesse caratterizzanti i due ricorsi.

La Suprema Corte si è pronunciata per la prima volta in materia in occasione di un ricorso in cui veniva contestata la natura meramente riepilogativa della nota fornita alla difesa dai Carabinieri, la quale si limitava a riassumere sommariamente le modalità di acquisizione delle *chat* del sistema *Sky ECC*.[629] Il pubblico ministero aveva infatti preventivamente acquisito, tramite OEI, la trascrizione di tali messaggi scambiati dai soggetti operanti in Italia e aveva

[625]Cass. sez. I penale n. 34059 del 15 settembre 2022, 5.
[626] Ibid, 6.
[627] Ibid.
[628]Cass. sez. IV penale n. 23999 del 5 giugno 2023, motivi della decisione, para 6.
[629] Cass. sez. IV penale n. 32915 del 7 settembre 2022.

rigettato la richiesta della difesa di accedere alla relativa documentazione, comprensiva dei *file* e con annessi i verbali delle attività compiute, consegnata da Europol. Il rifiuto della richiesta della difesa trovava ragion d'essere, secondo la tesi dell'accusa, nella natura informale e segreta degli scambi informativi intervenuto tra forze di polizia di paesi diversi, non utilizzabili a processo. Di conseguenza, l'acquisizione in copia della messaggistica doveva ritenersi sufficiente ai fini del rispetto del diritto alla *discovery* digitale.

I gradi di giudizio inferiore avevano accolto la tesi pubblico ministero: considerando che le prove erano state acquisite tramite l'OEI, vigeva una presunzione di fiducia reciproca che le operazioni di ricerca e acquisizione dei dati fossero stata condotte legalmente da parte delle autorità francesi. Al contrario, la Corte Suprema ha accolto il ricorso, confermando l'inutilizzabilità dei dati acquisiti come prove, anche nell'udienza preliminare, a meno che il diritto alla difesa, e in particolare il principio della parità delle armi, non venissero adeguatamente garantiti.

Nel suo ragionamento la Corte ha sottolineato che "il principio del contraddittorio implica che la dialettica procedimentale non si esplichi soltanto relativamente al vaglio del materiale acquisito ma si estenda alle modalità di acquisizione del predetto materiale. Ciò è funzionale al controllo della legittimità del procedimento acquisitivo, anche nell'ottica delineata dall'art. 191 cod. proc. pen., il quale stabilisce l'inutilizzabilità delle prove acquisite in violazione dei divieti stabiliti dalla legge, proiettando i propri effetti anche nello specifico contesto del procedimento incidentale de libertate, a condizione, naturalmente, che, come nel caso di specie, risulti l'effettiva incidenza dell'elemento dimostrativo in disamina sul convincimento del giudice".[630] Pertanto, per un pieno esercizio del diritto alla difesa deve essere garantita la possibilità di conoscere sia le modalità di svolgimento dell'attività investigativa che la procedura di acquisizione di tali dati. Ciò avviene quando si instaura "una proficua dialettica procedimentale in ordine ad ogni profilo di ritualità, rilevanza, attendibilità e valenza dimostrativa che possa venire in rilievo, nell'ottica dell'imputazione."[631] Il rifiuto da parte del pubblico ministero è stato quindi ritenuto lesivo del principio del contradditorio e delle garanzie della difesa in quanto alla stessa non era stata concessa opportunità di comprendere quale fosse il contenuto degli "scambi

[630] Ibid, 4-5.
[631] Ibid, 5.

informativi" tra le forze di polizia dei due Stati membri e quali fossero state le modalità di acquisizione dei dati.

Nella seconda pronuncia,[632] intervenuta a circa un anno di distanza dalla sentenza appena analizzata, la Corte si trova nuovamente ad affrontare il tema dell'utilizzabilità dei dati raccolti nei casi *EncroChat* e *Sky ECC*, ma dalle premesse, a detta della stessa Corte, differenti. Nel caso in esame, la difesa ha avuto accesso alla documentazione, trasmessa dall'autorità giudiziaria francese alla Procura della Repubblica; quest'ultima ha poi specificato che "si trattava di dati autonomamente acquisiti dalla magistratura francese nell'ambito di procedimenti penali in Francia" e che "trattandosi di informazioni che la legislazione di quello Stato consente di tenere segrete, il Tribunale di Parigi non ha trasmesso la documentazione relativa alle modalità di acquisizione dei dati".[633] In particolare, il codice di procedura francese vigente consente alle autorità giudiziarie, nel corso delle indagini, di avvalersi "di risorse dello Stato soggette al segreto di difesa nazionale" al fine di aver accesso, registrare, archiviare e trasmettere i dati informatici, e se necessario, procedere alla loro decriptazione.[634] Ciò posto, la Corte attesta che l'apposizione del "segreto di difesa nazionale" ha impedito alle autorità giudiziarie francesi di fornire informazioni circa le modalità di acquisizione dei dati, osservando, tuttavia, che alla luce di quanto stabilito dalla DOEI e attuato dal d. lgs. 108/2017, pur dovendo l'OEI avere ad oggetto un'indagine consentita nello Stato di emissione, le modalità di svolgimento della stessa non possono che avvenire secondo le regole dello Stato ricevente l'ordine.[635] Tale assunto trova la sua giustificazione nella presunzione di fiducia reciproca tra gli Stati membri, che permette di presumere il rispetto da parte dell'autorità incaricata del diritto dell'Unione e in particolare dei diritti fondamentali garantiti dalla Corte di Nizza e del principio di proporzionalità, "salvo concreta verifica di elementi di segno contrario".[636] Pertanto, nell'eseguire l'OEI, i diritti della difesa sono regolati dalla legge dello Stato di esecuzione, e lo scrutinio circa il loro rispetto spetta al giudice di tale Stato membro, essendo il giudice dello Stato di emissione legittimato a presumere il loro rispetto.

---

[632] Cass. sez. IV penale n. 23999 del 5 giugno 2023.

[633] Ibid, motivi della decisione, para 2.
[634] Ibid, para 3.
[635] Ibid, para 4.
[636] Ibid.

Allo stesso tempo, viene osservato che le autorità giudiziarie francesi hanno comunque provveduto a fornire documentazione attestante "la regolarità del trasferimento di quei dati su supporto non modificabile", il quale è stato "inviato in plico sigillato" alla Procura italiana.[637] L'attestazione, da parte delle autorità d'oltralpe, di aver decriptato dei dati trasmessi e la constatazione che una simile attività non possa che essere stata compiuta facendo uso di un algoritmo, certifica, secondo la Corte, la genuinità ed integrità dei dati acquisiti, salvo che la difesa contesti diversamente.[638] Tuttavia, non sono stati presentati elementi in tal senso nel ricorso. Alla luce di tali considerazioni, la Corte ha dunque dichiarato l'utilizzabilità dei dati acquisiti tramite OEI.

3. L'orientamento della *Bundesgerichtshof* e il rinvio pregiudiziale della Corte di Berlino

La Corte di Cassazione tedesca ("**BGH**"), interrogata circa l'utilizzabilità dei dati, acquisiti nell'operazione *EncroChat* e trasmessi alle autorità giudiziarie tedesche per mezzo di OEI, si è pronunciata in senso favorevole.[639] La BGH ha basato il suo ragionamento sulla premessa che la base giuridica per l'utilizzo delle prove nei procedimenti penali, vale a dire la Sezione 261 del Codice di procedura penale tedesco, si applica anche ai dati ottenuti attraverso i canali di cooperazione giudiziaria *cross-border*. A differenza del procedimento penale italiano, che dedica un momento formale all'ammissibilità della prova, l'ordinamento tedesco prevede, ex Sezione 261 del Codice, che il giudice eserciti il suo potere decisionale secondo la propria discrezionalità e convinzione sulla base delle prove presentate al processo, che devono essere incluse in un *numerus clausus* di quattro diverse e molto ampie categorie di prove. Pur non essendo dunque previste delle disposizioni *ad hoc* che regolino l'utilizzo delle prove digitali, dal momento che l'utilizzo come prova dei dati digitali acquisiti nell'operazione *EncroChat* potrebbe comportare una violazione del diritto alla riservatezza delle telecomunicazioni, garantito dall'art. 10 della Costituzione tedesca[640],[641] l'organo giudicante, nella sua valutazione, deve tenere conto del principio di proporzionalità. Confermando il *dictum* di precedenti sentenze in tema di OEI, la BGH ribadisce che l'utilizzabilità in un procedimento penale

[637] Ibid, para 3.
[638] Ibid, para 7.
[639] BGH, Decisione 2 marzo 2022 – 5 StR 457/21.
[640] Legge fondamentale della Repubblica Federale di Germania [1949].
[641] BGH, Decisione 2 marzo 2022 – 5 StR 457/21.

tedesco di prove, acquisite e trasmesse tramite OEI, è valutata esclusivamente sulla base del diritto nazionale, non rilevando la circostanza che gli atti di indagine eseguiti nello Stato di esecuzione, in ottemperanza del diritto di suddetto Stato membro, avrebbe potuto essere ordinati ed eseguiti anche nell'ordinamento tedesco. Allo stesso tempo, la Corte ha confermato un suo orientamento precedente,[642] affermando che tali prove possono essere dichiarate inutilizzabili se (i) le modalità di acquisizione risultano in violazione dell'"ordine pubblico tedesco", categoria cui rientrano, ad esempio, i principi costituzionali, o (ii) se fermo restando la correttezza delle modalità acquisitive, l'utilizzo risulti incompatibile con tale ordine pubblico. Sotto questo profilo, se la BGH afferma, senza soffermarsi ulteriormente, che le modalità acquisitive dei dati non violano l'ordine pubblico, e in particolare i diritti umani e i principi costituzionali fondamentali, mentre nessun riferimento viene fatto a possibili violazioni del diritto alla difesa.

In contrasto con l'approccio adottato dalla BGH, nel giugno 2021 il Tribunale di Berlino, dopo aver dichiarato i dati di EncroChat inutilizzabili, ha sollevato una questione pregiudiziale alla CGUE.[643] La Corte di Berlino ha chiesto, in sostanza, se le violazioni del diritto dell'UE da parte delle autorità investigative tedesche nell'acquisizione dei dati tramite OEI debbano impedire l'ammissibilità e l'utilizzo di tali dati come prova nei procedimenti penali nazionali, con la conseguenza di aver un'influenza sulla decisione finale.[644] Il giudice del rinvio parte dalla premessa che l'orientamento giurisprudenziale tedesco ha, fino a quel momento, virato a favore dell'uso dei dati raccolti nell'operazione *EncroChat*. In particolare, nello stabilire, alla luce del principio di proporzionalità, un equilibrio tra le esigenze investigative e la protezione dei diritti fondamentali degli utenti di *EncroChat* interessati, nonostante la gravità delle interferenze con suddetti diritti, il "peso" delle fattispecie di reato da perseguire ha fatto pendere la bilancia a favore del primo gruppo di interessi. [645]

Posta tale premessa, il Tribunale di Berlino domanda alla CGUE se tale valutazione possa ritenersi compatibile con la giurisprudenza della CGUE in tema di ammissibilità delle prove

---

[642] BGH, Decisione 21 novembre 2012 – 1 StR 310/12, paras 21-22.
[643] Decisione del 19 ottobre 2022 – LG Berlin (525 KLs) 279 Js 30/22 (8/22).
[644] Case C-670/22 Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice (24 October 2022) <https://curia.europa.eu/juris/showPdf.jsf;jsessionid=EC96DF526C3215018B87A8851CAB56CB?text=&docid=268449&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2347801> ultimo accesso 29 settembre 2023.
[645] Ibid, para 48.

digitali in ambito domestico, dove la Corte di Lussemburgo sembra aver raggiunto un equilibrio differente tra gli interessi della lotta al crimine e le interferenze delle prove digitali con il diritto ad una vita privata, il diritto alla difesa e la tutela giurisdizionale effettiva, come garantiti dalla Carta. [646] Più specificamente, come sottolineato dal giudice del rinvio, sorgono dubbi sul fatto che l'ammissibilità e l'utilizzo di tali prove violino sia il principio di effettività che il principio di equivalenza, alla luce del ragionamento espresso nella sentenza *LQDN* e ribadito nella sentenza *Prokuratuur*. Secondo il giudice del rinvio, tale bilanciamento, se condotto in base al principio di effettività, che prescrive ai giudici nazionali di prendere in considerazione, nel valutare se escludere o meno la prova, il rischio di violazione del diritto ad un equo processo e in particolare del principio del contraddittorio, avrebbe dovuto portare all'esclusione obbligatoria della prova. Come sottolineato dalla Corte di Berlino, il diritto ad un processo equo è stato violato in più occasioni.[647] In primo luogo, il fatto che i dati richiesti tramite OEI non possano essere esaminati da un perito a causa dell'apposizione di motivi di "segretezza di difesa nazionale" da parte delle autorità francesi è suscettibile di soddisfare le condizioni stabilite dal caso *Grand Steffensen*, citato dalla CGUE in *LQDN*, in base alle quali la corte è tenuta ad escludere tali dati come prove. Inoltre, ad avviso della Corte di rinvio, Eurojust ed Europol e i pubblici ministeri tedeschi hanno ulteriormente ostacolato "l'indagine sui fatti e la difesa", rifiutandosi di consegnare parti del fascicolo del caso, importanti per la difesa, e in primo luogo, di includere in tale fascicolo documenti rilevanti per l'intero procedimento. [648] Secondo il Tribunale di Berlino, il giudice delle indagini preliminari è stato tenuto all'oscuro di tutta una serie di informazioni essenziali, mancando, durante l'intero corso del procedimento, un controllo esterno ed indipendente rispetto alle attività di raccolta e successivo utilizzo dei dati. [649]

In attesa della decisione della CGUE, è interessante osservare come, le motivazioni dedotte nel rinvio pregiudiziale tedesco, siano state portate a sostegno dei motivi di ricorso nel recente caso portato di fronte alla Corte di Cassazione, sopra esaminato.[650] Tuttavia, la Suprema Corte ha censurato una simile analogia, sottolineando come nel caso tedesco le attività eseguite da parte delle autorità francesi "avessero *ab* origine l'obiettivo di mettere successivamente a

[646] Ibid.
[647] Ibid, para 46.
[648] Ibid.
[649] Ibid.
[650]Cass. sez. IV penale n. 23999 del 5 giugno 2023, motivi della decisione, para 4.

disposizione" delle autorità tedesche i dati ottenuti. Se, da un lato, tale distinzione sussiste, dall'altro, non sembra che questa si rifletta o giochi un ruolo determinante rispetto alle interferenze al diritto ad un processo equo, e in particolare alle restrizioni imposte al principio del contradditorio, contestate dalla difesa in entrambi i casi in esame.

4. L'*Hoge Raad* e una rigida applicazione del principio di *mutual trust*

A solo due anni dalla conclusione delle indagini, l'operazione *EncroChat* ha già portato a più di 200 sentenze da parte dei corti olandesi, che nella maggior parte dei casi hanno riconosciuto l'utilizzabilità dei dati raccolti, attraverso un'applicazione del principio di *mutual trust* piuttosto rigida tra Stati nell'ambito delle indagini svolte.[651] Anche nei Paesi Bassi, come nel resto di Europa, la difesa ha più volte contestato l'impossibilità di accedere alle modalità di acquisizione dei dati, diventando così impossibile per le parti esercitare il proprio diritto di difesa e venendo sottratte tali modalità anche alla verifica di legalità da parte dell'organo giudicante. Di fronte alle contestazioni della difesa, le corti olandesi hanno però adottato un approccio differente.[652] I giudici nazionali hanno infatti fatto riferimento alla giurisprudenza della Corte EDU in materia di bilanciamento tra il diritto alla *discovery*, da un lato, e la grande mole di dati sequestrati, che possono contenere anche informazioni su terzi, dall'altro, esaminato al Capitolo 1.[653] Come emerso dalla prassi, i pubblici ministeri olandesi hanno infatti previsto una procedura standard di accesso della difesa ai dati di EncroChat già previamente "filtrati".[654]

Un'applicazione così rigida del principio di *mutual trust* ha recentemente portato a sollevare una questione pregiudiziale di fronte all'*Hoge Raad*, la Corte Suprema olandese ("**HR**"), volta comprendere se i dati estratti dalla polizia francese con un metodo non conoscibile possano essere utilizzati come prove nei procedimenti olandesi sulla base del principio di fiducia reciproca.[655] Prima della pronuncia intervenuta a giugno 2023, l'Avvocato generale ha

---

[651] Jan-Jaap Oerlemans e Dave van Toor, 'Legal Aspects of the EncroChat Operation: A Human Rights Perspective' (2022) 30 European Journal of Crime, Criminal Law and Criminal Justice 309, 309.
[652] Si veda a titolo esemplificativo, Corte di Rotterdam 25 giugno 2021, ECLI:NL:RBROT:2021:6113, para. 3.2.4.
[653] *Sigurđur Einarsson e altri c Islanda*, App no 39757/15 (Corte EDU 4 settembre 2019).
[654] Jan-Jaap Oerlemans e Dave van Toor, 'Legal Aspects of the EncroChat Operation: A Human Rights Perspective' (2022) 30 European Journal of Crime, Criminal Law and Criminal Justice 309, 325. Sotto questo profilo, occorre sottolineare che non essendoci nei Paesi bassi una Corte Costituzionale o una Costituzione, ed essendo invece la CEDU direttamente applicabile, la giurisprudenza della Corte EDU riveste un fondamentale ruolo di guida per le corti olandesi.
[655] Hoge Raad, 13 giugno 2023 ECLI:NL:HR:2023:913.

presentato le sue conclusioni, suggerendo un'applicazione più indulgente del principio di "*mutual trust*".[656] In particolare, l'Avvocato generale ha sottolineato che quando un'indagine ha ad oggetto la ricerca e acquisizione di prove digitali, due aspetti principali dovrebbero essere esaminati dall'organo giudicante, vale a dire la legittimità dell'indagine e l'affidabilità dei dati raccolti.[657] Se la raccolta è avvenuta sotto la responsabilità di un altro Stato, parte della CEDU, come nel caso in questione della Francia, il compito delle corti olandesi si limita a garantire che il modo in cui i dati raccolti vengono utilizzati nel procedimento penale non violi il diritto a un equo processo dell'imputato, garantito dall'art. 6 CEDU. Pertanto, il controllo della legittimità della raccolta delle prove è parzialmente limitato dal principio della fiducia reciproca. Al contrario, i giudici olandesi devono valutare l'affidabilità delle prove digitale indipendentemente dal fatto che esse abbiano un'origine nazionale o straniera.

La Corte, seguendo il parere dell'Avvocato Generale, ha adottato un approccio che favorisce il principio di fiducia reciproca tra gli Stati.[658] In pratica, il tribunale non può valutare se le indagini rispettino le leggi straniere, poiché questo minerebbe la sovranità di un altro paese. Se tuttavia un'indagine violasse i diritti umani garantiti dalla CEDU, l'indagato potrebbe presentare un ricorso nel paese in cui sono state condotte le indagini. La Corte ritiene che le decisioni delle autorità giudiziarie straniere su cui si basano le indagini debbano essere rispettate, a meno che non intervenga una decisione irrevocabile che confermi violazioni gravi rispetto alle leggi applicabili. La Corte sembra preoccuparsi dei diritti dell'indagato e fa riferimento alla giurisprudenza della Corte di Strasburgo per sottolineare che l'utilizzo di prove provenienti da indagini straniere in un processo penale è consentito, a condizione che non violi il diritto a un giusto processo ai sensi dell'art. 6 CEDU, e che il giudice nazionale garantisca la loro "correttezza complessiva". Tuttavia, sorge una domanda legittima su come la difesa possa individuare segni concreti di inattendibilità riguardo alle modalità di svolgimento delle indagini a cui non può accedere a causa delle leggi straniere o dei provvedimenti, anche se legittimi, del paese estero.[659]

---

[656] Hoge Raad, Conclusioni dell'Avvocato generale 9 maggio2023 ECLI:NL:PHR:2023:477.
[657] Ibid, para 5.6.
[658] Hoge Raad, 13 giugno 2023 ECLI:NL:HR:2023:913.
[659]. Roberto De Vita e Marco Della Bruna, 'Corte Suprema dei Paesi Bassi: utilizzabilità all'estero dei dati Sky-ECC e EncroChat' (23 luglio 2023 DEVITALAW) <https://www.devita.law/paesi-bassi-utilizzabilita-sky-ecc-encrochat/#_ftn1> ultimo accesso 29 settembre.

Alla luce delle sentenze che hanno stabilito l'utilizzo dei dati raccolti durante le operazioni *EncroChat* e *Sky ECC*, sembra che le corti nazionali degli Stati membri stiano privilegiando il principio di fiducia reciproca e la necessità di preservare importanti operazioni internazionali di polizia, a discapito dei diritti fondamentali dei soggetti interessati, sacrificando così il principio del giusto processo e subordinando il procedimento penale non ai principi di uno Stato di diritto, ma piuttosto a contingenti "ragioni di Stato".[660]

[660] Ibid.

Considerazioni conclusive

L'analisi fino a qui condotta mira a fornire una ricostruzione del panorama giuridico europeo in relazione al ruolo della prova digitale nel procedimento penale, mettendone in evidenza i principali profili critici e identificando possibili prospettive future. A tal fine, nella prima parte, vengono esaminate le giurisdizioni sovranazionali, rilevando, in primo luogo, come il Consiglio d'Europa abbia assunto, e continui ad assumere, un ruolo pioneristico in materia, mostrandosi attento a recepire gli sviluppi dell'era digitale, non solo attraverso l'adozione di trattati internazionali, ma anche con un'intensa attività di *soft law*, che fornisce una preziosa guida "tecnica" per le autorità nazionali. Allo stesso tempo, sebbene l'UE sembri recepire l'influenza rispetto alle iniziative del Consiglio d'Europa in materia, queste ultime vengono, tuttavia, tradotte e adattate dal legislatore dell'Unione alla luce della differente cooperazione giuridica esistente tra Stati membri in materia penale nello SLSG, governato dai principi del mutuo riconoscimento e della fiducia reciproca. E se, come evidenziato dall'analisi svolta, il legislatore sovranazionale sembra aver speso le proprie risorse al fine di rendere, alla luce degli ostacoli posti dalla natura della prova digitale, la cooperazione transnazionale più efficiente, diverso è il ruolo assunto dalla Corte EDU e dalla CGUE. Le due Corti europee hanno cercato di bilanciare le esigenze delle autorità investigative di fronte a tali ostacoli con la necessità di rispettare i diritti fondamentali degli individui affetti dalle misure investigative informatiche, attraverso un'interpretazione evolutiva dei diritti ad una vita privata e ad un processo equo garantiti dalla CEDU e dalla Carta.

Alla luce di queste prime considerazioni, è possibile trarre una prima conclusione: al fine di ricostruire l'attuale materia processuale penale anche solo in chiave domestica, non è più possibile adottare una prospettiva che guardi solo a ciò che accade entro i confini nazionali. Oggi, il livello sovraordinato europeo con le relative scelte di politica criminale incide, attraverso le norme di recepimento, *tout court*, sulla dimensione sotto ordinata nazionale.[661] Una simile influenza è ancora più pregnante in una materia come quella delle indagini informatiche e della prova digitale, in cui i legislatori e le corti nazionali sembrano "brancolare nel buio" e che, allo stesso tempo, è in grado di mettere "in crisi" quel sistema di valori e garanzie individuali, fondanti le "carte dei diritti fondamentali" tanto nazionali che europee.

[661] Fabiana Falato, 'La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale' (2018) Archivio Penale 1, 5.

Del resto, è possibile osservare quanto appena esposto esaminando il quadro normativo italiano in materia, in cui è evidente un'attenzione da parte del legislatore e del giudice nazionale, anche se non sempre dai risultati tempestivi, di adeguare la normativa e gli orientamenti ermeneutici interni con i dettati sovrannazionali.

Eppure, anche da un'analisi svolta attraverso la lente europea, è possibile constatare che numerose rimangono le questioni aperte e le contraddizioni da sciogliere. In primo luogo, occorre sottolineare, come è possibile evincere dalla *ratio* sottesa alle varie iniziative legislative, sia nazionali che sovranazionali, esaminate nel presente elaborato, che la materia in esame è un'area del diritto procedurale penale in cui il già difficile bilanciamento tra esigenze contrastanti si scontra quotidianamente con le dinamiche politiche: in un clima pro-securitario, di fronte alle minacce sempre più pressanti di una criminalità digitale che si trova sempre un passo avanti rispetto agli operatori del diritto, si evidenzia una tendenza a relegare gli interventi legislativi al presentarsi di situazioni emergenziali in un'ottica che, più che regolare nuove garanzie procedurali, deroga a quelle vecchie. In secondo luogo, le scarse iniziative legislative in materia finiscono comunque per diventare presto obsolete di fronte ad un rapido evolversi delle tecnologie digitali. Ad esempio, la portata innovativa della Convenzione di Budapest nell'ordinamento italiano con la legge 48/2008 è stata travolta da un'entrata in vigore della riforma coincidente con la diffusione di nuovi mezzi di ricerca, le c.d. indagini informatiche *online,* e in particolare del captatore informatico, su cui la legge 48 è del tutto silente. E ancora, se ad oggi, come sottolineato al Capitolo 4, le corti nazionali, in attesa di una risposta della CGUE, si chiedono come qualificare al livello processuale il fenomeno delle piattaforme di comunicazioni criptate e, soprattutto, come utilizzare i miliardi di dati raccolti in indagini *cross-border* all'insegna della fiducia reciproca e dell'opposizione di segreti di Stato, la tecnologia è già passata oltre.

Di fronte ai delineati profili critici, sembra opportuno domandarsi se mai possano esistere delle prospettive future che riducano il divario tra le opportunità investigative presentate dalla prova digitale e una cornice normativa inadeguata a coglierle, rispettando al contempo le garanzie procedurali dell'indagato/imputato e i diritti fondamentali di terzi. Una domanda a cui il presente elaborato tenta di rispondere, analizzando la materia sotto una prospettiva non solo *de iure condido* ma anche *de iure condendo*.

Per quanto concerne le modalità acquisitive due sono gli aspetti che in futuro potrebbero contribuire a rendere più efficiente le modalità di acquisizione e conservazione della prova digitale.

In primo luogo, dedicare maggiore attenzione alla formulazione di linee guida e *best practices*. Sebbene, tali strumenti di *soft law* non siano di per sé sufficienti al fine di regolare la materia delle indagini informatiche, possono comunque avere un ruolo complementare che aiuti a ridurre il divario informativo esistente tra le autorità investigative e gli organi giudicanti.

In secondo luogo, il nuovo quadro di cooperazione diretta con i *service providers* adottato dal Consiglio d'Europa e poi oggetto di un nuovo pacchetto legislativo anche al livello di Unione europea, potrebbe rappresentare la chiave di volta del sistema di acquisizione della prova digitale. Ciò alla luce del fatto che non solo le procedure ivi previste permetteranno di avere un quadro giuridico certo e celere, e non più basato su un'infelice alternativa tra cooperazione volontaria e canali diplomatici, ma anche rispetto alla contestazione che un'europeizzazione della materia permetterà di stabilire presto nuove forme di cooperazione con gli Stati Uniti, sede della maggior parte dei *service providers* attualmente sul mercato. Allo stesso tempo, un quadro giuridico, come quello adottato dal Regolamento e Direttiva UE esaminati, che non vede più una cooperazione con le autorità competenti di un atro Stato membro, ma direttamente con i privati, richiede un livello di *mutual trust* tra Stati membri ancora più elevato rispetto, ad esempio, a quello richiesto, dalla DOEI. Sotto questo profilo, sarà interessante osservare come una simile premessa in astratto possa tradursi in concreto in un'Unione europea in cui attualmente regna un clima di segno opposto, di "*mutual distrust*". Sul punto occorre infine segnalare la scelta di affidare ai privati il complesso e delicato ruolo di "guardiani dei diritti fondamentali" di fronte alle sempre più invasive, e non attente alle esigenze della difesa, tecniche investigative.

Rispetto a quest'ultimo profilo, se, da una parte, vanificare, in sede processuale, gli sforzi e il grande impiego di risorse da parte delle autorità investigative, attraverso un'applicazione rigida di garanzie, interpretate ancora secondo i canoni di una società predigitale, non sembra una strada percorribile, allo stesso tempo, un nuovo equilibrio deve essere trovato. Sotto questa prospettiva, indicazioni utili arrivano proprio dalla giurisprudenza europea, che tenta di rileggere la tutela dei diritti fondamentali rispetto alle novità introdotte dalla prova digitale. Se la protezione del diritto ad una vita privata e familiare deve essere ricalibrata rispetto al nuovo significato che assume oggi il concetto riservatezza nella società digitale, allo stesso tempo il

diritto alla difesa non può essere spogliato della sua essenza, anche di fronte ad indagini che hanno ad oggetto milioni di dati, che per la loro volatilità richiedono modalità di acquisizione protette.

Una simile rilettura non può che essere svolta alla luce del principio di proporzionalità, *fil rouge* nella ricerca di un bilanciamento in materia da parte delle giurisprudenze europee e nazionali. Tuttavia, il rispetto del principio di proporzionalità non può essere ridotto ad un mero elenco di garanzie procedurali da "spuntare" da parte dei governi nazionali. Occorre, dunque, che in virtù dei principi di riserva di legge e di giurisdizione, il principio di proporzionalità si erga a "termine necessario di raffronto tra compressione dei diritti quesiti e la giustificazione della loro limitazione",[662] da stabilire prima al livello legislativo, e poi da verificare in concreto, caso per caso, di fronte all'organo giudicante. Un principio la cui essenza risiede nel concetto di "stretta necessarietà", che impedisce che di fronte agli ostacoli posti dalla natura della prova digitale la deroga ai diritti fondamentali diventi regola, perdendo la sua natura di eccezione. Da qui è possibile muovere una conclusione finale: il procedimento penale deve rimane il luogo dell'accertamento di un determinato fatto di reato attraverso un percorso di prestabilite garanzie, non dovendosi mai trasformare, anche di fronte alle nuove sfide e minacce del mondo digitale, in un'occasione di "lotta di contrasto alla criminalità".

[662] Cass. sez. VI penale n. 34265 del 22 settembre 2020, 7.

FONTI

LEGISLAZIONE

CONSIGLIO D'EUROPA

Consiglio d'Europa, 'Convenzione Europea dei Diritti dell'Uomo' (1950) ETS 5.

Consiglio d'Europa, 'Convenzione europea di assistenza giudiziaria in materia penale' (1959) STE No 030.

Council of Europe, Convention on Cybercrime (Budapest Convention on Cybercrime) (2001) ETS No 185.

Versione in italiano: Osservatorio Permanente sulla Criminalità Organizzata, 'Convenzione del Consiglio d'Europa sulla Criminalità Informatica' <https://www.poliziadistato.it/statics/14/convenzione-cybercrime.pdf> ultimo accesso 29 settembre 2023.

Council of Europe, 'First Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems' (2003) ETS 189.

Council of Europe, 'Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence' (2022) CETS 224.

UNIONE EUROPEA

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 [2000] OJ L 197/3.

Decisione Quadro del Consiglio del 13 giugno 2002 relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (2002/584/GAI) OJ L 190/1.

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche OJ L 201/37.

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 [2003] OJ L 196/45.

Direttiva 2006/24/CE del Parlamento e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione [2006] OJ L 105/54.

Direttiva 2006/123/CE del Parlamento Europeo e del Consiglio del 12 dicembre 2006 relativa ai servizi nel mercato interno [2006] OJ L 376/36.

Versione Consolidata del Trattato sull'Unione Europea [2008] OJ C 326/13.

Versione Consolidata del Trattato sul funzionamento dell'Unione Europea [2008] OJ C 115/47.

Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale [2014] OJ L 130/1.

Carta dei diritti fondamentali dell'Unione europea [2016] OJ C 364/1.

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 [2016] OJ L 119/1.

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 [2016] OJ L 119/89.

'Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE' COM(2017) 10 final.

Direttiva (UE) 2018/1972 del Parlamento Europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche [2018] OJ L 321/36.

'Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale' COM(2018) 225 final

'Proposta di Direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali' COM(2018) 226 final.

Council of the European Union, 'Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - general approach' [2019] 2018/0108(COD).

European Parliament, 'Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters'[2020] < https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html#_section1> ultimo accesso 29 settembre 2023.

Testo di compromesso <https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf> ultimo accesso 29 settembre 2023.

Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio del 12 luglio 2023 relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali [2023] OJ L 191/118.

Direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio del 12 luglio 2023 recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali [2023] OJ L 191/181.

ITALIA

Costituzione della Repubblica Italiana [1948]

Codice di procedura penale [1988].

Legge 23 dicembre 1993 n. 547.

Decreto legislativo 30 giugno 2003, n. 196.

Decreto-Legge 24 dicembre 2003, n. 354

Decreto legislativo 7 marzo 2005, n. 82.

Legge 31 luglio 2005, n. 155.

Legge 18 marzo 2008, n. 48.

Decreto-Legge 18 febbraio 2015, n. 7.

Decreto legislativo 3 ottobre 2017, n. 149.

Decreto legislativo 21 giugno 2017, n. 108

Decreto-Legge 30 settembre 2021, n. 132.

GERMANIA

Legge fondamentale della Repubblica Federale di Germania [1949].

Codice di procedura penale tedesco (Strafprozeßordnung – StPO) [1987].

GIURISPRUDENZA

CORTE EUROPEA DEI DIRITTI DELL'UOMO

Klass e altri c Germania, App no 5029/71 (Corte EDU 6 settembre 1978).

Deweer c Belgio, App no 6903/75 (Corte EDU, 27 febbraio 1980).

Schenk c Svizzera, App no 10862/84 (Corte EDU 12 luglio 1988).

Kostovski c Olanda, App no 11454/85 (Corte EDU 20 novembre 1989).

Huvig c Francia, App no 11105/84 (Corte EDU 24 aprile 1990).

Mantovanelli c Francia, App no 21497/93 (Corte EDU 18 marzo 1997).

Echeverri Rodriguez c Olanda, App no 43286/98 (Corte EDU 27 giugno 2000).

Khan c Regno Unito, 35394/97 (Corte EDU 4 ottobre 2000).

Petri Sallinen e altri c Finlandia, App no. 50882/99 (Corte EDU 27 settembre 2005).

Jalloh c Germania, App no 54810/00 (Corte EDU 11 luglio 2006).

Copland c Regno Unito, App no 62617/00 (Corte EDU 3 luglio 2007).

Wieser e Bicos Beteiligungen GmbH c Austria, App no 74336/01 (Corte EDU 16 ottobre 2007).

Aleksandr Zaichenko c Russia, App no 39660/02 (Corte EDU 18 febbraio 2010).

Gäfgen c Germania, App no 22978/05 (Corte EDU 1° giugno 2010).

A.M. c Italia App no 40020/03 (Corte EDU 13 luglio 2012).

Robathin c Austria, App no 30457/06 (Corte EDU 3 ottobre 2012).

Dragojević c Croatia, App no 68955/11 (Corte EDU, 15 gennaio 2015).

Roman Zakharov c Russia, App no 47143/06 (Corte EDU 4 dicembre 2015).

Karabeyoğlu c Turchia, App no 30083/10 (Corte EDU 7 giugno 2016).

Ibrahim e altri c Regno Unito, Apps nos 50541/08, 50571/08, 50573/08 e 40351/09 (Corte EDU 13 settembre 2016).

Lazoriva c Ucraina, App no 6878/14 (Corte EDU 17 luglio 2018).

Sigurđur Einarsson e altri c Islanda, App no 39757/15 (Corte EDU 4 settembre 2019).

Ayetullah Ay c Turchia, Apps nos 29084/07 and 1191/08 (Corte EDU 27 ottobre 2020).

Saber c Norvegia, App no 459/18 (Corte EDU 17 dicembre 2020).

Liebscher c Austria, App no 5434/17 (Corte EDU 6 aprile 2021).

Centrum för Rättvisa c Svezia, App no 35252/08 (Corte EDU 25 maggio 2021).

Big Brother Watch e altri c Regno Unito, Apps nos 58170/13, 62322/14 e 24960/15 (Corte EDU 25 maggio 2021).

Negulescu c Romania, App no 11230/12 (Corte EDU 31 maggio 2021).

CORTE GIUSTIZIA DELL'UNIONE EUROPEA

Opinione Corte 2/13, *Adhésion de l'Union à la CEDH* [2013] ECLI:EU:C:2014:2454.

Caso C-399/11, *Stefano Melloni c Ministerio Fiscal* [2013] ECLI:EU:C:2013:107.

Casi C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECLI:EU:C:2014:238.

Caso C-419/14, *WebMindLicenses* [2015] ECLI:EU:C:2015:832.

Casi C-404/15 and C-659/15 PPU, *Aranyosi e Căldăraru* [2016] ECLI:EU:C:2016:198.

Casi C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* [2016] ECLI:EU:C:2016:970.

Caso C-207/16, *Ministerio Fiscal* [2016] ECLI:EU:C:2018:788.

Caso C-216/18 PPU, *LM* [2018] ECLI:EU:C:2018:586.

Caso C-64/16, *Associação Sindical dos Juízes Portugueses contro Tribunal de Contas* [2018] ECLI:EU:C:2018:117.

Caso C-310/16, *Dzivev and Others* [2019] ECLI:EU:C:2019:30.

Caso C-511/18 *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791.

Caso C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2021] ECLI:EU:C:2020:790.

Caso C-852/19, *Gavanozov II* [2021] ECLI:EU:C:2021:902.

Caso C-746/18 *Prokuratuur - Conditions d'accès aux données relatives aux communications électroniques* [2021] ECLI:EU:C:2021:152.

Caso C-746/18 *Prokuratuur - Conditions d'accès aux données relatives aux communications électroniques* [2020] ECLI:EU:C:2020:18 Opinione dell'AG Pitruzzella.

Caso C-140/20, *G.D. c Commissioner of An Garda Síochána e altri* [2022] ECLI:EU:C:2022:258.

Caso C-276/01, *Joachim Steffensen* [2003] ECLI:EU:C:2003:228.

Rinvii pregiudiziali alla Corte di Giustizia dell'Unione europea

Case C-241/22 Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice <https://curia.europa.eu/juris/showPdf.jsf?text=&docid=261123&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2345814> ultimo accesso 29 settembre 2023.

Case C-241/22 Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice <https://curia.europa.eu/juris/showPdf.jsf?text=&docid=261123&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2345814> ultimo accesso 29 settembre 2023.

ITALIA

Corte d'appello di Bologna, sez II penale n. 1823 30 gennaio 2008.

Sez. Unite sentenza n. 18253 del 7 maggio 2008.

Cass. sez. VI penale n. 241318 del 31 ottobre 2008.

Cass. sez. IV penale n. 40903 del 28 giugno 2016.

Sez. Unite sentenza n. 40963 del 20 luglio 2017.

Cass. sez. VI penale n. 1822 del 17 gennaio 2020.

Cass. sez. VI penale n. 12975 del 27 aprile 2020.

Cass. sez. VI penale n. 34265 del 22 settembre 2020.

Cass. sez. II penale n. 35447 del 21 ottobre 2020.

Cass. sez. I penale n. 34059 del 15 settembre 2022.

Cass. sez. IV penale n. 32915 del 7 settembre 2022.

Cass. sez. II penale n. 39529 del 1° luglio 2022.

Cass. sez. I penale n. 6364 del 15 febbraio 2023.

Cass. sez. IV penale n. 23999 del 5 giugno 2023.

Corte Costituzionale n. 170/2023.

GERMANIA

Decisione del 19 ottobre 2022 – LG Berlin (525 KLs) 279 Js 30/22 (8/22).

BGH, Decisione 21 novembre 2012 **–** 1 StR 310/12.

BGH, Decisione 2 marzo 2022 – 5 StR 457/21.

Bundesverfassungsgericht del 27 febbraio 2008 1 BvR 370/07.

OLANDA

Corte di Rotterdam 25 giugno 2021, ECLI:NL:RBROT:2021:6113.

Hoge Raad, Conclusioni dell'Avvocato generale 9 maggio 2023 ECLI:NL:PHR:2023:477.

Hoge Raad, 13 giugno 2023 ECLI:NL:HR:2023:913.

BIBLIOGRAFIA

LIBRI E DOTTORATI DI RICERCA

Adam R e Tizzano A, *Lineamenti del Diritto dell'Unione europea* (Quarta Edizione Giappichelli Editore 2019).

Biasiotti MA *et al* (eds), *Trattamento e scambio della prova digitale in Europa*, (Edizioni scientifiche italiane 2016).

Cadoppi A *et al* (eds) *Trattati giuridici – Cybercrime* (2019 Utet Giuridica).

Caianiello M e Camon A (eds) *Digital Forensic Evidence Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Wolters Kluwer 2021).

Casey E, *Digital evidence and computer crime* (Academic Press 2000).

Conti C (ed), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi* (Giuffrè, Milano, 2011).

Giuffrida F and Ligeti K (eds) *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings* (University of Luxembourg 2019).

Hoerber T *et al* (eds.), *The Routledge Handbook of European Integrations* (prima edizione, Routledge 2021).

Luchtman M *et al* (eds) *EU Enforcement Authorities - Punitive Law Enforcement in a Composite Legal Order* (Hart Publishing 2023).

Marcolini S e Flor R, *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato* (Giappichelli 2022).

Mason S e Seng D (eds) *Electronic evidence* (quarta edizione, OBserving Law – IALS Open Book Service for Law 2017).

Mitsilegas V et al (eds) *Research Handbook on EU Criminal Law* (Edward Elgar Publishing Limited 2016).

Mitsilegas V, *EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe,* (Oxford Hart Publishing 2016).

Pittiruti M, *Digital evidence e procedimento penale* (Giappichelli editore 2017).

Ruggeri S (ed), *Transnational Evidence and Multicultural Inquiries in Europe* (Springer 2014).

Spangher G and Della Ragione L, *Codice di procedura penale ragionato* (Neldiritto Editore 2021).

Tonini P e Conti C (eds), *Manuale di Procedura Penale* (Giuffrè editore 2021).

Torre M, 'Indagini informatiche e processo penale' (Dottorato di ricerca in Scienze Giuridiche, Università degli Studi di Firenze, 2016).

Tumber H e Waisbord S (eds), *The Routledge Companion to Media and Scandal* (prima edizione Routledge 2019).

ARTICOLI ACCADEMICI E BLOGPOST

'Mass Surveillance and Snoopers' Charter Human Rights Groups win landmark Mass Surveillance ruling' (25 Maggio 2021 LIBERTY) <https://www.libertyhumanrights.org.uk/issue/human-rights-groups-win-landmark-mass-surveillance-ruling/> ultimo accesso 29 settembre 2023.

Alessia Senor M, 'Come funzionano i trojan di Stato? Analisi delle nuove norme e indicazioni operative' <https://www.altalex.com/documents/news/2018/01/22/come-funzionano-i-trojan-di-stato> ultimo accesso 29 settembre 2023.

Allegrezza S, 'Giustizia penale e diritto all'autodeterminazione dei dati' (2007) Protezione dei dati personali e accertamento penale.

Anderson P *et al*, 'Digital investigations: relevance and confidence in disclosure' (2021) 22 ERA Forum 587, 597.

Colaiocco A, 'La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria' (2019) 1 Archivio Penale 1, 5.

Arena M, ‘La Convenzione di Budapest Del Consiglio d’Europa sulla repressione della Criminalità Informatica’ (2021) CRIO Papers.

Armada I, ‘The European Investigation Order and the Lack of European Standards for Gathering Evidence. Is a Fundamental Rights-Based Refusal the Solution?’ (2015) 6(1) New Journal of European Criminal Law 8.

Bachmaier Winter L, ‘Transnational Criminal Proceedings, Witness Evidence and Confrontation: Lessons from the ECtHR’s Case Law’ (2013) 9(4) Utrecht Law Review 127.

Barbosa e Silva J, ‘The speciality rule in cross-border evidence gathering and in the European Investigation Order—let’s clear the air’ (2019) 19 ERA Forum 485.

Bartoli L e Maioli C, ‘La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti’ (2015) 1-2 Informatica e diritto 139.

Bartoli L, ‘Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature’ (2018) 1 Archivio Penale 1.

Bartoli L, ‘Parità delle armi e *discovery* digitale: qualche indicazione da Strasburgo’ (2022) La legislazione penale 1.

Caggiano G, ‘Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione’ (2018) 2 Rivista di Diritto dei Media 1.

Cajani F, ‘Il vaglio dibattimentale della digital evidence’ (2013) 3 Archivio penale 837.

Calavita O, ‘La Proposta di Regolamento sugli Ordini di Produzione e Conservazione Europei: Commissione, Consiglio e Parlamento a Confronto’ (2021) La Legislazione Penale 1.

Camaldo L, ‘La Direttiva sull'Ordine Europeo di Indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione’ (27 maggio 2014 Diritto Penale Contemporaneo) <https://archiviodpc.dirittopenaleuomo.org/d/3078-la-direttiva-sull-ordine-europeo-di-indagine-penale-oei-un-congegno-di-acquisizione-della-prova-dot#_ftnref> ultimo accesso 29 settembre 2023.

Cardone A, ‘Il sistema del Data Retention come strumento investigativo’ (2021) Giurisprudenza Penale Web, 1.

Chikuruwo S R, ‘The Effects of Volatile Features on Digital Evidence Preservation’ <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4332846> ultimo accesso 29 settembre 2023.

Clough J, ‘A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation’ (2014) Monash University Law Review 698.

Clough J, ‘The Council of Europe Convention on Cybercrime: defining ‘crime’ in a digital world’ (2012) Criminal Law Forum 363.

Conti S, ‘La legislazione in materia di prove digitali nell’ambito del processo penale. Uno sguardo all’Italia’ (2015) 24 Informatica e diritto 153.

Csonka P, ‘The Council of Europe's Convention on cyber-crime and other European initiatives’ (2006) 3 77 Revue internationale de droit penal 473.

Curtotti D *et al*, ‘Piattaforme criptate e prova penale’ (2023) 3 Sistema Penale 173.

Daniele M, ‘Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles’ (2015) 6(2) New Journal of European Criminal Law 179.

Daniele M, ‘L’ordine europeo di indagine penale entra a regime. Prime riflessioni sul d. lgs. n. 108 del 2017’ (2017) 7-8 Diritto Penale dell’Uomo 208.

De Amicis G, ‘Limiti e Prospettive del Mandato Europeo di Ricerca della Prova’ (2011) Diritto Penale Contemporaneo, 1.

de Luca C, ‘Il secondo protocollo aggiuntivo alla convenzione sulla criminalità informatica relativo alla cooperazione rafforzata e alla circolazione di prove elettroniche’ (2022) 3 Processo Penale e Giustizia 648.

De Vita R e Della Bruna M, ‘Corte Suprema dei Paesi Bassi: utilizzabilità all’estero dei dati Sky-ECC e EncroChat’ (23 luglio 2023 DEVITALAW) <https://www.devita.law/paesi-bassi-utilizzabilita-sky-ecc-encrochat/#_ftn1> ultimo accesso 29 settembre.

Falato F, ‘La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall’ordine europeo di indagine penale’ (2018) Archivio Penale 1.

Formici G, ‘The three Ghosts of data retention’: passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione’ (2022) 1 OSSERVATORIO COSTITUZIONALE 125.

Formici G. ‘La data retention saga al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture’ (2021) *DPCE Online* 1361.

Franssen V, ‘The European Commission’s E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?’ (European Law Blog 12 ottobre 2023) <https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/> ultimo accesso 29 settembre 2023.

Garamvölgyi B *et al*, ‘Admissibility of Evidence in Criminal Proceedings in the EU’ (2020) 3 eucrim 201.

Gialuz N e Della Torre J, ‘Lotta alla Criminalità nel Cyberspazio: la Commissione presenta due Proposte per facilitare la Circolazione delle Prove Elettroniche nei Processi Penali’ (2018) 5 Diritto Penale Contemporaneo 277.

Hirsch Ballin M e Galič M, ‘Digital investigation powers and privacy’ (2021) 4 Boom Strafblad 148.

Ho-Dac M, ‘The Principle of Mutual Trust in EU law in the Face of a Crisis of Values’ (EAPIL Blog 22 febbraio 2021)<https://eapil.org/2021/02/22/the-principle-of-mutual-trust-in-eu-law-in-the-face-of-a-crisis-of-values/> ultimo accesso 29 settembre 2023.

Iovene F, ‘Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale’ (2014) 3-4 Diritto Penale Contemporaneo 329.

Karagiannis C, ‘Digital evidence “hidden in the Cloud”: Is “possession” still a relevant notion?’ (2023) 23 ERA Forum 301, 310.

Kusak M, ‘Mutual admissibility of evidence and the European investigation order: aspirations lost in reality’ (2019) *ERA Forum* 19.

Lasagni G, ‘Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della privacy’, (2022) La legislazione penale 1.

Lupária L e Ziccardi G, LE “MIGLIORI PRATICHE” NELLE INVESTIGAZIONI INFORMATICHE: BREVI CONSIDERAZIONI SULL’ESPERIENZA ITALIANA, 1.

Luparia L, ‘La ratifica della Convenzione Cybercrime del Consiglio d’Europa’ (2008) 6 Criminalità informatica 696.

Maioli C e Sanguedulce E, ‘I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008’ (Altalex 7 maggio 2012) < https://www.altalex.com/documents/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008> ultimo accesso 29 settembre 2023.

Malacarne A e Tessitore G, ‘La ricostruzione della normativa in tema di data retention e l’ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?’ 3 Archivo penale 1.

Mcguire M e Dowling S, “Cybercrime: A review of the evidence” (2013) <https://www.semanticscholar.org/paper/Cyber-crime%3A-A-review-of-the-evidence-Mcguire Dowling/56624c6ef4e1d6f4cee7a0ab9a053724806bc669> ultimo accesso 29 settembre 2023.

Naddeo G, ‘Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella “data retention saga” dinanzi alla Corte di Giustizia UE’ (2022) 2 Freedom, Security and Justice: European Legal Studies 188.

Oerlemans JJ e van Toor D, ‘Legal Aspects of the EncroChat Operation: A Human Rights Perspective’ (2022) 30 European Journal of Crime, Criminal Law and Criminal Justice 309.

Palladini V, ‘Data retention e privacy in rete: verso una regolazione conforme al diritto UE?’ 1 Rivista Italiana di informatica e diritto 103.

Panzavolta M e Maes E, ‘Exclusion of evidence in times of mass surveillance. In search of a principled approach to exclusion of illegally obtained evidence in criminal cases in the European Union’ (2022) 26(3) The International Journal of Evidence & Proof 199.

Parodi C, ‘L’acquisizione della prova digitale’ (2019) Il diritto vivente 1.

Petroni G, ‘Il caso Prokuratuur: il difficile dialogo tra le Corti e le conseguenze della sentenza della Corte di Giustizia nell’ordinamento nazionale’ (Giustizia insieme 24 novembre 2021) < https://www.giustiziainsieme.it/en/diritto-ue/2026-il-caso-prokuratuur-il-difficile-dialogo-tra-le-corti-e-le-conseguenze-della-sentenza-della-corte-di-giustizia-nell-ordinamento-nazionale-di-giovanni-petroni?hitcount=0> ultimo accesso 29 settembre 2023.

Pezzuto R, ‘Accesso Transnazionale alla Prova Elettronica mel Procedimento Penale: la Nuova Iniziativa Legislativa della Commissione Europea al Vaglio del Consiglio dell’Unione’ (2019) 1 Diritto Penale Contemporaneo 57.

Pittiruti M, ‘Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus’ (Sistema penale 14 gennaio 2021) <https://www.sistemapenale.it/it/scheda/cass-sez-vi-sent-22-settembre-2020-dep-2-dicembre-2020-n-34265-pres-di-stefano-rel-silvestri.> ultimo accesso 29 settembre 2023.

Quattrocolo S, ‘Processo penale e rivoluzione digitale: da ossimoro a endiadi?’ (2020) 3 Rivista di d Diritto dei Media 121.

Quintel T e D Cole M, ‘Transborder Access to e-Evidence by Law Enforcement Agencies. A first comparative view on the Commission's Proposal for a Regulation on a European Preservation/Production Order and accompanying Directive’ (2018) University of Luxembourg Law Working Paper 1.

Ranaldi G, ‘Processo penale e prova informatica: profili introduttivi’ (*Diritto pubblico europeo rassegna online* 2020) <http://www.serena.unina.it/index.php/dperonline/article/view/7031/7976> ultimo accesso 29 settembre 2023.

Rojszczak M, ‘e-Evidence Cooperation in Criminal Matters from an EU Perspective’ (2022) 85(4) The Modern Law Review, 997.

Sajfert J, ‘The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?’ (European Law Blog 8 giugno 2021) <https://europeanlawblog.eu/2021/06/08/big-brother-watch-and-centrum-for-rattvisa-judgments-of-the-grand-chamber-of-the-european-court-of-human-rights-altamont-of-privacy/> ultimo accesso 29 settembre 2023.

Sanna A, ‘La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati’ (2022) Discrimen 1.

Simonato M, ‘Defence Rights and the use of Information Technology in Criminal Procedure’ (2014) 85 Revue Internationale de Droit Pénal 261.

Smuha N, ‘Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency’ (2018) 8(1) European Criminal Law Review 83.

Spiezia F, ‘International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime’ (2022) ERA Forum 101.

Stoykova R ‘The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations’ (2023) 49 Computer Law & Security Review 1.

Tartara V, ‘La Corte di Giustizia conferma il “divieto di conservazione generalizzata e indiscriminata” dei dati relativi al traffico delle comunicazioni elettroniche per finalità preventive di contrasto alla criminalità. possibili ricadute nell’ordinamento italiano’ (2022) 12 Sistema Penale 173.

Todaro G, ‘Restituzione di bene sequestrato, estrazione di copia e interesse ad impugnare: revirement delle Sezioni Unite’ (2017) 11 Diritto Penale Contemporaneo.

Tondi V, ‘La disciplina italiana in materia di data retention a seguito della sentenza della corte di giustizia UE: il tribunale di Milano nega il contrasto con il diritto sovranazionale’ Sistema penale (7 maggio 2021) <https://www.sistemapenale.it/it/scheda/tribunale-milano-22-aprile-2021-data-retention-corte-giustizia?out=print> ultimo accesso 29 settembre 2023.

Tondi V, ‘Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione’ (2019) 2 Diritto Penale Contemporaneo Rivista Trimestrale 439.

Tosza S, ‘All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order’ (2020) 11 New Journal of European Criminal Law 161.

Tosza S, ‘The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?’ (2023) 2 EDPL 163.

Turanjanin V, ‘When does bulk interception of communications violate the right to privacy? The limits of the state’s power and the European Court of Human Rights Approach’ (2022) 4 International Cybersecurity Law Review.

Tzanou M e Karyda S, ‘Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?’ <http://dx.doi.org/10.2139/ssrn.3970756> ultimo accesso 29 settembre 2023.

Tzanou M, ‘Public Surveillance before the European Courts’ (6 aprile 2022 VerfBlog) <https://verfassungsblog.de/os6-courts-surveillance/> ultimo accesso 29 settembre 2023.

Viafora P, ‘Le intercettazioni di massa all’esame della CEDU’ (2023) Amministrazioni in Cammino, 1.

Yeboah-Ofori A, ‘Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence’ (2020) 6 Journal of Forensic, Legal & Investigative Sciences 1.

Zalnieriute M, ‘A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence’ (4 giugno 2021 Blog of the European Journal of International Law) <https://www.ejiltalk.org/a-dangerous-convergence-the-inevitability-of-mass-surveillance-in-european-jurisprudence/> ultimo accesso 29 settembre 2023.

REPORT E FONTI DI SOFT LAW

Bundesamt für Sicherheit in der Informationstechnik ‘Leitfaden „IT-Forensik“ Version 1.0.1 (März 2011)’ <bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-

Sicherheit/Themen/Leitfaden_IT Forensik.pdf?__blob=publicationFile&v=2.> ultimo accesso 9 giugno 2023.

Circolare 26 ottobre 2017 - Attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale – Manuale operativo (Ministero della Giustizia 26 ottobre 2017) <https://www.giustizia.it/giustizia/it/mg_1_8_1.page?facetNode_1=0_0&facetNode_2=0_0_2&facetNode_3=4_10&facetNode_4=0_0_2_3&contentId=SDC58426&previsiousPage=mg_1_8> ultimo accesso 29 settembre 2023.

Commission of the European Communities, 'GREEN PAPER on obtaining evidence in criminal matters from one Member State to another and securing its admissibility' COM(2009) 624 final.

Commission Staff Working Document, Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' SWD(2018) 118 final.

Commissione dell'Unione Europea, 'Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24)' COM(2011) 225.

Corte Europea dei Diritti dell'Uomo, 'Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza' (31 agosto 2021) <https://www.giustizia.it/cmsresources/cms/documents/guida_cedu_articolo8_agg31ago2021.pdf> ultimo accesso 29 settembre 2023.

Corte Europea dei Diritti dell'Uomo, 'Guida sull'articolo 6 della Convenzione europea dei diritti dell'uomo Diritto a un processo equo (profilo penale)' (30 aprile 2022) <https://www.echr.coe.int/documents/d/echr/Guide_Art_6_criminal_ITA> ultimo accesso 29 settembre 2023.

Council of Europe ed European Union, ‘Data retention in the States Parties to the Budapest Convention on Cybercrime. Survey report 2020’ (2020) <https://rm.coe.int/2088-32-data-retention-report-2020/1680a1f305>, ultimo accesso 29 settembre 2023.

Council of Europe, ‘Explanatory Report to the Convention on Cybercrime’ (2001) ETS 185.

Council of Europe, ‘Explanatory Report to the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters’ (2022) CETS 224.

Council of Europe, ‘Recommendation No. R (95) 13 concerning problems of criminal procedure law connected with information technology’ (1995).

Council of the European Union, ‘Conclusions of the Council of the European Union on improving criminal justice in cyberspace,’ (9 June 2016) <https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf> ultimo accesso 29 settembre 2023.

Council of the European Union, ‘Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2 December 2016, 15072/16; Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward (22 maggio 2017) < https://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf> ultimo accesso 29 settembre 2023.

Council of the European Union, ‘The Stockholm Programme – An open and secure Europe serving and protecting the citizens’ [2009] 17024/09.

Cybercrime Convention Committee (T-CY), ‘T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention)’ (2017) <https://rm.coe.int/16806f943e> ultimo accesso 29 settembre 2023.

Cybercrime Convention Committee, ‘Assessment report, implementation of the provisions of the Budapest Convention. Adopted by the T-CY at its 8th Plenary (5-6 December 2012)’ (2012) < https://www.coe.int/en/web/cybercrime/assessments> ultimo accesso 29 settembre 2023.

Electronic Evidence Guide (2014) <https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf> ultimo accesso 29 settembre 2023.

Eurojust, Data retention regimes in Europe in light of the CJEU ruling of 21 December in Joined Cases C-203/15 and C-698/15 (2017) <https://data.consilium.europa.eu/doc/document/ST-10098-2017-INIT/en/pdf> ultimo accesso 29 settembre 2023.

Fair Trial, 'Policy Brief: The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters' (2018) <https://www.fairtrials.org/app/uploads/2022/02/JUD-IT-Fair-Trials-Policy-Brief-October-2018.pdf> ultimo accesso 29 settembre 2023.

Green paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility COM (2009) 624 final.

Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace (15072/1/16 Brussels, 7 December 2016).

Parlamento Europeo, 'Il diritto al rispetto della vita privata: le sfide digitali. Una prospettiva di diritto comparato' (2018) <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628243/EPRS_STU(2018)628243_IT.pdf> ultimo accesso 29 settembre 2023.

T-CY Cloud Evidence Group, 'Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group' (17 February 2016) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8> ultimo accesso 29 settembre 2023.

Tampere Consiglio europeo 15 e 16 ottobre 1999 Conclusioni presidenziali.

SITOGRAFIA

'iPROCEEDS-2: Launching of the Electronic Evidence Guide v.3.0'<https://www.coe.int/en/web/cybercrime/-/iproceeds-2-launching-of-the-electronic-evidence-guide-v-3-0> ultimo accesso 29 settembre 2023.

Council of Europe, ‘Council of Europe action against Cybercrime’ <https://www.coe.int/it/web/portal/coe-action-against-cybercrime> ultimo accesso 29 settembre 2023.

Cybercrime Convention Committee, ‘The Budapest Convention on Cybercrime: benefits and impact in practice’ (13 luglio 2020) <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac> accesso 29 settembre 2023.

Council of Europe, ‘PRESS RELEASE: Cybercrime: Council of Europe strengthens its legal arsenal’ (17 novembre 2021) <https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a48ca6> ultimo accesso 29 settembre 2023.

European Commission, ‘E-evidence - cross-border access to electronic evidence, Improving cross-border access to electronic evidence’ <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en> ultimo accesso 29 settembre 2023.

Council of the European Union, ‘PRESS RELEASE. Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence’ <https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/> ultimo accesso 29 settembre 2023.

Consiglio dell’Unione Europea, ‘Dichiarazione comune dei ministri della giustizia e degli interni dell'UE e dei rappresentanti delle istituzioni dell'UE sugli attentati terroristici di Bruxelles del 22 marzo 201’ (24 marzo 2016) <https://www.consilium.europa.eu/it/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/> ultimo accesso 29 settembre 2023.

‘Electronic Communications and Privacy Act’ (1986) <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=The%20ECPA%2C%20as%20amended%2C%20protects,conversations%2C%20and%20data%20stored%20electronically> ultimo accesso 29 settembre 2023.

Consiglio dell'Unione europea, 'Accesso alle prove elettroniche: il Consiglio autorizza gli Stati membri a ratificare un accordo internazionale' <https://www.consilium.europa.eu/it/press/press-releases/2023/02/14/access-to-e-evidence-council-authorises-member-states-to-ratify-international-agreement/> ultimo accesso 29 settembre 2023.

'E-Evidence compromise blows a hole in fundamental rights safeguards' (EDRi7 febbraio 2023) <https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/> ultimo accesso 29 settembre 2023.

Consiglio dell'Unione europea, 'Un migliore accesso alle prove elettroniche per combattere la criminalità' <https://www.consilium.europa.eu/it/policies/e-evidence/> ultimo accesso 29 settembre 2023.

Clarifying Lawful Overseas Use of Data Act (CLOUD Act) <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text> ultimo accesso 29 settembre 2023.

Eurojust, 'PRESS RELEASE. Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe' <https://www.eurojust.europa.eu/news/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe> accesso 29 settembre 2023.

Cybercrime: rassegna delle novità (gennaio-marzo 2023)' (12 maggio 2023 Sistema penale) <https://www.sistemapenale.it/it/scheda/cybercrime-rassegna-delle-novita-gennaio-marzo-2023> ultimo accesso 29 settembre 2023.