Università degli Studi di Palermo

AREA RICERCA E TRASFERIMENTO TECNOLOGICO
SETTORE DOTTORATI E CONTRATTI PER LA RICERCA
U. O. DOTTORATI DI RICERCA

Dottorato di ricerca in Pluralismi Giuridici. Prospettive antiche e attuali.
Dipartimento di Giurisprudenza
Diritto processuale penale

DIGITAL EVIDENCE E PROCESSO PENALE: ALLA RICERCA DI UN BILANCIAMENTO TRA SOVRANITÀ, PERSECUZIONE DEI REATI E TUTELA DEI DIRITTI FONDAMENTALI.

LA DOTTORESSA
IOLANDA ROBERTA SOLLIMA

IL COORDINATORE
PROF. VINCENZO MILITELLO

LA TUTOR
PROF.SSA ANNALISA MANGIARACINA

CICLO XXXV
ANNO CONSEGUIMENTO TITOLO 2023/2024

Sommario

CAPITOLO IV

PROVA DIGITALE E COOPERAZIONE GIUDIZIARIA: VERSO UNA NUOVA DISCIPLINA

Introduzione

Negli ultimi decenni, l'evoluzione della tecnologia ha permeato ogni aspetto della nostra vita, rivoluzionando il modo in cui interagiamo e comunichiamo, con inevitabili ripercussioni all'interno del processo penale, riflesso della società.

L'avanzamento delle tecnologie ha generato una vasta gamma di dati e informazioni che possono essere utilizzati come prove e, così, la prova digitale si è affermata come evento cruciale nel panorama giuridico contemporaneo, svolgendo un ruolo sempre più prominente nelle indagini.

La scelta del tema per la presente tesi di dottorato nasce, pertanto, dalla consapevolezza dell'importanza cruciale e crescente che la prova digitale assume nel contesto giuridico, nazionale e globale: un contesto in cui si fatica a disciplinare le innovazioni digitali, che avanzano senza sosta. Peraltro, le sfide che si pongono non riguardano le prove in sé, ma si estendono alla cooperazione giudiziaria, posto che la globalizzazione a cui abbiamo assistito e l'immaterialità degli elementi virtuali determinano la transnazionalità dei crimini e delle prove stesse.

"*E-evidence is of fundamental importance in a huge number of criminal investigations. Far from being limited to cybercrime, it is relevant for some 85% of criminal cases, covering every type of crime in the European Union today*"[1]. Sono queste le parole utilizzate da Didier Reynders, Commissario europeo alla giustizia, nell'introduzione al secondo *SIRIUS EU Digital Evidence Situation Report* e una conferma in tal senso si può ricavare anche dalla Relazione Annuale di Eurojust del 2021[2], dedicata ai 20 anni di cooperazione giudiziaria, nonché dalla più recente Relazione del 2022[3].

L'importanza della prova digitale all'interno del processo penale, non soltanto italiano, è una conseguenza dell'uso sempre più massiccio dei dispositivi informatici e digitali nella vita quotidiana: un processo incrementatosi durante la pandemia da Covid–19. come dimostrano le Relazioni Annuali di Eurojust[4], da cui emerge un incremento dei reati commessi mediante la rete e le comunicazioni criptate.

---

[1] *SIRIUS EU Digital Evidence Situation Report, Second Annual Report,* 2020, p. 5, https://www.ejn-crimjust.europa.eu/ejnupload/News/SIRIUS_DESR_2020.pdf.

[2] Relazione Annuale di Eurojust 2021, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-annual-report-2021-it.pdf, p. 25.

[3] Relazione Annuale di Eurojust 2022, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-annual-report-2022-it.pdf , p. 45.

[4] Relazione Annuale di Eurojust 2022, p. 25 «La quarta conferenza SIRIUS annuale, svoltasi nel dicembre 2021, si è concentrata sulla discussione dell'impatto della pandemia e sulla raccolta di prove elettroniche in relazione alle criptovalute e ai criptoscambi utilizzati per il riciclaggio di denaro, la cui incidenza è notevolmente aumentata dall'inizio della crisi sanitaria legata alla COVID-19».

In questo contesto, tuttavia, è da evidenziare come manchi nel panorama nazionale ed europeo una definizione di prova digitale uniformemente riconosciuta. Sul primo versante, questa assenza definitoria, inevitabilmente, finisce per attribuire un ruolo di supplenza ai giudici, chiamati a coprire i vuoti normativi mediante il ricorso a categorie codificate ovvero utilizzando quel contenitore che è rappresentato dalla prova "atipica" *ex* art. 189 c.p.p.

Sul secondo versante, invece, l'assenza di definizioni incide sull'efficacia della cooperazione giudiziaria in materia penale, che assume un rilievo crescente in ragione della natura transnazionale dei reati e della mobilità delle prove, soprattutto "digitali". Al di là dei profili definitori, quando ci si confronta con la prova "digitale" vengono comunemente enucleate alcune sue caratteristiche e, tra queste, l'immaterialità, la volatilità e la facile alterabilità.

Quanto all'immaterialità, questa è insita nella natura intrinseca di queste prove che non hanno una connotazione fisica e, pertanto, sono difficilmente conciliabili con gli strumenti previsti negli ordinamenti nazionali.

La mancanza di fisicità, inoltre, ne permette lo spostamento da un *server* all'altro, determinando la transnazionalità della prova. Questo fenomeno, alla base del c.c. *cloud computing*[5], è una diretta conseguenza della natura "*borderless"* del cyberspazio e dell'esigenza degli *internet service provider* di migliorare l'efficienza dei servizi offerti, utilizzando *server* localizzati in molteplici Stati e spostando i dati in maniera pressoché continua. Inoltre, la possibilità di perdere la prova digitale o che la stessa sia alterata, richiede l'adozione di particolari cautele per garantire la genuinità degli elementi acquisiti, assicurando al processo un dato conforme all'originale.

Gli strumenti tradizionali di cooperazione giudiziaria in ambito penale – sia quelli fondati sull'assistenza giudiziaria sia sul reciproco riconoscimento – hanno rivelato la loro inefficacia rispetto alla prova digitale se rapportati alla rapidità con cui un dato viene ad esistenza ed è poi modificato o eliminato.

Obiettivo del presente lavoro è quello di analizzare gli sviluppi legati all'acquisizione probatoria degli elementi digitali e le ricadute all'interno del sistema processual–penalistico sul fronte della protezione dei diritti fondamentali, con specifico *focus* sull'acquisizione dei dati in possesso di *provider* esteri, circostanza sempre più frequente a causa dell'ampio utilizzo degli strumenti *di cloud computing*.

[5] Per approfondimenti BONCINELLI V., *Modelli tecnici e disciplina giuridica del c.d*. cloud computing, in *Riv. italiana di informatica e diritto*, 2021, 1, p. 27.

In tale prospettiva, si prenderanno le mosse dalla definizione di prova digitale, o meglio, dalla varietà di definizioni esistenti, e dalla valutazione degli elementi che possono essere ricompresi all'interno di tale categoria, avvalendosi anche di un approccio interdisciplinare che combina elementi di informatica forense e diritto.

Dopo un primo capitolo dedicato esclusivamente alla individuazione dei profili definitori della prova digitale e agli elementi a questa riconducibile, si analizzeranno la legislazione italiana e spagnola e le modalità di acquisizione della prova digitale, valutandone l'efficacia e l'idoneità rispetto alle caratteristiche di quest'ultima.

Una specifica attenzione sarà dedicata alle modalità di acquisizione dei dati da parte degli *internet service provider* esteri, verificando se esistano degli strumenti *ad hoc* per obbligare tali soggetti alla consegna di dati, in relazione ad un procedimento penale, e analizzando eventuali criticità e/o punti di forza.

Successivamente, per meglio comprendere i più recenti sviluppi, si proseguirà con la disamina degli strumenti di cooperazione giudiziaria utilizzati nell'ambito del Consiglio d'Europa e dell'Unione europea, esaminando anche il rispetto dei principi di territorialità e proporzionalità e dei diritti fondamentali.

Tale analisi, pertanto, muoverà dalla Convenzione di Budapest e dal successivo avvento, in ambito europeo, del principio di mutuo riconoscimento, fino ai più recenti sviluppi legati all'ordine europeo di indagine e al "pacchetto" sulla c.d. *e-evidence* approvato dell'Unione europea dopo un lungo negoziato e pubblicato nella Gazzetta ufficiale dell'Unione europea nel luglio 2023.

L'idoneità degli strumenti di cooperazione verrà valutata anche in rapporto a quella che possiamo definire la "crisi del principio di territorialità", causata dall'avvento di Internet e dall'abbattimento di ogni barriera geografica a cui si riconducono la sovranità statale e la giurisdizione territoriale.

Al di là della specifica analisi sulle misure utilizzabili in ambito europeo, la localizzazione dei maggiori *service provider* oltre oceano richiede di analizzare le forme di cooperazione con gli Stati Uniti d'America: in particolare, dal *Cloud Act* fino ai negoziati tra UE e USA, che hanno preceduto il nuovo regolamento sugli ordini europei di produzione e di conservazione dei dati (c.d. pacchetto *e-evidence*).

L'elaborato è volto a tracciare un quadro completo sulla natura e sulle caratteristiche della prova digitale, nonché sulle modalità del suo innesto all'interno del processo penale e sul rapporto con i tradizionali atti di indagine, con specifico sguardo agli ordinamenti italiano e spagnolo. In questo contesto, di rilievo appare l'evoluzione della cooperazione giudiziaria tra Stati nello specifico ambito della prova digitale. Un'indagine che richiede una costante

attenzione verso le pronunce delle Corti nazionali e sovranazionali, alle quali va riconosciuto il merito di avere tentato di colmare il *deficit* normativo, con uno sguardo sempre attento al rispetto dei principi fondamentali degli individui coinvolti da questa tipologia di indagini "a elevato impatto" sul fronte dei diritti.

CAPITOLO I

Lo "statuto" della prova digitale

1.1 La prova digitale: alla ricerca di una definizione

Nell'attuale contesto processuale, nonostante la prova digitale abbia assunto un ruolo fondamentale ai fini delle indagini e del successivo accertamento dei fatti in un numero crescente di procedimenti penali, è da registrare un "*lack of agreement on basic terminology*"[6], mancando una definizione di *digital evidence* uniformemente riconosciuta. Sul piano lessicale, la locuzione digitale, dal latino *"digitus"* – utilizzata[7] in ambito elettronico e informatico in contrapposizione ad "analogico" – fa riferimento alla tecnologia attraverso cui si traducono le informazioni in numeri.

Il termine "*digitus"* rimanda, infatti, alle dita e al modo di effettuare la numerazione: da qui l'utilizzo dell'aggettivo digitale per indicare il processo con il quale una determinata informazione viene cifrata, generalmente attraverso il codice binario. Quest'ultimo, infatti, permette di riprodurre informazioni in linguaggio informatico attraverso una combinazione di due valori (0 e 1).

Detta nozione può indicare non solo gli apparecchi che utilizzano grandezze sotto forma numerica, ma anche i dati presenti in tali *device* e le corrispettive rappresentazioni.

Al riguardo, il Dizionario Garzanti [8] esplicita come tale termine non sia impiegato esclusivamente in riferimento a un dispositivo, ma anche per le informazioni da questo

---

[6] Così CASEY E., *Digital Evidence and Computer Crime. Forensics Science, Computer and the Internet, Elsevier*, 2011, p. XXIV.

[7] Espressione utilizzata principalmente da CASEY E., *Digital Evidence and Computer Crime. Forensics Science, Computer and the Internet*, *passim*; DANIELE M., *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Revista Brasileira de Dereito Procesal Penal*, 2019, vol. 5, 3, p. 1277.; DELGADO MARTIN J., *La prueba digital. Concepto, clases, aportación al proceso y valoración,* in *Diario La Ley*, n. 6, *Sección Ciberderecho*, Wolters Kluwer, 11 aprile 2017; MAGRO SERVET V., *Cómo aportar la prueba digital en el proceso penal?,* in *Diario La Ley*, *Seccìon Doctrina*, n. 9824, Wolters Kluwer , 7 aprile 2021; PITTIRUTI M., Digital evidence *e procedimento penale*, G. Giappichelli Editore, 2017; VACIAGO G., Digital evidence*: i mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato,* Giappichelli Editore, 2012.

[8] Garzanti Linguistica, https://www.garzantilinguistica.it/ricerca/?q=attinente%20ai%20numeri,%20numerico;%20in%20particolare%20si%20dice%20di.

elaborate o gestite. Ebbene, nonostante la diffusione sempre più ampia dell'espressione, il nostro sistema la utilizza unicamente in relazione alla "firma digitale"[9].

La situazione non appare diversa se ci si sposta oltre confine. Gli ordinamenti nazionali dei singoli Stati si occupano, per lo più, di definire i concetti di documento elettronico e firma elettronica – in questo senso si colloca la Spagna – mentre solo un ristretto numero di Stati prevede una definizione all'interno del proprio ordinamento[10].

In dottrina, si fa riferimento alla prova digitale con espressioni differenti e spesso adoperate in maniera promiscua, talvolta non tenendone del tutto in considerazione la natura e le caratteristiche. Si passa, infatti, dalle meno utilizzate prova tecnologica, prova scientifica, prova cibernetica, prova informatica[11], alla più frequente prova elettronica[12] .

---

[9] Al riguardo v. art. 24 d. lgs. 7 marzo 2005 n. 82, c.d. Codice dell'amministrazione digitale, in G.U. n. 112 del 16 maggio 2005 - Suppl. Ordinario n. 93.

[10] É il caso della Lettonia. Il codice di procedura penale, alla *Section* 136. dedicata alla *Electronic Evidence*, prevede: «*Evidence in criminal proceedings may be information regarding facts in the form of electronic information that has been processed, stored, or broadcast with automated data processing devices or systems*». Alcuni Stati, come Francia, Paesi Bassi, Spagna e Slovenia, si limitano a recepire le definizioni della Convenzione sul cybercrime o a definire dati elettronici o prove in formato elettronico.

[11] Il termine informatica, derivante dalla fusione dei termini francesi "*information*" e "*automatique*" indica la «scienza e tecnica che si occupa del trattamento automatico dell'informazione per mezzo di elaboratori elettronici in grado di raccogliere i dati nella propria memoria e di riordinarli secondo il programma assegnato»: così GABRIELLI A., Grande Dizionario Italiano, HOEPLI, https://www.grandidizionari.it/Dizionario_Italiano/parola/I/informatica.aspx?query=informatica. Vedasi anche Garzanti Linguistica, https://www.garzantilinguistica.it/ricerca/?q=informatica e Treccani Vocabolario Online, https://www.treccani.it/vocabolario/informatica_res-edc1d4b0-0020-11de-9d89-0016357eee51/. Il corrispondente aggettivo è, ad oggi, utilizzato per lo più per definire «supporti o elaborati elettronici contenenti dati, informazioni o programmi», Treccani Vocabolario Online, https://www.treccani.it/vocabolario/informatico/ , (consultati 23/01/2023). V. SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, G. Giappichelli Editore, p. 15: «Nel quadro del codice di procedura penale il termine informatica ricorre più volte, specialmente come aggettivazione dei termini "sistema", "programmi", "servizi", "comunicazioni", "dati" e "documenti"».
In ambito italiano, la Corte di Cassazione ha delineato i confini dell'espressione "sistema informatico" con la sentenza n. 3065 del 04 ottobre 1999 ritenendo che il concetto sia riferibile ad una pluralità di apparecchiature che, per compiere le proprie funzioni, si avvalgono di tecnologie informatiche. Queste ultime permettono di memorizzare su supporti adeguati, attraverso impulsi elettronici, dei dati consistenti in rappresentazioni elementari di un fatto, effettuate attraverso combinazioni di simboli numerici (*bit*) in combinazioni diverse.

[12] L'aggettivo "elettronico" fa riferimento all'elettronica in quanto «scienza che si occupa dei fenomeni che interessano gli elettroni e in particolare la conduzione elettrica attraverso il vuoto, gas, conduttori e semiconduttori»: così GABRIELLI A., Grande Dizionario Italiano, cit. SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 12: «In tal senso, l'elettronica si concentra nella realizzazione di circuiti elettrici composti in massima parte da componenti elettronici dedicati all'elaborazione di segnali informativi di natura elettromagnetica ed è posta a fondamento dell'informatica». ABEL LLUCH X. (a cura di), *La prueba electrónica*, Bosch, 2011; ABRAHA H.H., *Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiative*, in *International Journal of Law and Information Technology*, 2021, vol. 29, 2; BORGES BLAZQUEZ R., La *prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajeria instantánea*, in *Rev. Boliv. de Derecho*, 2018, p. 25; BUENO DE MATA F., *Prueba Electronica y Proceso 2.0,* Tirant Lo Blanch, 2014; COLOMBO E., *Ordini europei di produzione e conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento* , in *Cass. Pen.*, 2019, 7, p. 2722; KASPER A., LAURITS E., *Challenges in Collecting Digital Evidence: a legal perspective,* in KERIMKMAE T., RULL A., (a cura di) *The future of law and eTechnologies*, Springer, 2016; ORTIZ PRADILLO J.C., *Problemas procesales de la ciberdelincuencia*, Colex, 2013; PEZZUTO R., *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, in *Dir. Pen. Cont.*, 29 gennaio 2019; TONDI V.,

Una novità si registra rispetto a quest'ultima tipologia di prova sul versante europeo. L'espressione *electronic evidence* o e-*evidence* è infatti oggetto di definizione nel nuovo regolamento della Commissione[13] sull'ordine europeo di conservazione e produzione di "prove elettroniche", approvato il 12 luglio 2023.

Nello specifico, all'art. 3 si precisa come per *"electronic evidence"* debba intendersi ogni dato relativo agli abbonati, al traffico o al contenuto, che sia conservato in formato elettronico da o per conto di un prestatore di servizi[14].

Questa definizione, tuttavia, non sembra assumere portata generale, ma appare limitata ai dati in possesso dei prestatori di servizi destinatari dell'ordine europeo di produzione e conservazione, alla cui analisi si passerà successivamente[15].

Occorre domandarsi cosa possa essere ricondotto all'espressione *digital evidence.*

Se guardiamo al testo della Convenzione di Budapest per la lotta al *cybercrime*[16], primo strumento ideato per fronteggiare e perseguire i crimini legati al mondo digitale,

---

*L'accesso transfrontaliero all'*electronic evidence, *tra esigenze di effettività e tutela dei diritti,* in *Dir. Pen. Cont. Rivista Trimestrale,* 2019, 2, p. 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*, in *New Journal of European Criminal Law*, 2020, vol. 11, p. 161.

[13] Regolamento del Parlamento Europeo e del Consiglio 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, del 12 luglio 2023, n. 1543, in G.U. L. 191 del 28 luglio 2023.

[14] La definizione inizialmente prevista dalla proposta, all'art. 2, considerava dati elettronici quelli relativi agli abbonati, agli accessi, alle operazioni o al contenuto. In seguito, si è preferito inserire l'espressione dati di traffico in sostituzione di dati sugli accessi (*access data*) e sulle operazioni (*transactional data*). Ai sensi di quanto previsto, gli *access data* erano finalizzati a identificare l'utente; riguardando l'inizio o la fine di una sessione di accesso a un servizio, la data e l'ora d'uso, dati di *log in* e *log off*, indirizzo IP, dati delle interfacce usate e identificativo dell'utente. All'interno della categoria andavano ricondotti i metadati relativi alla trasmissione, distribuzione o scambio di comunicazioni elettroniche, compresi quelli idonei a tracciare e identificare fonte e destinatario, i dati sulla localizzazione, data, ora, durata e tipo di comunicazione. I *transactional data* venivano invece definiti come i dati riguardanti la fornitura di un servizio offerto da un prestatore di servizi che servono per fornire informazioni di contesto o supplementari sul servizio, generati o trattati da un sistema di informazione del prestatore di servizi, come la fonte e il destinatario di un messaggio o altro tipo di interazione, i dati sull'ubicazione del dispositivo, la data, l'ora, la durata, le dimensioni, il percorso, il formato, il protocollo usato e il tipo di compressione, a meno che tali dati costituissero dati relativi agli accessi. All'interno di questa categoria venivano ricondotti i metadati delle comunicazioni elettroniche, come definiti all'articolo 4, paragrafo 3, lettera c), del regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche. Cfr. 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 finale. Vedasi testo della proposta emendata, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5448_2023_INIT ed anche 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/.

[15] Regolamento 1543/2023, art. 2 co. 6: «"prove elettroniche": le prove conservate in formato elettronico dal prestatore di servizi o per suo conto al momento della ricezione del certificato di ordine europeo di produzione o di conservazione, consistenti nei dati conservati relativi agli abbonati, agli accessi, alle operazioni o al contenuto».

[16] Convenzione sulla criminalità informatica, firmata a Budapest il 23 novembre 2001, entrata in vigore il 01° luglio 2004, STE n° 185. Cfr. ILARDA G., MARULLO G. (a cura di), Cybercrime: *Conferenza Internazionale: la Convenzione Del Consiglio d'Europa sulla criminalità informatica. Osservatorio permanente sulla criminalità organizzata: 1*, Giuffrè, 2004.

questo utilizza il termine "prova elettronica" o "in formato elettronico", omettendo di offrirne una definizione e neppure nel testo del più recente Secondo Protocollo alla Convenzione di Budapest[17], del quale l'UE ha di recente autorizzato la ratifica[18], vengono indicati i confini di tale nozione.

L'assenza di un concetto univoco, sul quale fare convergere il *consensus* degli Stati, genera indubbiamente dei problemi allorquando si effettuino indagini in relazioni a crimini transnazionali o quando, come spesso accade, informazioni necessarie per le autorità investigative siano archiviate in *server* localizzati in altri Stati[19].

Vieppiù, volendo andare al di là della fase delle indagini, l'assenza di armonizzazione sul tema e la mancanza di regole *ad hoc* per questa tipologia di prove, può generare problemi anche sul fronte della loro ammissibilità, laddove siano state ottenute avvalendosi dei meccanismi di cooperazione giudiziaria.

Secondo autorevole dottrina[20], la *digital evidence* è qualsiasi dato memorizzato o trasmesso usando un *computer*, che supporta o respinge una teoria su come è avvenuto un fatto offensivo o che individua elementi critici dell'offesa come l'intenzionalità o l'alibi.

In questo ambito possono pertanto includersi elementi di vario tipo, tra i quali testi, immagini, audio e video.

Questa definizione può, tuttavia, essere ampliata, riconoscendo la vastità di dati digitali che vengono creati e elaborati da altri *device*, il cui catalogo passa dagli *smartphone* ai computer di bordo delle auto e, perfino, a dispositivi di *health-care* e agli *smartwatch*.

L'espressione potrebbe essere utilizzata come contenitore per tutte le fonti di prova che facciano riferimento al dato digitale, considerando che il massimo comune denominatore è dato dalla circostanza che il dato non è immediatamente percepibile e che la sua natura è collegata a impulsi elettrici e al codice binario.

Quanto ai risultati, infatti, risulta arduo teorizzare un inquadramento della *digital evidence* nella consueta bipartizione tra prove rappresentative-dirette e prove critiche-indirette[21]. Ciò in quanto la natura informatica del dato da cui trarre il risultato probatorio

---

[17] Secondo Protocollo Addizionale alla Convenzione sul potenziamento della cooperazione e sull'accesso alle prove elettroniche, aperto alla firma il 12 maggio 2022, CETS n. 224, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 .

[18] Decisione (UE) 2023/436 del Consiglio del 14 febbraio 2023 che autorizza gli Stati membri a ratificare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche, in G.U.U.E. L 63/48 del 28 febbraio 2023.

[19] Per approfondimenti CARPANELLI E., LAZZERINI N. (a cura di), *Use and Misuse of New Technologies. Contemporary Challenges in International and European Law*, Springer, 2019.

[20] CASEY E., *Digital Evidence and Computer Crime. Forensics Science, Computer and the Internet*, cit., p. 7: «*Digital evidence is defined as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi*».

[21] PITTIRUTI M., Digital evidence *e procedimento penale*, cit., p. 8.

può vertere sia direttamente sul *thema probandum*, sia su un fatto secondario da cui risalire al fatto principale: al primo caso è riconducibile un'immagine pedopornografica in formato digitale il cui possesso è contestato all'imputato; al secondo, invece, i file di *log* relativi all'accesso ad un *social network* per mezzo di un computer localizzato sulla *scena criminis*, nell'arco temporale in cui è stato commesso il delitto.

Lo *Scientific Working Group on digital evidence* (di seguito SWGDE)[22] rimanda alla prova digitale come ogni informazione di valore probatorio che è memorizzata o trasmessa in forma digitale[23].

Allo stesso modo, parte della dottrina spagnola[24] ritiene che la prova digitale sia ogni tipo di «*información de valor probatorio contenida o transmitida por un medio electrónico*» capace di dimostrare i fatti all'interno di un processo finalizzato alla persecuzione dei reati.

Seppure il legame con i dispositivi elettronici lasci ipotizzare che la prova digitale possa rappresentare solo fatti ed eventi verificatesi nel cyberspazio, è bene non incorrere in tale errore. Infatti, l'utilizzo sempre più frequente di *device* elettronici per gestire la vita quotidiana o per cristallizzarne alcuni momenti (video e foto) rende tale prova idonea anche a dimostrare fatti fisici.

Se le informazioni contenute in un *computer* possono permettere di ricostruire le operazioni e attività svolte nel mondo virtuale, d'altro canto, informazioni contenute in un dispositivo possono fornire un alibi e ulteriori indicazioni utili su fatti verificatesi nel mondo reale, quando siano relative al suo utilizzo o alla localizzazione di un soggetto.

Alla luce di quanto sin qui esposto, in via generale, la *digital evidence* può essere definita come qualunque tipo di informazione lecitamente ottenuta a partire da un dispositivo elettronico o mezzo digitale, cifrata attraverso un codice binario, che abbia un valore probatorio e permetta di rappresentare all'interno del processo fatti fisici o informatici.

1.2 Le molteplici caratteristiche della prova digitale

Nell'elaborazione dottrinale[25], quando ci si confronta con la prova digitale vi è la tendenza a enucleare le seguenti caratteristiche: l'eterogeneità, l'immaterialità, l'ubiquità, la tracciabilità, la trascendenza, l'oggettività, la volatilità e, infine, la facile alterabilità.

---

[22] Gruppo di lavoro che riunisce più *stakeholder* (forze dell'ordine, membri della comunità accademica, soggetti operanti nell'imprenditoria) che operano nel cambio della *digital forensics*. Cfr. https://www.swgde.org/ .

[23] Letteralmente «*Information of probative value that is stored or transmitted in binary form*». Cfr. SWGDE *Glossary*, https://www.swgde.org/glossary.

[24] DELGADO MARTIN J., *La prueba digital. Concepto, clases, aportación al proceso y valoración,* cit., p.1.

[25] V., tra i tanti ARRABAL PLATERO P., *La prueba tecnológica: aportación, practica y valoración,* Tirant Lo Blanch, 2020; ORTIZ PRADILLO J.C., *Nuevas medidas tecnológicas de investigación criminal para la*

Prendendo le mosse dalla prima delle caratteristiche menzionate, l'eterogeneità, va evidenziato che la *digital evidence* può essere costituita da una grande varietà di elementi, il cui numero non può essere limitato, per via della rapida capacità di evoluzione e innovazione delle tecnologie.

Immagini, video, audio, file di *log*, documenti, dati sulle operazioni, pagine *web*, messaggi, *email*, indirizzi IP sono solo alcune delle tipologie a cui possiamo fare riferimento.

Come già segnalato, infatti, il tratto comune delle prove digitali può essere individuato nella codificazione binaria, in ragione dei vari tipi di fonti di prova e degli elementi e risultati probatori.

Altra caratteristica è quella della immaterialità[26]. Posto che ogni dato è trasmesso utilizzando il codice binario e impulsi elettromagnetici, la prova digitale non è fisicamente percepibile. Questa «carenza di fisicità»[27] determina, come stretta conseguenza, il rischio che la prova sia modificata, cancellata o spostata con estrema facilità da un *server* localizzato in uno Stato ad uno situato in un altro Stato. Quest'ultimo aspetto fa sì che la prova digitale sia considerata come «ontologicamente transnazionale»[28], trovandosi «in una sorta di "meta-territorio", dove sembra perdere consistenza la naturale propensione dell'uomo di rapportarsi al mondo "reale" con l'uso dei cinque sensi»[29].

Ancora, vanno richiamate la volatilità e la facile alterabilità: questi aspetti, strettamente connessi all'immaterialità, fanno sì che qualunque informazione possa essere cancellata in un attimo o manipolata. Ciò può avvenire intenzionalmente o in maniera accidentale, ad esempio semplicemente spegnendo o accendendo un dispositivo ovvero aprendo un *file*.

Pertanto, non vanno sottovalutati i metodi utilizzati nelle indagini, che devono rispondere a regole procedurali e a specifici *standard*, affinché la prova venga acquisita in maniera legittima nel rispetto dei diritti fondamentali delle persone coinvolte, anche al fine di assicurarne l'utilizzabilità sul piano probatorio.

---

obtención de prueba electrónica, in PEREZ GIL J., *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*, La Ley, 2012, p. 273; PITTIRUTI M., Digital evidence *e procedimento penale,* cit.

[26] Parla di «materialità non immediatamente percepibile», PITTIRUTI M., Digital evidence *e procedimento penale,* cit., p. 9.

[27] COSTABILE G., Digital Forensics & Digital Investigation*: classificazione, tecniche e linee guida nazionali ed internazionali,* in ATERNO S., CAJANI F., COSTABILE G., CURTOTTI D., (a cura di) Cyber Forensics *e Indagini digitali. Manuale tecnico-giuridico e casi pratici,* G. Giappichelli Editore, 2021, p. 5.

[28] PITTIRUTI M., *L'apprensione all'estero della prova digitale*, in LUPARIA L., MARAFIOTI L., PAOLOZZI G. (a cura di), *Dimensione tecnologica e prova penale*, G. Giappichelli Editore, 2019, p. 205 ss.

[29] COSTABILE G., Scena criminis*, documento informatico e formazione della prova penale*, in *Dir. Inf.*, 2005, p. 531.

Guardando, inoltre alla caratteristica dell'ubiquità, questa è correlata alla frequente presenza della medesima informazione in più dispositivi, a causa dell'avvento dell'*Internet* e in ragione della sopra citata immaterialità dei dati. Secondo parte della dottrina, è più coerente parlare di plurilocalizzazione[30] della prova piuttosto che di "*loss of location*" o delocalizzazione. I dati relativi all'utilizzo di un *account* o di un'applicazione non sono, infatti, strettamente correlati a un unico dispositivo, ma sono anche nella disponibilità degli *internet service provider.*

Allo stesso modo, se pensiamo a un file conservato nel *cloud*, questo è accessibile dal *provider* e anche dall'utente, che attraverso la semplice connessione può scaricare i dati su illimitati supporti fisici (*smartphone* e *computer*) o permettere ad altri soggetti di visionarli. A oggi, qualunque tipo di dispositivo, dal momento della configurazione richiede l'accesso ad un *account*. In tal modo, ogni nuovo dispositivo viene sincronizzato con i precedenti dati, immagini, file, rubrica dei contatti, cronologia delle *chat* e ogni tipo di informazione creata o archiviata attraverso un altro dispositivo e la copia di ogni nuovo file viene così salvata sul *cloud* per averne la disponibilità su tutti i dispositivi in uso e su quelli futuri.

Sul fronte della tracciabilità, bisogna sottolineare come una delle caratteristiche delle tecnologie informatiche e del cyberspazio risieda nel fatto che ogni operazione lascia una traccia, un'impronta che permette successivamente di identificare l'azione, *l'account* o il dispositivo attraverso il quale è stata compiuta, il momento iniziale e finale e ogni *step* intermedio.

La prova digitale, inoltre, è considerata "trascendentale" poiché oltre ad assumere un rilievo fondamentale per indagare e perseguire i crimini informatici, fornisce informazioni essenziali per ogni tipo di reato, in ragione del legame creato tra le nostre vite e i mezzi elettronici[31].

Va, inoltre, evidenziata la sua oggettività, dal momento che il dato digitale è obiettivo per sua natura e, se non alterato o modificato, fornisce una prova chiara, precisa e neutra.

È, tuttavia, necessario effettuare delle opportune precisazioni: anzitutto, è fondamentale che il dato non sia stato in alcun modo alterato, volontariamente o accidentalmente; in secondo luogo, pur rappresentando in maniera obiettiva un fatto, questo

[30] In tal senso SPIEZIA F., *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: Il ruolo di Eurojust*, in *www.sistemapenale.it*, 14 luglio 2023, p. 6.

[31] ORTIZ PRADILLO J.C., *Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica,* cit., p. 273.

può talvolta mantenere un velo di incertezza se riguarda la corrispondenza tra un indirizzo IP di un dispositivo e la persona fisica che lo abbia utilizzato.

Come si illustrerà in seguito, ogni *device* che si connette alla rete *Internet* viene identificato attraverso un indirizzo IP a questo assegnato e, durante le indagini, una delle prime operazioni eseguite per identificare un soggetto risiede nella ricerca del suddetto indirizzo e del dispositivo connesso. Tuttavia, non solo è arduo avere certezza del soggetto che abbia utilizzato un *device* in uno specifico momento ma, inoltre, il rapporto IP-dispositivo potrebbe risultare falsato o manomesso.

Si parla di "maschera elettronica" o "*media electrónica*"[32] per indicare la facilità con cui il cyberspazio si presta a mantenere l'anonimato, a costruire identità fittizie o a usurpare altrui identità, complicando la possibilità di identificazione di un soggetto.

È, infatti, necessario tenere in considerazione che l'assegnazione di un indirizzo IP a un dispositivo può essere aggirata con più tecniche[33].

Tra queste, possono richiamarsi le seguenti:

- la connessione a reti *wireless* aperte o non controllate, facilmente violabili;
- l'anonimizzazione attraverso specifici *proxy*[34], che permettono di effettuare operazioni avvalendosi dell'indirizzo IP del *proxy* stesso, o di *proxy chain*, costituiti da catene di *server* che attraverso l'instradamento rendono la comunicazione totalmente anonima.

1.3 La classificazione delle prove digitali

Come anticipato, l'elemento comune alle prove digitali può essere individuato nella codificazione di tipo binario, seppure la varietà degli elementi e delle fonti di prova sia ampia.

---

[32] ARRABAL PLATERO P., *La prueba tecnológica: aportación, practica y valoración,* cit., p. 51.

[33] COSTABILE G., *Rete Internet e "dintorni": aspetti tecnici di base*, in ATERNO S., CAJANI F., COSTABILE G., CURTOTTI D., (a cura di) Cyber Forensics *e Indagini digitali. Manuale tecnico-giuridico e casi pratici,* cit., p. 38 ss.

[34] Il *proxy* è un *server* che opera da intermediario nella ricerca di servizi su altri *server*, rendendo quindi visibile il proprio indirizzo IP e mantenendo anonimo quello dell'utente che lo utilizza. V. https://www.aranzulla.it/server-proxy-63922.html .

Tra questi è possibile distinguere:

- prove che possono essere raccolte da siti *web* a disposizione del pubblico (*blog post* o immagini presenti su *social network*);
- prove relative all'identità di un utente o metadati utili per identificare una persona, partendo dalla sorgente della comunicazione;
- prove di contenuto, tra cui e-mail o documenti non disponibili pubblicamente e che sono conservati su un *server* [35].

Benché l'impressione sia quella di percepire l'informazione in maniera diretta, la prova digitale consta di un elemento tecnico su cui è incorporata (*hardware*) e di uno logico (*software*).

Per una valutazione quanto più puntuale, sarebbe utile convogliare la prova in dibattimento attraverso un supporto elettronico, affinché il giudice possa apprezzarne personalmente le varie sfumature. Infatti, pur considerando la possibilità di stampare un'immagine o un documento, il trasferimento dell'informazione da un supporto elettronico a uno cartaceo potrebbe causare la perdita di numerose informazioni connesse, rappresentate dai metadati. Tuttavia, non sempre il giudice gode dell'*expertise* idoneo ad effettuare una tale analisi e, pertanto, la prova digitale viene acquisita al processo attraverso il ricorso alle perizie informatiche e, soprattutto, per mezzo delle dichiarazioni dibattimentali dei periti.

1.3.1 Dati e metadati

È opportuno effettuare una classificazione, non certamente esaustiva, dei vari elementi che possono costituire una prova digitale.

In primis, è necessario operare una distinzione tra dati e metadati.

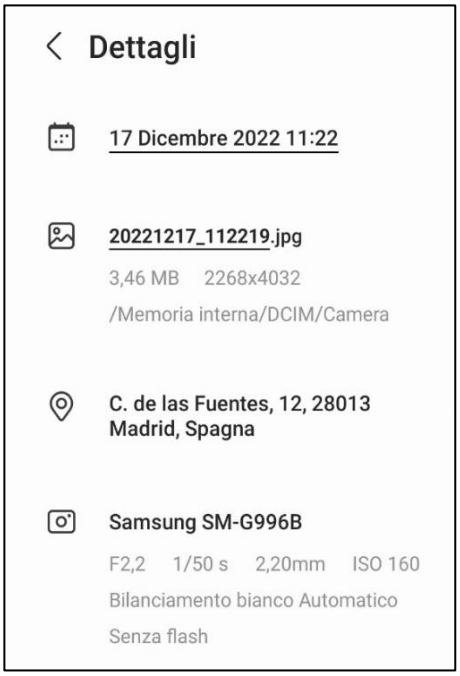
Se assumiamo il dato come la rappresentazione di un'informazione, possiamo identificare il metadato come l'informazione aggiuntiva relativa al dato stesso, «*data about data*»[36]. Questi elementi, visionabili attraverso i dettagli di ogni *file*, sono strettamente legati al dato e forniscono indicazioni sulla creazione dello stesso, sulle modifiche, sull'autore (per

[35] RACHAVELIAS M. G., *Online financial crimes and fraud committed with electronic means of payment – a general approach and case studies in Greece*, in *ERA Forum*, 2018, p. 340.

[36] HASSAN N.A., *Digital Forensics Basics. A practical guide using Windows OS*, cit., p. 43.

esempio, nel caso di *Microsoft Office*[37]), sulle revisioni, sul dispositivo che lo ha generato o sulle coordinate GPS al momento dello scatto di una foto e su ogni altro tipo di informazione che vi si possa ricondurre.

Si riportano, a titolo esemplificativo, degli *screenshoot* effettuati da uno *smartphone*, che forniscono metadati di base su alcune fotografie scattate con il dispositivo.

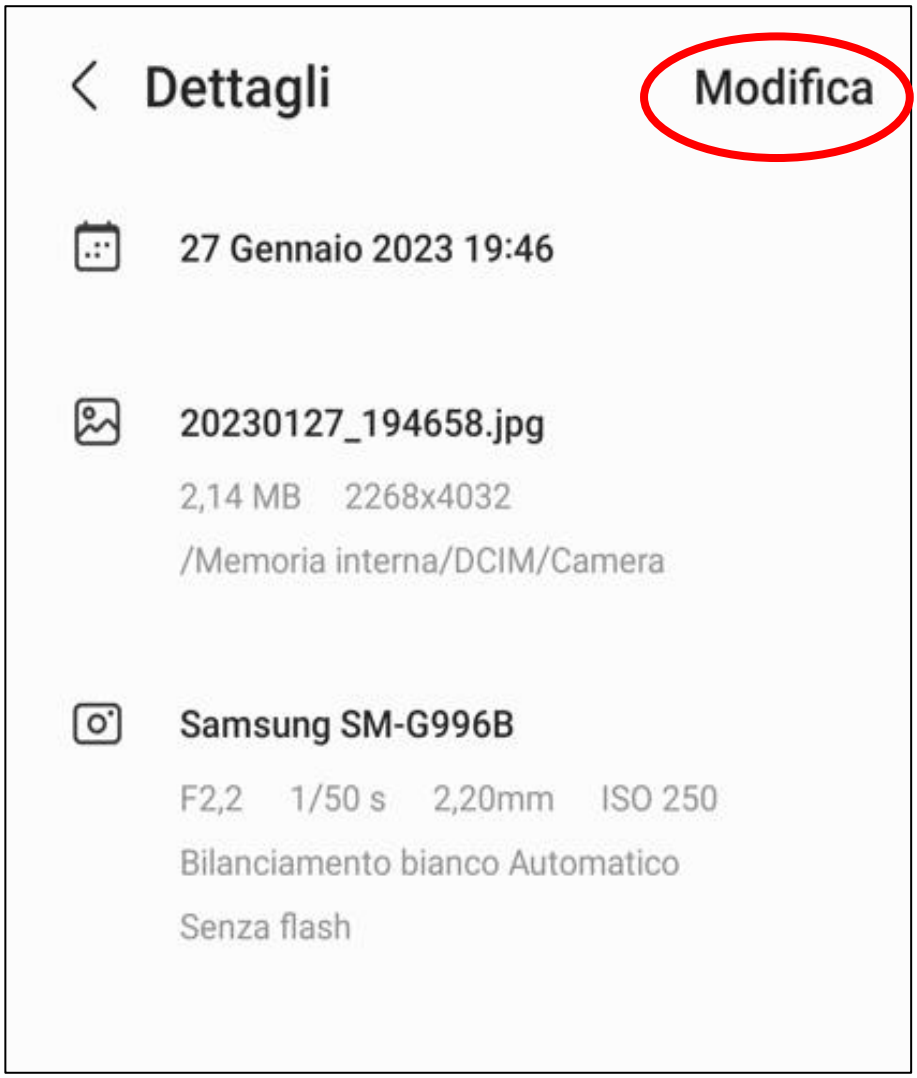


Dalle immagini riprodotte si può constatare come sia possibile visionare con facilità le informazioni relative alla foto: data, ora, nome del file ed estensione, dimensione, risoluzione, localizzazione all'interno delle cartelle del dispositivo, localizzazione GPS, indicazione dello *smartphone* da cui è stata scattata la foto e informazioni sulle modalità di scatto (bilanciamento, apertura dell'otturatore, ISO, tempo di apertura e utilizzo del *flash)*.

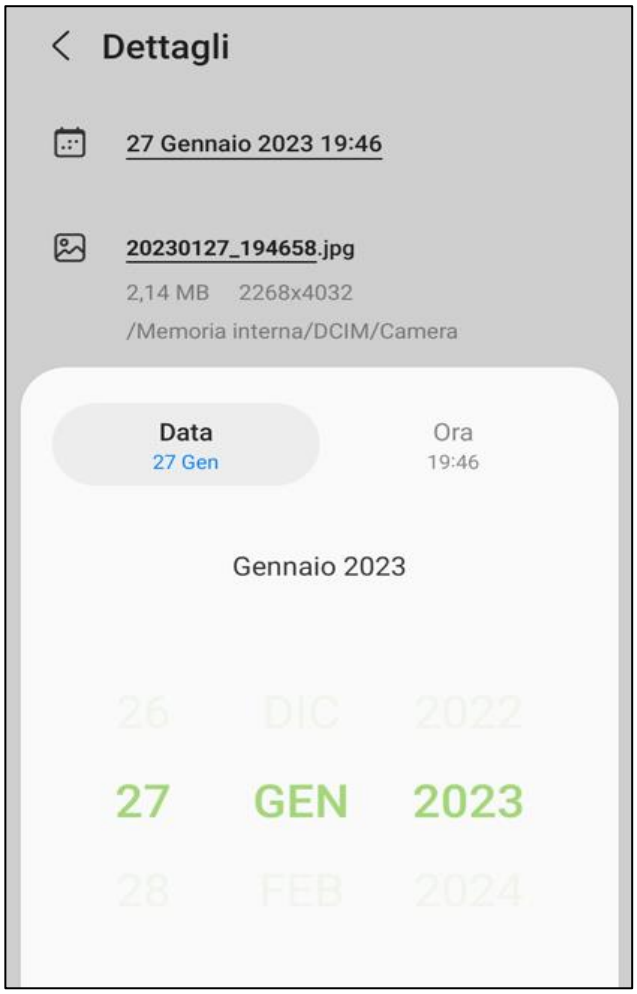
Ciò che si evidenzia è la possibilità di modificare alcune informazioni (data e posizione): circostanza che conferma quanto facilmente possano essere alterate le prove digitali.

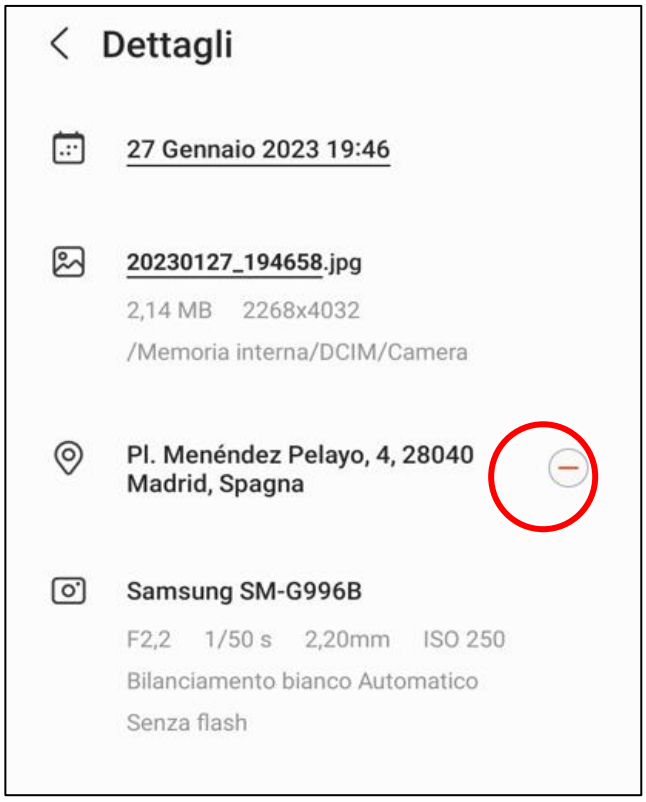
---

[37] «*Microsoft Office files come with a lot of metadata that can be of great interest to a computer forensic examiner. The office metadata holds several pieces of information including:*
• Name of original author,
• Name of the person who last saved the document,
• Original creation date,
• Last save date,
•When the document was last printed
• Total time spent working on the document», KÄVRESTAD J., *Fundamentals of Digital Forensics. Theory, Methods, and Real-Life Applications*, Springer, 2018, p.115.

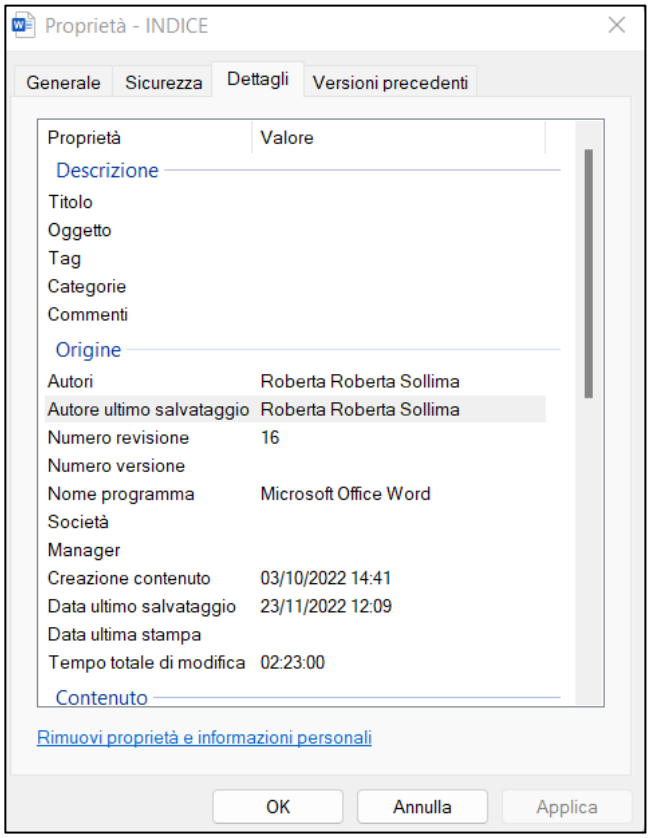


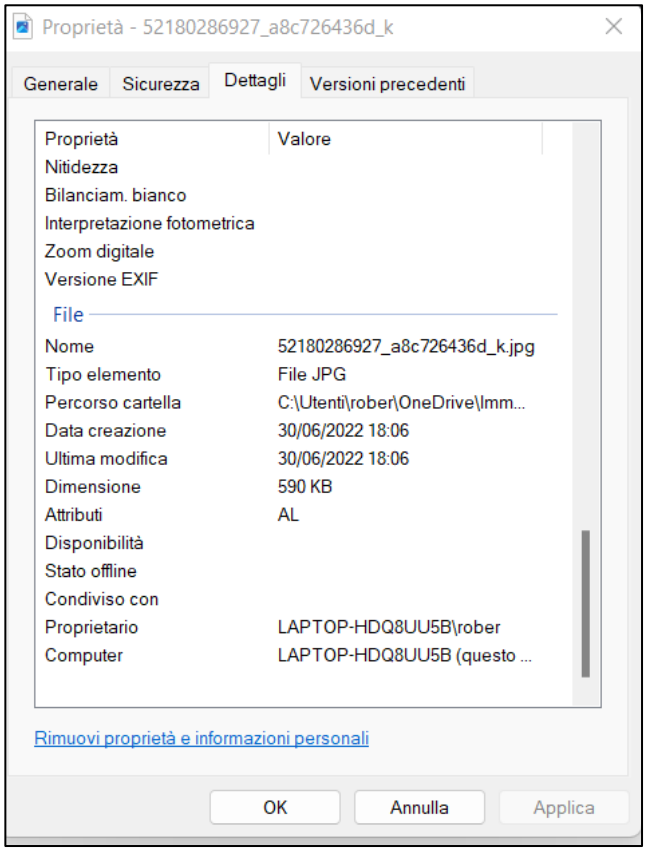
Il dispositivo offre, infatti, la possibilità di cambiarle con un semplice tocco e di inserire perfino una localizzazione, anche se non era stata precedentemente indicata.

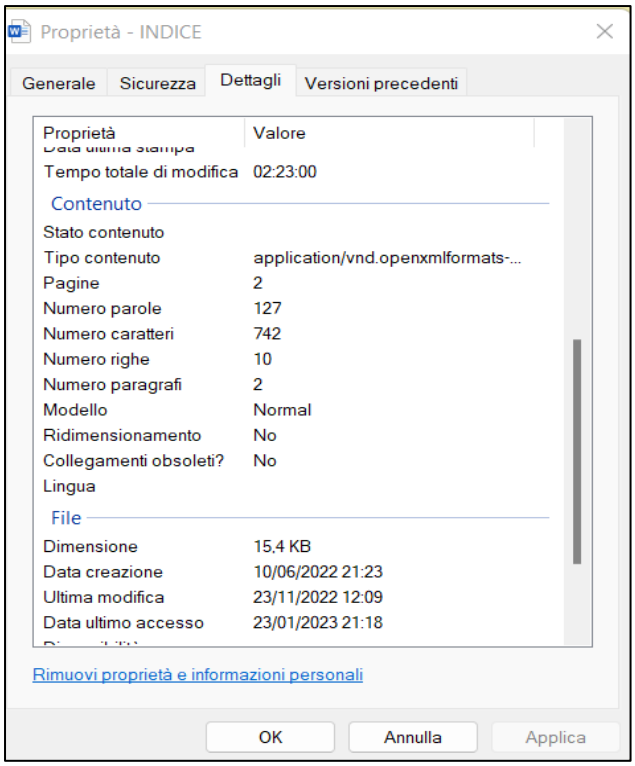

Dettagli
27 Gennaio 2023 19:46
20230127_194658.jpg
2,14 MB 2268x4032
/Memoria interna/DCIM/Camera
Data
27 Gen
Ora
19:46
Gennaio 2023
26 DIC 2022
27 GEN 2023
28 FEB 2024


Dettagli
27 Gennaio 2023 19:46
20230127_194658.jpg
2,14 MB 2268x4032
/Memoria interna/DCIM/Camera
Pl. Menéndez Pelayo, 4, 28040
Madrid, Spagna
Samsung SM-G996B
F2,2 1/50 s 2,20mm ISO 250
Bilanciamento bianco Automatico
Senza flash

Le immagini che seguono permettono, invece, di visionare alcuni metadati in relazione ad un file *Word*:







Talvolta questi dati sono accessibili solo attraverso il dispositivo stesso e il processo di acquisizione, funzionale a preservarli da alterazioni, richiede attività più complesse della semplice visualizzazione dei dettagli, oltre a specifiche *skills* in campo di *digital forensics.*

Proprio per tale ragione è sovente necessario l'intervento di un esperto e, quindi, di un perito o di un consulente tecnico che effettui tutte le operazioni necessarie in modo da mettere il giudice o il pubblico ministero nelle condizioni di meglio valutare il risultato acquisito.

1.3.2 Le categorie di dati acquisibili

La *digital evidence* è generalmente estratta da *hard drive.* Tuttavia, il rapido progredire della tecnologia rende possibile ottenere elementi utili anche da altri tipi di dispositivi: *computer*, *tablet*, *server*, *router*, dispositivi di domotica con accesso a *Internet* (frigoriferi o altri elettrodomestici), dispositivi di *Internet of Things* (IoT), sistemi di sorveglianza, lettori audio, dispositivi GPS, *smartphone*, *consolle* per videogiochi (*Playstation, Xbox*), macchine fotografiche digitali, *smart card*, cercapersone, registratori vocali, *hard disk* esterni, *pen drive*, *scanner*, stampanti, fax, ecc.

I dati che costituiscono il fondamento della prova digitale vanno catalogati per poter meglio comprendere le fasi del procedimento probatorio che vanno dall'acquisizione alla valutazione e le problematiche a esso connesse.

A tal fine, distinguiamo[38] tra *user created data* e *machine* o *network created data*.

I dati riconducibili alla prima categoria comprendono tutto ciò che è creato da una persona fisica usando un *device*. Vi si includono, seppure non in via esaustiva: file di testo, *database*, fogli di lavoro e testo, audio e video, immagini in formato digitale, registrazioni di *webcam*, file del calendario, file nascosti e criptati, copie di *backup*, account creati dall'*user* e dettagli (*username*, foto, *password*), email e allegati, pagine *web*, account *social*, file conservati nel *cloud*.

Per *machine* o *network created data* si intendono, invece, i dati generati automaticamente da un dispositivo elettronico, quali file di *log*, configurazione dei file, *audit trails*[39], *browser data* (*cookies*, cronologia delle pagine visitate e dei *download*), cronologia dei messaggi istantanei e rubrica dello *smartphone* o di specifiche app (*Skype, Whatsapp*, *Telegram*), cronologia GPS, cronologia delle applicazioni, *temporary files*, file di sistema, coda dei file in stampa, ecc.

Tutti questi dati possono essere divisi in *content* e *non content data*.

I *content data* racchiudono informazioni legate a comunicazioni, testi, immagini, video o audio e vengono per lo più definiti come categoria residuale rispetto alle più specifiche tipologie di *non content data*[40].

Rispetto ai *non content data* è possibile operare una distinzione in [41]:

---

[38] Cfr. HASSAN N.A., *Digital Forensics Basics. A practical guide using Windows OS*, cit., p. 18.

[39] Un *Audit Trail* è dato dalla registrazione di più eventi informatici, inclusi data e ora, che si verificano nell'ambito di un'operazione. Rappresenta un dato utile a ricostruire la cronologia di una determinata attività svolta con o su un dispositivo.

[40] *L'Explanatory Report* della Convenzione sul *Cybercrime*, relativamente alle comunicazioni, riporta: « *"Content data" is not defined in the Convention but refers to the communication content of the communication, i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)*», par. 209.
Inoltre, la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, all'art. 2 (10) indicavacome "*dati relativi al contenuto*": qualsiasi dato conservato in formato digitale, come testo, voce, video, immagine o suono, diverso dai dati relativi agli abbonati, agli accessi e alle operazioni.

[41] Commissione europea, *Study on the retention of electronic communications non-content data for law enforcement purposes. Final report*, 2020, https://op.europa.eu/en/publication-detail/-/publication/081c7f15-39d3-11eb-b27b-01aa75ed71a1/language-en, p. 48.

- *subscriber data*: informazioni che permettono di identificare un utente, ovvero nome, indirizzo, numero di telefono.

La Convenzione sul Cybercrime[42] e il Regolamento della Commissione sull'ordine europeo di produzione e conservazione della prova elettronica[43] vi ricomprendono nome, data di nascita, indirizzo, dati di fatturazione e pagamento, numero di telefono e indirizzo *e-mail* fornito, il tipo di servizio utilizzato e la sua durata, compresi i dati tecnici e quelli che identificano le misure tecniche correlate o le interfacce usate e i dati connessi alla convalida dell'uso del servizio che siano ricavabili dal contratto di sottoscrizione del servizio.

- *Traffic data*: in questo gruppo rientrano informazioni vincolate ad una comunicazione e utili ad individuare il tipo di comunicazione, data, tempo e durata.

Sono compresi anche i dati di identificazione del mittente e del destinatario e i *location data*, utili a localizzare i *device* (cella a cui si sono agganciati, *wi-fi*, *hotspot*).

Non c'è, ad oggi, *consenso* sulla categoria a cui ricondurre alcune tipologie di dati quali indirizzo IP, numero di SIM, numeri identificativi del *device* (IMSI, IMEI), numero di porta per gli indirizzi IP dinamici.

Rispetto all'indirizzo IP, la questione della sua riconducibilità alla prima o alla seconda categoria è particolarmente dibattuta.

---

[42] Art. 3 co.3.: "*For the purpose of this article, the term "**subscriber information**" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*

a) the type of communication service used, the technical provisions taken thereto and the period of service;

b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c) *any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement".*

[43] Art. 3 (9), Regolamento 1543/2023 sull'ordine europeo di produzione e conservazione di prove elettroniche, cit.: "**dati relativi agli abbonati**": i dati riguardanti:

(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 pagamento, il numero di telefono o l'indirizzo e-mail forniti;

(b)il tipo di servizio e la sua durata, compresi i dati tecnici e i dati che identificano le misure tecniche correlate o le interfacce usate dall'abbonato o dal cliente o a questo fornite e i dati connessi alla convalida dell'uso del servizio, ad esclusione di password o altri mezzi di autenticazione usati al posto di una password, forniti dall'utente o creati a sua richiesta".

Generalmente, tale indirizzo è collegato ad un unico e specifico *device* connesso ad una rete, con la conseguenza che due dispositivi non possono avere il medesimo indirizzo IP nello stesso *network*[44].

È, inoltre, genericamente combinato con un altro protocollo chiamato *Transmission Control Protocol* (TCP) che permette a un *device* di stabilire una connessione virtuale tra una destinazione e una fonte per scambiare informazioni e dati.

Si distingue tra IP pubblico o privato e, inoltre, tra statico o dinamico.

Il numero IP statico è associato a un dispositivo in maniera permanente, e verrà da lì utilizzato per tutte le comunicazioni su *Internet*.

L'IP dinamico, invece, viene assegnato in maniera automatica e dinamica tra un gruppo potenzialmente ampio, e cambia ad ogni connessione del sistema alla rete.

Ne consegue che, se da un indirizzo IP dinamico si vuole risalire a un dispositivo, sarà necessaria la conoscenza del preciso momento in cui questo ha utilizzato la rete, tuttavia, come già anticipato, uno dei problemi della prova digitale è dato dalla circostanza che, pur potendosi stabilire con certezza cosa avvenga in un determinato sistema informatico o attraverso questo, e pur riconnettendo l'attività ad un determinato IP, non permette di stabilire con certezza chi abbia utilizzato in un dato momento il *device*.

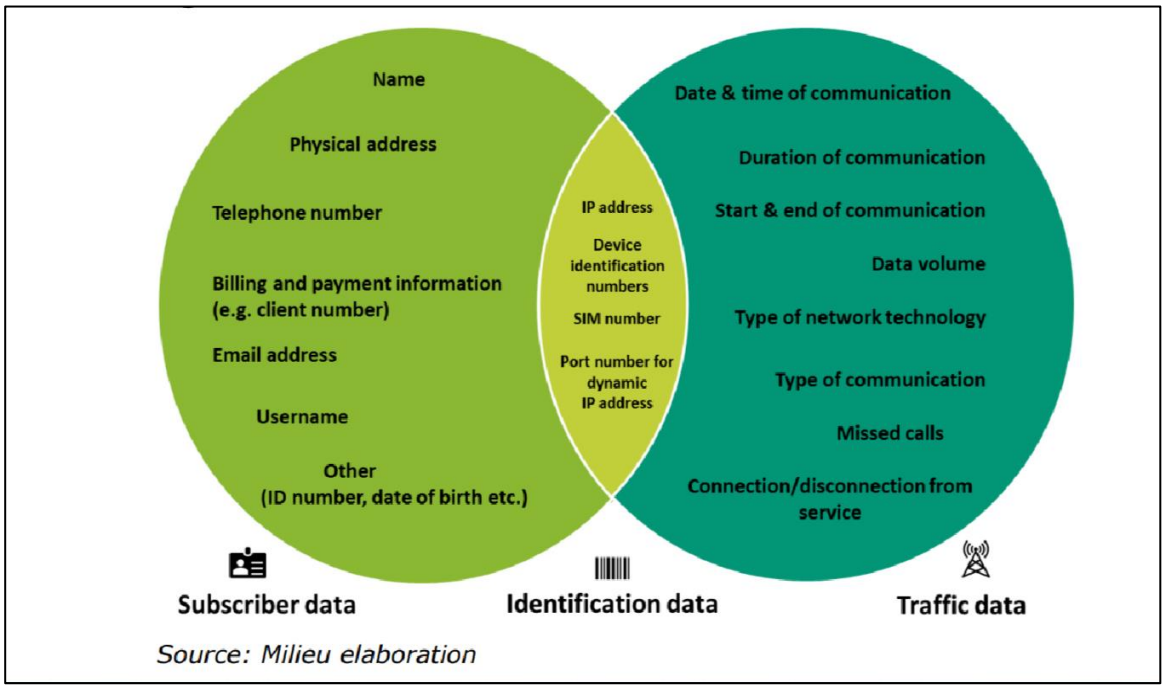
Gli indirizzi IP vengono generalmente considerati *traffic data* e, talvolta, *subscriber data*.

La seguente immagine, tratta dallo studio effettuato dalla Commissione sulla *digital evidence*[45], chiarisce il rapporto tra *subscriber data* e *traffic data* e l'area di sovrapposizione delle due categorie in relazione alle specifiche tipologie di dati di cui sopra.

---

[44] Per approfondimenti v. COSTABILE G., *Rete Internet e "dintorni": aspetti tecnici di base*, cit., p. 33.

[45] Commissione europea, *Study on the retention of electronic communications non-content data for law enforcement purposes. Final report,* 2020, https://op.europa.eu/en/publication-detail/-/publication/081c7f15-39d3-11eb-b27b-01aa75ed71a1/language-en .



In particolare, riguardo ai *non content data* emerge come alcuni Stati (tra cui Francia, Estonia e Islanda) li classifichino come *subscriber data*, mentre altri (Germania, Spagna, Italia, Polonia, Slovenia) come *traffic data*.

Questa difformità di trattamento può incidere sulla tutela dei diritti dei soggetti coinvolti, dal momento che l'accesso ai *subscriber data* generalmente non richiede l'autorizzazione del giudice, invece necessaria per i *traffic data*. Questi ultimi, secondo quanto affermato dalla Corte di Strasburgo[46] e dalla Corte di Giustizia[47], si profilano come maggiormente invasivi, determinando un'ingerenza nella vita privata degli individui idonea a tracciare un quadro sulla loro vita e a trarre conclusioni precise sulle loro abitudini. Sicché, rispetto a questa tipologia di dati, l'accesso può rivelarsi lesivo del diritto al rispetto della vita privata e familiare comunicazioni, come delineato dall'art. 8 CEDU.

Una soluzione di compromesso è stata adottata dal Regolamento sull'ordine di produzione dei dati elettronici che, come si vedrà, assimila le condizioni per la richiesta dei *subscriber data* e dei *traffic data* richiesti ai soli fini identificativi[48].

[46] Corte EDU, Sez. IV, 24 aprile 2018, ricorso n. 62357/14, *Benedik* c. Slovenia, in www.hudoc.echr.coe.int.
[47] CGUE, Grande Camera, 2 ottobre 2018, C-207/16, *Ministerio Fiscal*.
[48] Regolamento 1543/2023, Considerando n. 32: «Tuttavia, ai fini di un'indagine penale specifica, le autorità di contrasto possono dover richiedere un indirizzo IP nonché i numeri di accesso e le relative informazioni al solo fine di identificare l'utente prima che i dati relativi agli abbonati collegati a quell'identificativo possano essere richiesti al prestatore di servizi. In tali casi, è opportuno applicare lo stesso regime applicabile ai dati relativi agli abbonati, quali definiti nel presente regolamento". Art. 5 co. 3: "L'ordine europeo di produzione per ottenere dati relativi agli abbonati o per ottenere dati richiesti al solo scopo di identificare l'utente, quali definiti all'articolo 3, punto 10), può essere emesso per qualsiasi reato e per l'esecuzione di una pena o di una

1.4 *Dalla ricerca al risultato probatorio*

Il procedimento che porta all'immissione di una prova nel processo penale e al suo utilizzo a fini decisori si articola in più fasi[49]: alla preliminare ricerca e identificazione degli elementi utili seguono l'ammissione in dibattimento, l'acquisizione e la valutazione da parte del giudice.

Il momento della ricerca e dell'identificazione presenta, per la prova digitale, aspetti ben più complessi rispetto a quelli riscontrabili nel caso di una prova caratterizzata dalla materialità. L'approccio al dispositivo, anche per lo svolgimento di una semplice attività di ispezione, va effettuato da personale esperto, al fine di garantire la genuinità del dato ed evitare di eliminare o danneggiare accidentalmente elementi utili.

Nelle fasi che portano dall'individuazione alla cristallizzazione del dato, è fondamentale fare riferimento ai rigorosi *standard* delineati dalla *digital forensics*[50], identificati con le sigle ISO/IEC 27037[51] e ISO/IEC 27042[52]. Questi *standard* individuano le linee guida applicabili in relazione a specifiche attività di indagine e alla gestione delle prove digitali e si traducono in raccomandazioni finalizzate all'utilizzo di approcci simili, non determinando alcun vincolo per le autorità e gli esperti di *forensics*.

La ricerca e individuazione di elementi utili ai fini delle indagini prevede un controllo meticoloso di tutto il materiale a disposizione, che può agevolmente sfociare in un'intrusione

misura di sicurezza detentiva di almeno quattro mesi, a seguito di un procedimento penale, irrogata con decisione non pronunciata in contumacia, nei casi in cui la persona condannata è latitante».

[49] V. CARLIZZI G., *La prova tecnologica nel processo penale*, in LUPARIA L., MARAFIOTI L., PAOLOZZI G. (a cura di), *Dimensione tecnologica e prova penale*, cit., p. 77; COSTABILE G., Digital forensics & digital investigation, cit., *passim*., p. 5; UZAROVSKA LAZETIK B G., O. KOSHEVALISKA, *Digital evidence in criminal procedures – A comparative approach*, in *Balkan Social Science Review*, 2013, n. 2, p. 63.

[50] La *digital forensics* è una branca delle scienze forensi che utilizza la conoscenza scientifica per raccogliere, analizzare, e documentare prove digitali e permetterne l'utilizzabilità all'interno del processo penale. Tale termine è ampiamente utilizzato come sinonimo di *computer forensics*, tuttavia comprende al suo interno altre branche: *computer forensics*, *email forensics*, *mobile forensics*, *network forensics*,*database forensics*, *cloud storage forensics*, *IoT forensics*, *multimedia forensics*, *hardware forensics*,*memory forensics, malware forensics; v*edasi CASEY E., *Digital Evidence and Computer Crime. Forensics Science, Computer and the Internet*, cit., pp. 37 -38. Inoltre, per approfondimenti, HASSAN N.A., *Digital Forensics Basics. A practical guide using Windows OS*, cit., p. 10; IACOBELLI A., BERTI A., MATTIUCCI M., FRATINI P., *La testimonianza esperta nell'Arma dei Carabinieri*, in CARLIZZI G., TUZET G. (a cura di), *La prova scientifica nel processo penale*, G. Giappichelli Editore, 2018.

[51] "*Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*".

[52] "*Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*". Per approfondire le procedure di *digital forensics* v. HASSAN N.A., *Digital Forensics Basics. A practical guide using Windows OS,* cit.; PETERSON G., SHENOI S. (a cura di*), Advances in Digital Forensics XV*, Springer, 2019; KÄVRESTAD J., *Fundamentals of Digital Forensics. Theory, Methods, and Real-Life Applications*, cit.

generalizzata e sproporzionata all'interno della sfera privata di un individuo, allorquando si determini un controllo ad ampio raggio della sua sfera personale.

Tuttavia, una ricerca di questo tipo si pone a volte in rapporto di necessità con il prosieguo delle indagini, essendo altamente improbabile che i *file* connessi all'attività criminosa siano visibili *ictu oculi* sul *desktop* di un computer con diciture palesemente rinviabili all'illecito.

Ben più probabile, invece, è che si trovino in cartelle nascoste e localizzate all'interno di un percorso creato per confondere chi, ignorando l'esatto posizionamento, volesse cercarle, anche attraverso l'utilizzo di *software* idonei.

Quanto detto si verifica in maniera più netta in relazione alle informazioni criptate.

La crittografia, infatti, è una «tecnica che permette, con l'aiuto di un algoritmo matematico, di trasformare un messaggio leggibile da tutti, in una forma illeggibile per quegli utenti che non possiedano una chiave segreta di decifrazione[53]. L'obiettivo è quello di preservare l'accesso alle informazioni delle imprese, di autorità pubbliche o, anche, alle comunicazioni tra persone fisiche, come nel caso di Whatsapp o Blackberry.

L'informazione criptata può essere svelata solo utilizzando la chiave di cifratura, che può essere di due tipi[54].

Una particolare forma di crittografia è la *end-to-end*, tale per cui solo il destinatario di una comunicazione possiede la chiave per decriptare e leggere il dato.

In relazione al tipo di applicazione utilizzata, il dato è spesso archiviato nel *cloud* ma, in tal caso, i *provider* non posseggono la chiave di cifratura, con notevoli difficoltà per la *disclosure* dei dati alle autorità[55].

Una volta effettuata l'identificazione degli elementi utili per le indagini, l'acquisizione è realizzata mediante una copia conforme attraverso la *bit stream o mirror*

---

[53] ZICCARDI G., *Crittografia e diritto,* G. Giappichelli Editore, 2003, p. 38. Europol e Eurojust, *First report of the observatory function on encryption*, 2019, https://www.eurojust.europa.eu/sites/default/files/2019-01/2019-01_Joint-EP-EJ-Report_Observatory-Function-on-Encryption_EN.pdf, p. 13: « *The process of converting data, such as messages or pieces of information, in a way which prevents unauthorised access*». Eurojust, *Second report of the observatory function on encryption,* 2020, https://www.europol.europa.eu/cms/sites/default/files/documents/second_observatory_function_report.pdf .

[54]Si distingue tra crittografia simmetrica e asimmetrica: nel primo caso, è utilizzata una sola chiave, che è la sequenza di *bit* utilizzati per cifrare l'informazione, per criptare e decriptare il dato. La crittografia asimmetrica prevede, invece, l'utilizzo di una combinazione di chiavi per chiudere e aprire il documento. Quest'ultima è utilizzata da app quali Whatsapp e Telegram.

[55] Il terzo *report* sulla crittografia pubblicato da Europol e Eurojust chiarisce che Danimarca, Francia, Germania, Polonia, Svezia, Svizzera e Paesi Bassi sono gli unici Stati membri con norme relative all'utilizzo da parte delle autorità di polizia di strumenti per contrastare la crittografia. *Europol, Eurojust, Third report of the observatory function on encryption,* 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/3rd_report_of_the_observatory_function_on_encryption-web.pdf , p. 11 ss.

image, ovvero la copia dei dati *bit* per *bit*, che permette di creare un'immagine esatta delle informazioni contenute, senza alterarle e senza disperdere metadati utili ai fini investigativi[56].

In tal modo è possibile creare più copie del dispositivo originario, mantenendo questo inalterato, al fine di effettuare poi l'analisi sulle copie e poter, eventualmente, ripetere le operazioni qualora fosse necessario. Con riguardo allo svolgimento di questa operazione, è dibattuto se si tratti di un atto ripetibile o non ripetibile.

Mentre la dottrina[57] propende per la l'irripetibilità, la giurisprudenza[58] ritiene che si tratti di atto ripetibile. Un dibattito che, in relazione all'ordinamento italiano, assume rilievo non già meramente teorico: la riconduzione all'una o all'altra categoria influisce sull'applicabilità della disciplina più garantita in materia di accertamenti tecnici irripetibili ai sensi dell'art. 360 c.p.p.[59]. In questa evenienza, infatti, il pubblico ministero, a tutela del contraddittorio, è tenuto a informare l'indagato, la persona offesa e i difensori, affinché possano partecipare all'atto e nominare propri consulenti tecnici. Questi ultimi avranno il diritto di assistere agli accertamenti e di formulare osservazioni e riserve.

---

[56] Cfr. ZICCARDI G., *Le tecniche informatico-giuridiche di investigazione digitale*, in LUPARIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica,* cit., p. 63.

[57] *Ex multis* SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p 223 ss.; PITTIRUTI M., Digital evidence *e procedimento penale*, cit., p. 105 ss.

[58] Cass., Sez. I, 30 aprile 2009, n. 23035; Cass, Sez. II, 4 giugno 2015, n. 24998 : «La conclusione alla quale si è pervenuti, trova un puntuale riscontro nella giurisprudenza di questa Corte la quale, in fattispecie similari, ha ritenuto che: […] non dà luogo ad accertamento tecnico irripetibile l'estrazione dei dati archiviati in un *computer*, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte». E anche Cass., Sez. VI, 20 dicembre 2018, n. 15838: «Del tutto logico e consequenziale, quindi, circa l'ambito di applicazione della previsione che disciplina l'accertamento tecnico irripetibile *ex* art. 360 c.p.p., risulta l'esclusione dell'attività di estrazione di copia di file da un computer. Ormai da tempo, infatti, la tecnica consente di acquisire il dato attraverso operazioni meramente esecutive e materiali, il cui unico scopo è quello di assicurare alla fase processuale quanto di rilevante è contenuto all'interno dello stesso in formato digitale, operazione che non necessità di perizia o consulenza tecnica».

[59] «Art. 360 – **Accertamenti tecnici non ripetibili**: quando gli accertamenti previsti dall'art. 359 riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici.
2. Si applicano le disposizioni dell'articolo 364 comma 2.
3. I difensori nonché i consulenti tecnici eventualmente nominati hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve.
3-bis. Il pubblico ministero può autorizzare la persona sottoposta alle indagini, la persona offesa dal reato, i difensori e i consulenti tecnici eventualmente nominati, che ne facciano richiesta, a partecipare a distanza al conferimento dell'incarico o agli accertamenti.
4. Qualora, prima del conferimento dell'incarico, la persona sottoposta alle indagini formuli riserva di promuovere incidente probatorio, il pubblico ministero dispone che non si proceda agli accertamenti salvo che questi, se differiti, non possano più essere utilmente compiuti.
4-*bis*. La riserva di cui al comma 4 perde efficacia e non può essere ulteriormente formulata se la richiesta di incidente probatorio non è proposta entro il termine di dieci giorni dalla formulazione della riserva stessa.
5. Fuori del caso di inefficacia della riserva di incidente probatorio previsto dal comma, se il pubblico ministero, malgrado l'espressa riserva formulata dalla persona sottoposta alle indagini e pur non sussistendo le condizioni indicate nell'ultima parte del comma 4, ha ugualmente disposto di procedere agli accertamenti, i relativi risultati non possono essere utilizzati nel dibattimento».

All'indagato è, inoltre, data facoltà di formulare richiesta di incidente probatorio, affinché la prova venga assunta nelle forme più garantite del contraddittorio, ai sensi dell'art. 360 co 4 c.p.p. In questo caso, *ex* art. 360 co. 4-*bis* e co. 5 c.p.p., il pm non potrà procedere con gli accertamenti, pena l'inutilizzabilità di quanto acquisito, a meno che il loro differimento comporti l'impossibilità di eseguirli.

Seppure, come detto, la giurisprudenza[60] propenda per la natura ripetibile di tale atto, vista la possibilità di effettuare più analisi sulle copie, va considerato che un errato svolgimento dell'operazione potrebbe irrimediabilmente compromettere la prova, con notevoli pregiudizi per il contraddittorio e per la difesa dell'indagato[61].

Queste considerazioni assumono maggior rilievo se si considera che, per questa particolare tipologia di prova, l'acquisizione del dato cognitivo avviene quasi sempre in un momento anteriore rispetto al dibattimento, ovvero nella fase delle indagini preliminari, con un sensibile *vulnus* per il contraddittorio. Per rimediare a questo possibile rischio è fondamentale disporre di copie conformi, create secondo gli *standard* previsti, che favoriscano la ripetibilità degli atti, a garanzia della genuinità della prova.

E proprio in ragione di tali peculiarità, è da domandarsi se la prova dichiarativa sia ancora la protagonista del dibattimento, dal momento che il contraddittorio per la formazione della prova si riduce a un mero esercizio di dialettica su materiali non decifrabili e già preconfezionati in sede di indagini preliminari[62].

«La necessità di "assicurare la conservazione", nonché impedire l'alterazione del dato informatico originario, ha duplice finalità: da un lato, garantire la genuina acquisizione di elementi probatori che potranno assumere successivamente valenza di prova; dall'altro, sul fronte delle garanzie difensive, permettere un controllo sull'operato degli inquirenti, il quale deve necessariamente prendere le mosse dalla verifica sulle procedure acquisitive»[63].

La fase successiva consta dell'analisi dei dati raccolti, per poter estrapolare le informazioni utili alle indagini.

Come già anticipato, tutte queste operazioni devono svolgersi secondo precisi *standard* idonei a non alterare o distruggere i dati, per poter ottenere una prova genuina. In questa e nelle precedenti fasi, rivestono fondamentale importanza i sigilli informatici, c.d.

---

[60] Cass., Sez. II, 19 febbraio 2015, n. 8607; Cass., Sez. I, 25 febbraio 2009, n. 11503.

[61] Rischio evidenziato da CURTOTTI D., *Attività di acquisizione della* digital evidence*: ispezioni perquisizioni e accertamenti tecnici,* in ATERNO S., CAGLIANI F., COSTABILE G., CURTOTTI D. (a cura di), Cyber forensics *e indagini digitali*, cit., p. 442.

[62] Così LUPARIA L., *La disciplina processuale e garanzie difensive* in LUPARIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica,* cit., p. 128.

[63] CURTOTTI D., *Attività di acquisizione della* digital evidence*: ispezioni perquisizioni e accertamenti tecnici,* cit., p. 445.

hash, e la catena di custodia, che consta nella realizzazione di *report* relativi a ogni attività, idonei a tracciare il procedimento di repertamento e a permetterne la conseguente valutazione. Ogni attività deve essere compiuta secondo precisi protocolli investigativi e *standard*, affinché i risultati ottenuti possano spiegare il loro valore probatorio all'interno del dibattimento.

Va, tuttavia, specificato che, in alcuni casi, può essere necessaria la richiesta agli *internet service provider*, allorquando i dati ricercati non siano accessibili dal *device* stesso[64].

Come avremo modo di verificare più avanti, nel caso di *cloud computing*, dati connessi all'*Internet of Things* (IoT), dispositivi protetti da *password* o comunicazioni crittografate, danneggiamento fisico di un *device* o dati manipolati, le autorità di polizia non si trovano nella possibilità di acquisire gli elementi utili in maniera autonoma.

Questa problematica sarà oggetto di approfondimento nei successivi capitoli, per valutare le concrete criticità che si presentano allorquando sia necessario chiedere a enti privati, spesso avente sede legale in altri Stati, dati localizzati in Paesi terzi o dei quali si ignora la specifica posizione.

Una volta che la prova è stata cristallizzata, questa dovrà trovare ingresso nel processo per la successiva valutazione del giudice.

In proposito, preme sottolineare che il giudice e le parti coinvolte nel processo penale non sono talvolta in grado di valutare personalmente le prove digitali senza l'intervento di un perito che renda intellegibile la metodologia tecnologico -scientifica utilizzata.

In ragione di questa particolare caratteristica, seppur tavolta introdotta anche come prova documentale, il mezzo preferibile è costituito dalla perizia.

E infatti, *in primis,* non solo l'introduzione come prova documentale non permette di apprezzare e valutare tutte le sfaccettature dell'elemento digitale, ma, inoltre, lo stesso giudice non possiede, generalmente, le competenze necessarie.

Attraverso la perizia, invece, gli esperti possono fornire una valutazione più approfondita e un'analisi specifica degli elementi probatori, nel pieno rispetto del principio del contradditorio.

Per poter, tuttavia, ricoprire pienamente il suo ruolo ed essere valutabile dal giudice, la prova dovrà rispondere a determinati requisiti:

- autenticità,

[64] Al riguardo SPIEZIA F., *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: Il ruolo di Eurojust*, cit., p. 16, il quale richiama uno studio compiuto dal Gruppo di Stati per lo sviluppo della Convenzione sul *Cybercrime*, secondo il quale «nel 2015 vi sono state più di 138000 richieste ai maggiori OSP (*Apple, Facebook, Google, Microsoft, Twitter, Yahoo*) con un responso di circa il 60%. Se poi aggiungiamo le richieste formulate dagli Usa arriviamo ad un totale di circa 2300.000 richieste ricevute in un solo anno».

- completezza,
- affidabilità,
- credibilità.

Queste caratteristiche vengono valutate sulla base delle operazioni effettuate, laddove la catena di custodia e i sigilli permettano di verificare l'assenza di alterazioni o manipolazioni, tali da rendere la prova assunta identica a quella presente in origine sul dispositivo.

In aggiunta, in rapporto al processo, dovrà rispettare i requisiti di proporzionalità[65], liceità, pertinenza e rispondere alle condizioni previste dalla legge.

Affinché possa, infatti, essere ammissibile è necessario che la prova sia pertinente rispetto ai fatti oggetto di prova, ai sensi dell'art. 187 c.p.p.

Potrà poi dispiegare il suo valore probatorio ed essere utilizzata per la valutazione del giudice qualora sia stata assunta nel rispetto delle norme previste dal codice di rito, non sia contraria a norme di legge e rispetti i diritti fondamentali degli individui.

Un ruolo chiave, a tutela dei diritti fondamentali, è rivestito dal principio di proporzionalità che «rimanda alla necessità di effettuare un bilanciamento tra gli interessi in conflitto per limitare possibili abusi da parte dei poteri pubblici»[66].

In ambito europeo il principio è disciplinato dal TUE[67] e dalla Carta dei diritti fondamentali dell'Unione Europea[68] .

---

[65] KASPER A., LAURITS E., *Challenges in collecting digital evidence: a legal perspective*, in KERIMKMAE T., RULL A., (a cura di) *The future of law and eTechnologies*, Springer, 2016, p. 209.

[66] BACHMAIER WINTER L., *La orden europea de investigación y el principio de proporcionalidad*, in *Revista General de Derecho europeo*, 2011, p. 4; EAD, *The Role of proportionality principle in cross-border investigations involving fundamental rights*, in RUGGERI S. (a cura di), *Transnational inquiries and the protection of fundamental rights in criminal proceedings. A study in memory of Vittorio Grevi and Giovanni Tranchina,* Springer, 2013, p. 85.

[67] Trattato sull'Unione Europea, «**Art. 5** - 1. La delimitazione delle competenze dell'Unione si fonda sul principio di attribuzione. L'esercizio delle competenze dell'Unione si fonda sui principi di sussidiarietà e proporzionalità. […] 4. In virtù del principio di proporzionalità, il contenuto e la forma dell'azione dell'Unione si limitano a quanto necessario per il conseguimento degli obiettivi dei trattati».

[68] Carta dei diritti fondamentali dell'Unione Europea, «**Art .49 - Principi della legalità e della proporzionalità dei reati e delle pene:** Nessuno può essere condannato per un'azione o un'omissione che, al momento in cui è stata commessa, non costituiva reato secondo il diritto interno o il diritto internazionale. Parimenti, non può essere inflitta una pena più grave di quella applicabile al momento in cui il reato è stato commesso. Se, successivamente alla commissione del reato, la legge prevede l'applicazione di una pena più lieve, occorre applicare quest'ultima. 2. Il presente articolo non osta al giudizio e alla condanna di una persona colpevole di un'azione o di un'omissione che, al momento in cui è stata commessa, costituiva un crimine secondo i principi generali riconosciuti da tutte le nazioni. 3. Le pene inflitte non devono essere sproporzionate rispetto al reato». «**Art. 52 - Portata e interpretazione dei diritti e dei principi -** 1. Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

Il giudizio di proporzionalità richiede una valutazione sulla gravità del fatto, l'idoneità della misura da seguire, la necessità ai fini del giudizio, l'esistenza o meno di un'altra misura che permetta di raggiungere il medesimo risultato e il bilanciamento tra la limitazione dei diritti fondamentali, la finalità di interesse generale, la tutela dei diritti individuali e della libertà altrui[69].

L'inosservanza del suddetto principio e dei diritti individuali per privilegiare i fini investigativi e persecutori deve essere legittimata da una base legale, giustificata da una necessità sociale imperativa.

A partire dalla sentenza *Wednesbury*[70], in Inghilterra e Galles è stato perfezionato il c.d. *proportionality test* attraverso il quale si valutano ulteriori criteri quali: gravità del fatto illecito, intensità dei sospetti o serietà degli indizi, prospettive sul risultato dell'atto di indagine, utilizzo di risorse in relazione al risultato, pregiudizi causati ai diritti individuali in relazione al fine.

La Corte di Giustizia UE si è più volte espressa per delineare i contorni del principio di proporzionalità e ha affermato che le eccezioni alla tutela dei diritti fondamentali non possono superare il limite dello stretto necessario, richiedendo che, specie nel caso di misure particolarmente invasive, ci siano sufficienti indizi contro l'imputato[71].

Chiamata a pronunciarsi in relazione alla Direttiva 2006/24/CE sulla protezione dei dati personali[72], la Corte ha ritenuto che l'accesso ai dati vada limitato a quanto strettamente necessario, evitando ogni abuso attraverso una protezione idonea e richiamando il principio di specificità, in virtù del quale l'accesso deve essere relazionato a procedimenti specifici, e non utilizzato in via generalizzata.

I principi di diritto enunciati richiedono che ogni atto delle istituzioni deve limitarsi a realizzare gli obiettivi perseguiti dalla normativa senza superare i limiti di ciò che è idoneo

---

[69] Cfr. BACHMAIER WINTER L., *La orden europea de investigaciòn y el principio de proporcionalidad,* cit., p. 16; DANIELE M., *La metamorfosi del diritto delle prove nella Direttiva sull'ordine europeo di indagine penale*, in Diritto Penale Contemporaneo, 20 novembre 2014, p. 92; LARO GONZÁLEZ E., *La orden europea de investigación en el espacio europeo de justicia,* Tirant lo Blanch, 2021; NICOLICCHIA F., *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*; in *Dir. Pen. Cont.*, 8 gennaio 2018, TORRE M., I*ndagini informatiche e principio di proporzionalità*, in *Proc. Pen. Giust*, 2019, 6, p. 1433.

[70] *Court of Appeal of England and Wales,* 10 novembre 1947, *Associated Provincial Picture Houses v. Wednesbury Corporation*.

[71] Cfr. CGUE, 8 aprile 2014, cause riunite C-293/12 e C-593/12, *Digital Rights Ireland Ltd*. Per approfondimenti FLOR R., *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "Data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine? in Dir. Pen. Cont.*, 28 aprile 2014, .

[72] 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, in G.U.U.E. L 105 del 13 aprile 2006.

e necessario al conseguimento degli obiettivi stessi[73]. Gli elementi da valutare sono, pertanto, il fine da raggiungere, la misura impiegata e il risultato da ottenere, in relazione anche al delitto per cui si indaga.

In conclusione, una misura si considera proporzionata se risponde ai tre requisiti di idoneità, necessarietà e proporzionalità in senso stretto.

In tal senso è idonea se permette di raggiungere il fine proposto, necessaria laddove non esiste una misura meno restrittiva per ottenere lo stesso risultato con la stessa efficacia e proporzionale in senso stretto, allorquando da questa derivino più vantaggi e benefici rispetto al *vulnus* causato ai diritti individuali.

1.5 Le nuove frontiere dell'innovazione tecnologica: Cloud computing *e* Internet of Things

La categorizzazione dei dati che possono costituire una prova digitale non è certamente esaustiva e, come già anticipato, la rapida velocità dell'innovazione tecnologica fa sì che un numero sempre più vasto di elementi possa essere ricompreso in questo gruppo.

A tale riguardo, possiamo richiamare i dispositivi di *health-care*, il metaverso, i dati biometrici, i dispositivi di *Internet of Things*, con la conseguente difficoltà di catalogazione dei dati in *traffic, access* o *content* data o, più opportunamente, in una categoria di nuovo conio.

L'Internet of Things (IoT) è un'infrastruttura che permette di usufruire di servizi attraverso la connessione di dispositivi elettronici, elettrici e non-elettrici finalizzata allo scambio di comunicazioni e servizi [74].

Ogni dispositivo è connesso ad una piattaforma domestica, contribuendo alla creazione di dati personali dell'*user*.

L'analisi di uno strumento di IoT permette di dedurre abitudini dell'usuario, o di accedere alle conversazioni registrate.

Facendo riferimento, per esempio, ai dispositivi di *Amazon Echo* (ben più conosciuto come "Alexa"), all'assistente *Iphone* "Siri" o all'assistente di Google, va sottolineato come

[73] Cfr. CGUE, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige* e *Watson.*

[74] SADINENI L., PILLI E., BABU BATTULA R., *A holistic forensic model for the internet of things*, in PETERSON G., SHENOS S. (a cura di), *Advances in Digital Forensics XV,* Springer, 2019, p.3: «*The Internet of Things (IoT) is a global infrastructure that enables advanced services by interconnecting (physical and virtual) objects based on existing, evolving and interoperable information and communications technologies. The Internet of Things connects electronic, electrical and non-electrical objects to provide seamless communications and contextual services*».

i *device* su cui tali servizi sono installati mantengano il microfono costantemente acceso, per poter attivare l'assistente con parole chiave quali "Ehi Google", "Siri", "Alexa".

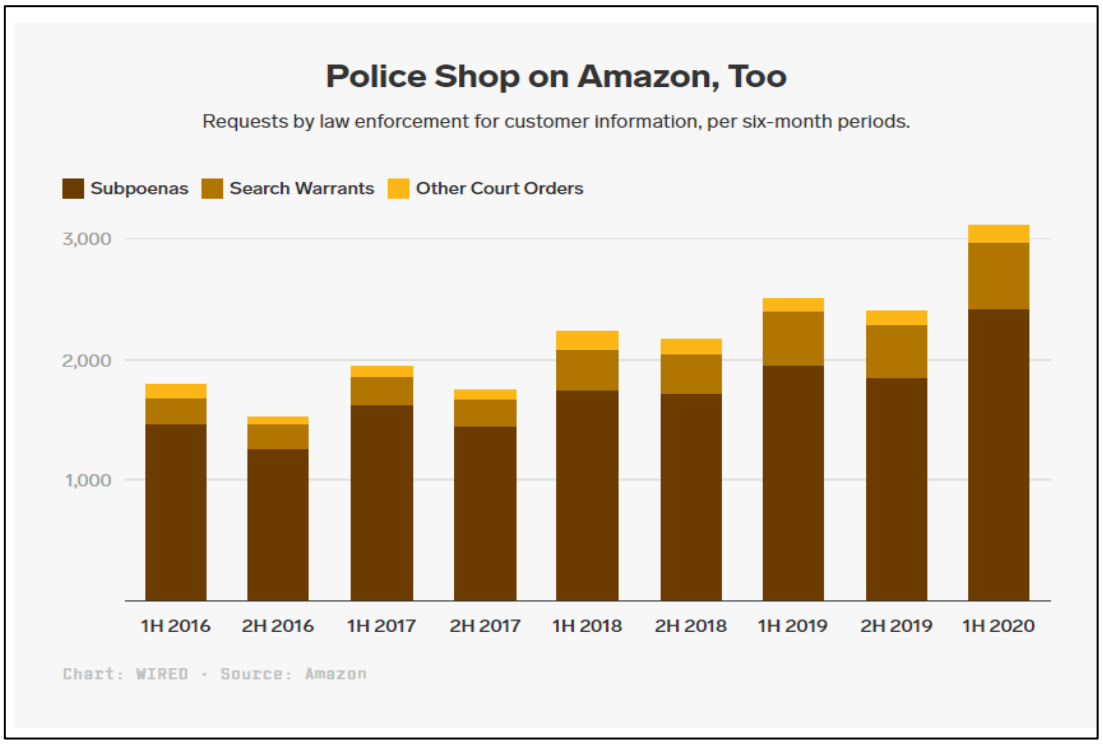
Una volta attivatosi con tali parole o, spesso, con parole dal suono similare, il dispositivo inizia ad interagire con l'utente e a registrare la comunicazione. Queste registrazioni sono finalizzate ad aumentare l'efficienza del servizio e, pertanto, vengono poi inviate ai *server* degli *internet service provider* (da qui in avanti ISP), permettendo di archiviare file che possono contenere dati e informazioni personali. Non è dato sapere come i *provider* utilizzino i dati e come li gestiscano. È plausibile che i dipendenti delle aziende prendano nota delle registrazioni per implementare il servizio e migliorare la risposta ai comandi da parte delle applicazioni.

I dispositivi Amazon e le informazioni in essi contenute sono entrati a far parte del materiale probatorio in alcuni procedimenti svoltisi negli Stati Uniti e le autorità di polizia si sono spesso rivolte al *provider* per ottenere le informazioni conservate nei *server*[75].

In ambito processuale, le registrazioni effettuate possono assumere rilevanza non soltanto come prove a carico, ma anche per integrare un alibi per l'indagato, dimostrando che si trovava in un luogo incompatibile con quello in cui si è consumato il fatto illecito

[75] BURKE M., *Amazon's Alexa may have witnessed alleged Florida murder, authorities say,* 2019, https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621 ; DWYER C., *Arkansas Prosecutors Drop Murder Case That Hinged On Evidence From Amazon Echo*, 2017, https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo ; KRUEGER C., MCKEOWN S., *Using Amazon Alexa APIs as a source of digital evidence*, in *International Conference on cyber security and protection of digital services (cyber security)*, 2020, p. 1; WHITTAKER Z., *Judge orders Amazon to turn over Echo recordings in double murder case*, 2018, https://tcrn.ch/2DEb3en.

.



[76] *Richieste di dati effettuate dalle forze di Polizia statunitensi nei confronti di Amazon*

Il *cloud computing* implica la possibilità per un utente di archiviare dati in uno spazio virtuale (appunto, il *cloud*), affinché vengano allocati su più *server* e siano accessibili da più dispositivi, una volta effettuato l'accesso. Questo servizio permette di superare l'ostacolo dato dalla memoria limitata dei dispositivi, potendo usufruire di uno spazio di archiviazione virtuale, aumentabile in base a diversi pacchetti offerti dal fornire.

Il *provider* si incarica di conservare i dati, avere copie di *backup* e proteggerli da attacchi informatici. Anche le imprese si avvalgono sempre più di tali servizi per abbattere i costi delle infrastrutture e aumentare l'efficienza dei *network* aziendali [77]. Lo spazio di archiviazione, a sua volta, si regge su più *server* spesso allocati in Stati diversi, facendo sì che i dati rientrino in giurisdizioni differenti.

I *provider*, infatti, spostano costantemente i dati, non necessariamente per sottrarsi alla giurisdizione di uno Stato, ma per ottimizzare le risorse attraverso la cd. ridondanza o *load balancing*, che permette di spostare i *file* da un *server* all'altro.

Gli ISP possono scegliere di conservare i dati all'interno di *server* che si trovino in giurisdizioni distinte rispetto a quella dell'utente, o anche in giurisdizioni diverse da quelle essi gli stessi abbiano sede legale.

[76] Richieste effettuare dalle autorità di polizia statunitensi ad Amazon, https://www.wired.com/story/star-witness-your-smart-speaker/ , consultato il 29/01/2023.
[77] HASSAN N.A., *Digital Forensics Basics. A practical guide using Windows OS*, cit., p. 60.

Si profilano, dunque, distinte ipotesi per le autorità di polizia, allorquando abbiano necessità di acquisire determinati dati: da un lato, l'accesso unilaterale ai file archiviati nel territorio di un altro Stato, dall'altro, l'accesso unilaterale ai dati attraverso un'attività "*trans-border",* senza tuttavia avere certezza della posizione ufficiale dei dati ai quali si ha accesso.

Il fenomeno in questione, denominato "*loss of knowledge of location*", determina l'impossibilità di stabilire con precisione la posizione dei dati e, di conseguenza, pone alcune problematiche relative all'individuazione della giurisdizione da parte delle autorità di polizia, soggette alla propria giurisdizione, in accordo con il principio di territorialità. Ebbene, se la localizzazione è nota, le autorità di polizia possono interfacciarsi con le autorità dello Stato interessato per condurre indagini sul suo territorio, secondo gli accordi di mutua assistenza giudiziaria o altri strumenti, quali l'ordine europeo di indagine[78] o, in via residuale, le rogatorie internazionali[79]. In caso contrario, si genera una situazione di incertezza giuridica che può pregiudicare l'efficacia delle indagini e la conseguente esigenza di una effettiva persecuzione dei reati.

Infatti, la mancata conoscenza del posizionamento del dato e della giurisdizione competente non permette neppure di attivare i meccanismi di cooperazione giudiziaria attualmente previsti, essendo il loro funzionamento strettamente connesso al principio di territorialità.

Le evoluzioni tecnologiche hanno determinato uno sconvolgimento degli equilibri tradizionali e un'inversione dei consueti meccanismi a cui siamo abituati.

La necessità di accedere a dati in possesso degli ISP fa sì che talvolta si debbano acquisire al processo dati raccolti da enti di diritto privato e non dalle autorità di polizia e dagli esperti di *forensics* a ciò deputati. In più, la raccolta di tali dati determina, senza ombra di dubbio, un'intrusione nella sfera personale degli individui, la cui salvaguardia dei diritti è lasciata alla discrezionalità e competenza di soggetti con forti interessi economici.

Gli ISP, infatti, sono chiamati ad effettuare un bilanciamento tra i diritti degli individui e le istanze pubbliche, ma è fuor di dubbio che su questo incidano anche forti interessi economici. Chiaramente, ciò incide sul diritto di difesa, sull'attendibilità dell'accertamento e sulla tutela della sfera privata che ogni individuo deve potere proteggere da intrusioni esterne.

---

[78] Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale, in G.U. L 130 del 1° maggio 2014.

[79] Per un *excursus* storico vedasi VALENTINI C., *L'acquisizione della prova tra limiti territoriali e cooperazione con autorità straniere*, CEDAM, 1998.

Lo spostamento dei dati tra varie giurisdizioni o l'incertezza sulla loro localizzazione, incide su un altro tema: quello della scelta delle norme e/o sugli strumenti di cooperazione da utilizzare per la raccolta degli elementi.

Nei successivi capitoli del presente elaborato, si focalizzerà l'attenzione sulle recenti innovazioni, appena esposte, e sulle modalità di acquisizione di dati che, in relazione all'IoT o al *Cloud computing*, siano in possesso degli ISP e, per loro natura, richiedono un ripensamento degli attuali meccanismi di cooperazione giudiziaria transnazionale, oltre che del principio di territorialità.

Ci si soffermerà, inoltre, sulle criticità relative all'acquisizione dei dati in possesso dei *provider*, sugli strumenti attualmente in vigore o *in fieri* deputati a ottenere tali elementi e sul loro rapporto con i diritti fondamentali degli individui.

CAPITOLO II

La prova "digitale" nell'ordinamento italiano

2.1. Una categoria ancora indefinita

Nell'attuale contesto, la prova digitale risulta di fondamentale importanza per un ampio numero di procedimenti penali, relativi non solo a reati informatici, ovvero commessi avvalendosi di sistemi informatici[80], ma anche a delitti comuni, quali omicidi, lesioni personali, atti persecutori, delitti a sfondo sessuale, etc...

Come è stato ben evidenziato, «grazie alla diffusione capillare degli apparati informatici, la maggior parte delle nostre attività – siano esse lavorative, sociali o personali – è destinata a essere immagazzinata in computer, in altri dispositivi analoghi ovvero nella "rete"» [81]. Con quanto ne consegue sul versante processuale. Le nuove tecnologie non si limitano a registrare i dati di accesso alla rete o quelli relativi alle comunicazioni e agli spostamenti, ma rendono possibile l'acquisizione di dati sull'attività che viene effettuata all'interno del domicilio o in altri luoghi riconducibili alla nozione di "privata dimora"[82],

---

[80] Si può fare riferimento ad una branca del diritto, denominata "diritto penale dell'informatica", che ricomprende i delitti commessi attraverso tecnologie di "*information communication*". Si distinguono le categorie dei *computer-crime* o reati informatici, caratterizzati dalla connessione con l'informatica, e dei *cybercrime*, relativi all'utilizzo della rete per fini criminosi. V. SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 39 ss.

[81] Così SIRACUSANO F., *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. Pen. Giust.*, 2017, 1, p. 178: «È questa, d'altronde, una svolta inevitabile; riflesso di un fenomeno che oltre a essere tecnologico è ormai divenuto sociale. I dispositivi informatici hanno, infatti, acquisito un'importanza fondamentale nello sviluppo dell'individuo sino a imporne un mutamento del perimetro di proiezione della sfera personale. Il bagaglio d'informazioni in essi contenuto costituisce una sorta di "corpo elettronico" – *pendant* del "corpo fisico" di ogni individuo – che ormai ciascuno di noi possiede e che lascia tracce ovunque. Un "corpo elettronico" dotato di sconfinata capienza, idoneo ad accogliere una massa sterminata d'informazioni capaci di rilevare il contenuto d'intere esistenze e adatte a sedare anche la più bulimica istanza di conoscenza. Un corpo, tra l'altro, estremamente *light*; facile da trasportare; rapido nei suoi spostamenti sì da renderlo, spesso, delocalizzabile. Un corpo, comunque, da tutelare e rispetto al quale le tradizionali garanzie apprestate per porre al riparo l'individuo da indesiderate invasioni della propria sfera personale si mostrano spesso inadeguate. Un corpo, quindi, in relazione al quale i principi tipici che fondano il corretto bilanciamento fra istanze repressive e garanzie individuali e su cui si basano i modelli di cooperazione giudiziaria non sempre offrono sufficienti presidi di tutela e, frequentemente, non paiono invocabili sì da rendere impraticabile il ricorso agli stessi».

[82] La nozione di privata dimora è, secondo la Cassazione, più estesa di quella di "abitazione". Caratteristiche sono: l'utilizzo del luogo per lo svolgimento di manifestazioni della vita privata, tra cui anche quella lavorativa, al riparo da intrusioni esterne; la stabilità del rapporto tra luogo e individuo; lo *ius excludendi alios*. Sulla riconducibilità dei luoghi di lavoro a luoghi di privata dimora v., Cass., S.U., 23 marzo 2017 n. 31345 , e anche BERNARDI S., *Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624-bis c.p.,* in *Dir. Pen. Cont.*, 4 luglio 2017; Cass., Sez. V, 18 luglio 2017, n. 38400. Sulla riconducibilità dello studio legale alla privata dimora v. Cass., Sez. V, 11 aprile 2023, n. 15216*;* MARTIN F., *Cass. Pen., Sez. V, 11 aprile 2023,*

oggetto di protezione all'art. 14 della Carta costituzionale e all'art. 8 della CEDU. E infatti, le profonde trasformazioni avvenute hanno portato a nuove declinazioni dei diritti tradizionali e, perfino, al riconoscimento di un "domicilio informatico" o "digitale", tale da profilare un diritto dinamico all' «intangibilità della vita digitale»[83].

In tal senso, il domicilio informatico[84] sarebbe configurabile «in rapporto a qualunque "luogo" informatico che, pur essendo immateriale, soddisfi gli stessi requisiti previsti per il domicilio tradizionale, che si compendiano nello *ius includendi se*, nello *ius includendi et excludendi alios*; nella destinazione del luogo ad attività private tipiche della vita domestica o a spazio di attività lavorativa»[85].

L'utilizzo massiccio di questa tipologia di prova ha finito per sottrarre alla testimonianza la sua natura di fonte privilegiata nel processo penale, con una conseguenza di non poco rilievo: lo spostamento dell'asse processuale verso la fase delle indagini preliminari, caratterizzata, com'è noto, da una tendenziale segretezza ma, soprattutto, dalla carenza di un contraddittorio con la difesa.

«Si osservi per inciso che, se il momento genetico della prova informatica si colloca fuori dall'alveo dibattimentale, l'incremento statistico del suo uso processuale coopera nel determinare la perdita di centralità del dibattimento nonché la crisi dell'assetto del sistema processuale tendenzialmente accusatorio voluto dal codice del 1988. La prova narrativa diventa sempre più residuale e con essa sfuma l'importanza del valore poietico del contraddittorio»[86].

Come già anticipato, il sistema processuale penale italiano, a oggi, non fornisce alcuna definizione di prova digitale[87], ma si è limitato ad adeguare alcuni istituti già presenti nel codice di rito alle innovazioni tecnologiche.

---

n. 15216, sulla nozione di privata dimora con riferimento allo studio legale, in www.iusinitinere.it, 2 maggio 2023.

[83] SIRACUSANO F., *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., p. 69.

[84] «Da intendere, in linea con quanto emergente dalla Raccomandazione del Consiglio d'Europa n. 9 del 1989, quale "spazio ideale di esclusiva pertinenza di una persona fisica o giuridica", delimitabile prendendo come parametro il domicilio delle persone fisiche, ed al quale risulta estensibile la tutela della riservatezza della sfera individuale, che costituisce bene costituzionalmente protetto», Cass., Sez. II, 14 gennaio 2019, n. 21987. V. anche Cass., Sez. V, 14 ottobre 2020, n. 37524.:«il legislatore ha assicurato la protezione del "domicilio informatico" quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto, Tuttavia l'art. 615-*ter* c.p. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "*jus excludendi alios*", quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente», Cass., Sez. V, 8 maggio 2012, n. 42021.

[85] Cfr., SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 63.

[86] In questi termini SANNA A., *La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati*, in *Discrimen*, 2022, p. 229.

[87] Sulle lacune dell'ordinamento v. DANIELE M., *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. Pen. Giust.*, 2018, 5, pp. 831-838: «Mai nella storia gli organi inquirenti

L'occasione è stata offerta dall'esecuzione, sia pure con notevole ritardo, della Convenzione di Budapest sul *cybercrime*. Quest'ultima, aperta alla firma il 23 novembre 2001, assume particolare rilievo poiché costituisce il primo documento internazionale dedicato agli strumenti processuali di contrasto ai crimini commessi attraverso *internet* o altre reti informatiche.

Come però sottolineato dalla dottrina[88], con l'esecuzione ad opera della l. 18 marzo 2008, n. 48[89], il legislatore si è limitato a una mera trasposizione della normativa europea, perdendo l'occasione per introdurre una nuova disciplina compiutamente dedicata al fenomeno delle indagini informatiche[90].

Peraltro, il ritardo di sette anni dalla data di ratifica della Convenzione ha finito per vanificare la potenziale portata innovativa delle norme introdotte dalla legge n. 48/2008, alcune peraltro già collaudate attraverso le prassi applicative messa in atto nelle procure tradizionalmente più attente ai profili delle cyber investigazioni[91].

L'intervento normativo si è infatti mosso in una duplice direzione: da una parte, si è inciso sui tradizionali mezzi di ricerca della prova, disciplinati nel libro III del c.p.p., adeguandoli alle caratteristiche della prova digitale, con l'obiettivo di preservare l'integrità

---

hanno avuto a disposizione armi così potenti e pericolose. Eppure, finora il legislatore non è stato abbastanza rapido nel frenarne l'utilizzo, ignorando gli sviluppi dell'informatica o, comunque, non riuscendo a coglierne tutte le implicazioni. Un'inadeguatezza che emerge tanto a livello nazionale, considerate le lacune e le incoerenze che contraddistinguono le norme vigenti in materia, quanto a livello sovranazionale, laddove la cooperazione giudiziaria non riesce a liberarsi di schemi ormai superati. […] Dovrebbe essere la legge a contenerne le violazioni, autorizzando compressioni della *privacy* nei limiti dello stretto indispensabile. Ma non è questa la sensazione che si ricava dalla disciplina italiana, la quale manca tuttora di un approccio adeguato alla tematica».

88 CAJANI F., *Giurisdizione e competenza nelle indagini informatiche*, in ATERNO S., CAJANI F., COSTABILE G., CURTOTTI D., (a cura di) Cyber Forensics *e Indagini digitali. Manuale tecnico-giuridico e casi pratici,*cit.

89 Per approfondimenti, v., tra i tanti, BARTOLI L., LASAGNI G., *The handling of digital evidence in Italy*, in CAIANIELLO M., CAMON A. (a cura di), *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, Cedam, 2021; CONTI S., *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, 2015, 1-2, pp.153-164; LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. I profili processuali*, in *Dir. Pen. proc*., 2008, pp. 717 e ss; TORRE M., *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, in *Informatica e diritto*, 2015, vol. XXIV, 1-2, pp- 65-2014; PITTIRUTI M., *Profili processuali della prova informatica,* in L. MARAFIOTI, G. PAOLOZZI (a cura di), '*Incontri ravvicinati' con la prova penale*, G. Giappichelli Editore, 2014, p. 53.

90 SIRACUSANO F., *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., p. 190: «È noto come, entro i nostri confini, l'opera d'innesto delle "nuove tecnologie" nel tessuto dell'accertamento processuale si è tradotta – per il tramite della ratifica della Convenzione del 2001 – in una mera "riscrittura" dei tradizionali strumenti di ricerca e raccolta della prova (ispezioni, perquisizioni, sequestri, accertamenti urgenti di p.g., acquisizione di plichi e corrispondenza), riqualificandoli nella natura "informatica", adattandoli all'estrema volatilità e alterabilità del dato digitale attraverso il costante richiamo all'esigenza di adottare procedure idonee ad assicurare la conformità dei dati acquisiti a quelli originali e la loro immodificabilità; secondo un itinerario più volto a specificare l'obiettivo da raggiungere che a regolare le modalità della raccolta».

91 In questi termini CAJANI F., *Giurisdizione e competenza nelle indagini informatiche*, cit., p. 178.

e l'autenticità dei dati acquisiti; dall'altra, si è agito sul d. lgs. 30 giugno 2003, n. 196, c.d. Codice della *privacy* [92], introducendo alcune disposizioni in materia di *data retention*.

Dalla riforma del 2008 – sulla quale si tornerà nel prossimo paragrafo – il tema della prova digitale non è stato più al centro degli interessi del legislatore.

Sul versante dei mezzi di ricerca della prova, l'attenzione si è piuttosto concentrata sulle intercettazioni di conversazioni (art. 266 ss. c.p.p.), con l'introduzione – sull'onda delle Sezioni Unite "Scurato"[93] – di una specifica disciplina per quelle compiute mediante l'utilizzo del captatore informatico (c.d. *trojan)* su dispositivi mobili, *ex* art. 266 co. 2 e 2-*bis* c.p.p, 267 co. 2-*bis* c.p.p. e 270 co. 1-*bis* c.p.p.

La novella introdotta con il d. lgs. 29 dicembre 2017, n. 216[94], in attuazione dei criteri contenuti all'art. 1 co. 84 lett. e) della l. 23 maggio 2017 n. 103 (c.d. Riforma Orlando)[95], è stata oggetto di successivi aggiustamenti, nel tentativo di trovare un equilibrio tra esigenze investigative e protezione dei diritti individuali.

Nello specifico, riguardo all'uso del *trojan*, equiparato a un'intercettazione ambientale, si è codificato una sorta di "doppio binario" o, addirittura, "triplo", in relazione alla tipologia di reati per i quali si sta procedendo. L'intercettazione per i reati comuni non potrà, infatti, svolgersi nel domicilio, a meno che vi sia fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

---

[92] D. lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, in G.U. n.174 del 29-07-2003 - Suppl. Ordinario n. 123.

[93] Cass., Sez. Unite, 28 aprile 2016, n. 26889: la Corte ha stabilito che, solo nei casi di procedimenti per delitti di criminalità organizzata, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti - mediante installazione di un "captatore informatico" in dispositivi elettronici portatili - anche nei luoghi di privata dimora *ex* art. 614 c.p., pur se non singolarmente individuati e se ivi non si stia svolgendo attività criminosa. Sull'argomento, v., tra i tanti, CENTORAME F., *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. It. Dir. e Proc. Pen.*, 2022, 2, pp. 499 -523; GIORDANO L., *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in *Dir. Pen. Cont.*, 27 settembre 2017; GIORDANO L., *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *www.sistemapenale.it,* 21 aprile 2020. V. anche CAPRIOLI F., *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. de dereito processual penal*, 2017, vol. 3, 2. Per una disamina sull'evoluzione della disciplina vedasi FELICIONI P., *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. Pen. Giust.*, 2016, 5, p. 118.

[94] D. lgs. 29 dicembre 2017, n. 216, recante *Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103*; in G.U. Serie Generale n.8 del 11/01/2018.

[95] L. 23 giugno 2017, n. 103, *Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario,* in G.U. Serie generale n. 154 del 04/07/2017. V. il commento di GALLUCCIO A., in *Dir. Pen. Cont.*, 6 luglio 2017; DIDDI A., *Le novità in materia di intercettazioni telefoniche*, in *www.penaledp.it, 31* agosto 2020; GIALUZ M., CABIALE A., DELLA TORRE J., *Riforma Orlando: le modificazioni attinenti al processo penale, tra codificazione della giurisprudenza, riforme attese da tempo e confuse innovazioni*, in *Dir. Pen. Cont.*, 20 giugno 2017.

La captazione all'interno del domicilio è, invece, sempre prevista per i delitti più gravi *ex* art. 51 co. 3-*bis* e *quater* c.p.p. e per quelli contro la pubblica amministrazione[96] commessi da pubblici ufficiali o incaricati di pubblico servizio, per cui è prevista la pena della reclusione non inferiore nel massimo a 5 anni.

In linea con la disciplina generale, l'intercettazione mediante captatore è disposta dal pubblico ministero, previa autorizzazione del giudice per le indagini preliminari (art. 276 co. 1 c.p.p.), che a seguito dell'ultimo intervento di riforma[97], oltre ad indicare i presupposti che legittimano l'utilizzo di questo strumento così invasivo, dovrà dare conto delle ragioni che rendono necessaria tale modalità di captazione, svolgendo una autonoma valutazione in concreto[98]. Il GIP dovrà, inoltre, precisare i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione microfono, ad eccezione dei casi in cui si proceda per delitti di cui all'articolo 51 co. 3-*bis* e 3-*quater* e per i delitti contro la pubblica amministrazione commessi da pubblici ufficiali o incaricati di pubblico servizio per cui è prevista la pena della reclusione non inferiore nel massimo a 5 anni.

Nei casi di urgenza, il pubblico ministero potrà disporre l'intercettazione a mezzo captatore emanando un decreto motivato da comunicare immediatamente, e non oltre le 24 ore, al giudice e solo per le specifiche categorie di delitti di cui sopra (art. 267 co. 2 c.p.p.).

L'intercettazione potrà proseguire solo qualora entro 48 ore il giudice decida sulla convalida con decreto motivato.

L'intervento normativo non ha mancato di sollevare perplessità per la sua incompletezza. Il legislatore, infatti, si è limitato a disciplinare l'uso del captatore come strumento di acquisizione delle conversazioni, trascurando le innumerevoli potenzialità che questo assume sul piano operativo. Secondo la giurisprudenza[99], «il "captatore informatico", lungi

---

[96] Il riferimento ai delitti contro la pubblica amministrazione è stato aggiunto dall'art. 1 co. 4 lett. a) della l. 9 gennaio 2019, n. 3 recante "*Misure per il contrasto dei reati contro la pubblica amministrazione nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*". V. GRIFFO M., *Rilievi sull'impiego del troyan nei procedimenti per i reati contro la pubblica amministrazione*, in *Proc. Pen. Giust.*, 2020, 2, pp. 482-489.

[97] D.l. 10 agosto 2023 n. 105, *Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché' in materia di personale della magistratura e della pubblica amministrazione,* in G.U. Serie Generale n.186 del 10/08/2023, convertito con modifiche in l. 9 ottobre 2023 n. 137, *Conversione in legge, con modificazioni, del decreto-legge 10 agosto 2023, n. 105, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché' in materia di personale della magistratura e della pubblica amministrazione* in G.U. Serie Generale n.236 del 09/10/2023. V. CELOTTO A., *Sulla conversione in legge del decreto-legge 10 agosto 2023, n. 105 (disposizioni urgenti in materia di processo penale,* in *Giurisprudenza Penale,* 2023, 9; LAZZERI F., *Convertito in legge, con modificazioni, il d.l. 105/23: novità in materia di intercettazioni, incendio boschivo, ambiente e 231*, in *www.sistemapenale.it*, 5 ottobre 2023.

[98] Art. 1 co. 2-*bis* d.l. 105/2023. Sull'indicazione delle modalità di captazione v. Cass., 18 novembre 2020, n. 32428.

[99] Cass., Sez. V, 30 settembre 2020, n. 31604.

dal costituire un autonomo mezzo di ricerca della prova, è solo una particolare modalità tecnica per effettuare l'intercettazione delle conversazioni tra presenti».

È noto, però, come il captatore consenta di attivare la *webcam*, di effettuare una copia dei dati contenuti nel dispositivo (*online search*), di monitorare i flussi di dati *(online surveillance*), di verificare l'attività eseguita con le periferiche di *input* (tastiera e mouse) e di *output* (monitor, stampante).

Ebbene, come osservato dalla dottrina[100], «non regolamentare equivale a lasciar spazio a prassi devianti o ad improbabili letture giudiziarie più o meno marcatamente estensive della normativa vigente, piegata ad un adattamento forzato e spesso inadeguato imposto proprio dall'immobilismo del legislatore».

Di fatto ciò è quanto avvenuto: i vuoti normativi hanno favorito una giurisprudenza creativa che ha finito per ricondurre alla disciplina delle intercettazioni attività non assimilabili e che meriterebbero una disciplina *ad hoc* [101], come l'acquisizione di *screenshot* di *file excel* presenti in un dispositivo[102], nonché di escludere attività che potevano invece esservi ricondotte, come l'apprensione di *email* appositamente depositate nella cartella bozze della casella di posta[103].

2.1.1 La l. 48/2008: un'opera incompiuta

Come anticipato, il primo e ultimo intervento normativo in tema di prova digitale si deve alla l. n. 48/2008.

---

[100] LORUSSO S., *Digital evidence, cybercrime e giustizia penale 2.0*, in *Proc. Pen. Giust.*, 2019, 4, p. 822.

[101] Vedasi GIORDANO L., *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. Pen. Cont.*, 20 marzo 2017, p. 187.

[102] Cass., Sez. I, 7 ottobre 2021, 3591, Romeo, con nota di FROVA G., *La Cassazione sulla riconducibilità all'art. 266 c.p.p. degli* screenshot *tramite captatore informatico*, in *www.sistemapenale.it,* 2 giugno 2022: «Pur riconoscendo l'utilità pratica della soluzione fornita dalla pronuncia in esame, si esprime perplessità circa la conformità ai principi, in ragione di un'interpretazione dell'art. 266 *bis* c.p.p. da ritenersi eccessivamente ampia, in possibile contrasto con la lettera della legge ove richiede che il flusso informatico o telematico oggetto di intercettazione sia di carattere comunicativo. Tuttavia, se ne deve riconoscere l'ineluttabilità in ragione di una stasi del legislatore che quando nel 2017 con la c.d. "Riforma Orlando" ha normato l'utilizzo del captatore informatico per la prima – ed unica – volta, ha regolato il solo utilizzo che, forse, sarebbe stato dominabile dall'interprete, ossia quello relativo all'attivazione del microfono del dispositivo infettato al fine dell'intercettazione fra presenti ai sensi dell'art. 266 comma 2 c.p.p., evitando invece di disciplinare gli impieghi che risultano essere nella pratica maggiormente problematici».
Sulle modalità di captazione attraverso il captatore, e nello specifico sulla scarsa precisione dei decreti autorizzativi, sulla mancata adeguata documentazione e verbalizzazione delle operazioni vedasi Cass., Sez. IV, 24 settembre 2020, n. 32428 con nota di FILIPPI L, *Il* virus trojan*: uno strumento nelle mani incontrollabili della polizia giudiziaria,* in *www.penaledp.it,* 20 novembre 2020.

[103] In merito all'utilizzo del captatore con funzione di *keylogger* vedasi Cass., Sez. IV, 28 giugno 2016, n. 40903, Grassi. Nel caso di specie il captatore è stato utilizzato per apprendere tutto ciò che veniva digitato sulla tastiera. In tal modo le autorità hanno preso conoscenza degli *account* e delle *password* di *account* di posta elettronica che venivano utilizzati per lo scambio di *email* e di comunicazioni, che venivano lasciate appositamente nella cartella "bozze" per non incorrere nella possibilità di essere intercettati. Cfr. GIORDANO L., *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, cit.

Sul versante delle modifiche al codice di rito, questa ha operato nell'alveo della disciplina in tema di ispezioni, integrando l'art. 244 co. 2 c.p.p., e perquisizioni, mediante l'innesto del nuovo co. 1-*bis* dell'art. 247 c.p.p.

Inoltre, si è introdotto l'art. 254-*bis* c.p.p., relativo al sequestro di dati informatici e si è modificato l'art. 260 co. 2 c.p.p., in tema di apposizione di sigilli.

Tra gli obiettivi della riforma vi era quello di favorire l'acquisizione di una prova genuina e di garantire l'inalterabilità dei dati acquisiti, attraverso la creazione di copie conformi all'originale e modalità idonee e adeguate a tale scopo[104]. Tuttavia, come si avrà modo di analizzare, gli obiettivi non sembra siano stati conseguiti in maniera efficace, anche a causa di alcune lacune non colmate dal legislatore.

In particolare, nulla è stato precisato in merito al regime applicabile nel caso di mancata adozione delle procedure consigliate per l'acquisizione della prova, lasciando alla giurisprudenza il delicato compito di stabilire se si possano configurare dei casi di inutilizzabilità o se ciò rilevi solo in relazione alla valutazione da parte del giudice, con chiare ripercussioni sulla genuinità della prova, sul principio del contraddittorio e il diritto a un equo processo.

Nello specificare le modalità di esecuzione dell'ispezione e della perquisizione, qualora abbiano a oggetto sistemi informatici o telematici, il legislatore, come già anticipato, ha posto l'accento sulla necessità di adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione.

L'ispezione, mezzo di ricerca della prova finalizzato ad accertare le tracce e altri effetti materiali del reato, permette all'autorità giudiziaria di visionare e descrivere lo stato attuale di cose, luoghi, persone e di valutare quello preesistente e le eventuali modifiche intervenute.

Trattandosi di un atto irripetibile, le cui risultanze confluiscono nel fascicolo per il dibattimento, risulta fondamentale, nel caso di ispezioni su sistemi informatici o telematici, adottare le misure idonee a preservare i dati originali impedendone l'alterazione.

---

[104] COLAIOCCO A., *La rilevanza delle* best practices *nell'acquisizione della* digital evidence *alla luce delle novelle sulla cooperazione giudiziaria,* in *Arch. Pen.*, 2019, n. 1; ZICCARDI G., *L'ingresso della* computer forensics *nel sistema processuale italiano*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)*, Giuffrè, 2009, p. 170: «Corrette modalità di conservazione, procedure di duplicazione efficaci, garanzie di non alterabilità e *extrema ratio* del sequestro di servizi sono, in conclusione, i quattro principi della *forensics* introdotti nel nostro ordinamento».

Quanto alla perquisizione, l'attività, disposta con decreto motivato dell'autorità giudiziaria, si concretizza nella ricerca del corpo del reato o di cose pertinenti al reato su persone, luoghi o sistemi informatici o telematici, finalizzata al sequestro.

Anche in questo caso, in quanto atto strutturalmente irripetibile, le risultanze confluiranno nel fascicolo per il dibattimento e, allo stesso modo delle ispezioni di sistemi informatici, sarà opportuno l'utilizzo di misure tecniche dirette ad assicurare la conservazione dei dati originali e impedirne l'alterazione. Alcune questioni si sono poste rispetto al distinguo tra perquisizioni e captatore informatico.

In relazione a un caso in cui la polizia giudiziaria aveva "fotografato" un file *excel* contenuto nel personal computer del soggetto mediante l'utilizzo del *trojan*, la giurisprudenza[105] ha escluso l'applicazione della disciplina in tema di perquisizione.

Si è osservato, infatti, che l'attività investigativa non ha riguardato l'estrapolazione di materiale preesistente all'attività intercettiva, ma soltanto la captazione di flussi di dati *in fieri*, cristallizzati nel momento stesso della loro formazione. Una tale attività di mera "constatazione" dei dati informatici in corso di realizzazione, pur non costituendo una "comunicazione" in senso stretto, costituisce, invece, un comportamento cd. comunicativo, del quale è ammessa la captazione – previo provvedimento autorizzativo dell'AG – nonché la videoregistrazione, dunque anche la fotografia, nel caso di specie mediante *screen shot* della schermata.

L' esigenza di tutela dell'originalità dei dati si manifesta più chiaramente nella disciplina contenuta agli artt. 254-*bis* c.p.p. – specificamente dedicato al sequestro di dati informatici – e 260 co. 2 c.p.p., dove si prevede che la copia di dati, informazioni e programmi informatici vada effettuata su adeguato supporto, assicurando la conformità della copia all'originale e la sua immodificabilità, per impedirne l'alterazione.

In relazione all'acquisizione di messaggi all'interno di un cellulare, si è escluso[106] che la loro estrazione possa essere ricondotta alla categoria degli accertamenti tecnici irripetibili, neppure dopo l'entrata in vigore della l. n. 48/2008. Quest'ultima avrebbe solamente introdotto l'obbligo di adottare modalità acquisitive idonee a garantire la conformità dei dati informatici acquisiti a quelli originali, con la conseguenza che né la mancata adozione di tali modalità, né, a monte, la mancata interlocuzione delle parti al riguardo, comportano l'inutilizzabilità dei risultati probatori acquisiti, ferma la necessità di valutare, in

[105] Cass., Sez. I, 7 ottobre 2021, n. 282495.
[106] Cass., Sez. I, 10 giugno 2021, Marziano, n. 282072.

concreto, la sussistenza di eventuali alterazioni dei dati originali e la corrispondenza ad essi di quelli estratti.

Il rispetto di queste prescrizioni incide sulla integrità della prova e sulla sua genuinità: uniche garanzie per l'esercizio del diritto di difesa e il corretto svolgimento del contraddittorio, secondo quanto sancito dall'art. 111 Cost.[107]. In questa prospettiva, sarebbe stato opportuno che il legislatore stabilisse dei precisi confini ricollegando il mancato utilizzo delle procedure previste a delle precise sanzioni[108].

La genuinità di una prova, allorquando l'atto sia irripetibile e il difensore non abbia potuto partecipare al suo svolgimento nel rispetto del contraddittorio, non può che essere verificata *ex post*[109].

In tal caso, pertanto, sarà fondamentale, a garanzia del diritto di difesa e dei principi dell'equo processo, permettere che il contradditorio nella formazione della prova sia sostituito dal principio del contraddittorio "sulla" prova, da esercitarsi in giudizio, in termini di argomentazione critica delle prove digitali assunte nella fase investigativa[110], così da consentire alla difesa di confutare la correttezza delle procedure eseguite e la prova stessa.

Questo si verifica solo quando la parte sia posta nelle condizioni di verificare l'affidabilità della fonte e la genuinità, elementi essenziali per l'esercizio del contraddittorio.

E proprio questo riempirebbe di contenuto la nozione di "non ripetibilità", «destinata, altrimenti, a restare una formula contenitore delle più disparate accezioni»[111].

«Il contraddittorio sugli aspetti tecnici e procedurali resta comunque un valore da garantire, a prescindere dallo strumento investigativo impiegato. Ma, per consentire una verifica effettiva sull'attività svolta, occorrerebbe imporre agli operatori di dare riscontro di ogni loro mossa in maniera meticolosa, documentandola anche tramite videoripresa»[112].

---

[107] Com'è noto, in ossequio all'art. 111 Cost., principio cardine del processo penale è quello della formazione della prova in contradditorio, derogabile nei soli casi di consenso dell'imputato, accertata impossibilità di natura oggettiva o per effetto di provata condotta illecita.

[108] Cfr. SANNA A., *La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati*, cit.

[109] Cass., Sez. Un., 18 dicembre 2006, n. 4128, Greco: «La nozione di atto non ripetibile non ha natura ontologica ma va ricavata dalla disciplina processuale. Ciò che rileva è il tipo di informazione contenuto nell'atto redatto dalla polizia giudiziaria: se contiene un tipo di accertamento che non sarà possibile compiere nuovamente nel dibattimento, secondo i criteri indicati, l'atto dovrà essere considerato non ripetibile – e quindi inseribile nel fascicolo per il dibattimento – indipendentemente dalla sua denominazione».

[110] SANNA A., *La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati*, cit., p. 227.

[111] TONINI P., *Considerazioni su diritto di difesa e prova scientifica*, in *Arch. Pen.*, 2011, n. 3, p.9.

[112] PARLATO L., *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale, i*n *Proc. Pen. Giust.*, 2020, 2, p. 302, la quale osserva come nella consapevolezza di queste criticità «quanto al diverso fenomeno delle intercettazioni il legislatore ha ora cercato di introdurre qualche correttivo, a dire il vero non adeguato: da un canto, disponendo che possano essere «impiegati soltanto programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia», dall'altro, prevedendo "informazioni" e "controlli" in merito alle "condizioni tecniche di sicurezza e di affidabilità della rete di trasmissione" e sull'"integrità" dei sistemi utilizzati; ed ancora consentendo al difensore, al termine delle indagini, di estrarre copia di verbali e registrazioni custodite nell'"archivio informatico" introdotto dalla

Queste cautele «renderebbero tracciabile ciascun passaggio, rivelando lo specifico impatto delle manovre impresse al sistema informatico: pur trattandosi di operazioni non ripetibili, sarebbe così possibile garantire quantomeno un monitoraggio postumo sulla "sostenibilità scientifica" del procedimento eseguito».

Quanto detto assume particolare rilevanza sul fronte della prova digitale, specie in ragione della sua facilità di alterazione e manipolazione. Un minimo errore può, infatti, compromettere irrimediabilmente il valore probatorio dell'elemento e disperdere materiale fondamentale per le indagini e per il processo, oltre che per la difesa dell'imputato: si pensi a elementi utili al fine di dimostrare l'alibi.

Il valore della prova, infatti, deriva proprio dalla possibilità di esercitare un controllo sulla fonte stessa e sull'elemento acquisito. Tale controllo sarà possibile solo quando la prova sia rimasta inalterata; viceversa, la possibilità di valutarne la genuinità e affidabilità è preclusa *a priori*.

Nel caso della prova digitale, il metodo più corretto – secondo la *digital forensics* – consiste nell'effettuare una copia o *bit stream image* che riproduca *bit* a *bit* il dato che si vuole acquisire, per poter poi effettuare tutte le analisi sulla stessa, lasciando inalterato il dato originale. La copia andrà, inoltre, effettuata secondo le linee guida[113], per non alterarla o perderla inavvertitamente.

Le principali verifiche da eseguire *ex post* riguarderanno l'affidabilità del metodo di acquisizione, l'utilizzo delle linee guida o *best practices*, nonché il rispetto della catena di custodia. A questo punto, è da domandarsi quali siano le conseguenze se, acquisendo la prova in modo unilaterale, non sia rispettata la ripetibilità della prova o la correttezza delle procedure.

Parte della dottrina[114] ritiene che le norme introdotte dalla l. 48/2008, nella parte in cui richiedono l'utilizzo di mezzi atti a preservare l'integrità della prova, abbiano codificato

---

riforma: con la precisazione, tuttavia, che quest'ultima possibilità concerne le solo risultanze ritenute rilevanti dal pubblico ministero».

[113] La disciplina dettata dal legislatore non fornisce chiare indicazioni sulle procedure da utilizzare, per non creare una disciplina di dettaglio troppo rigida in vista della rapidità dell'evoluzione tecnologica. Gli *standard* a cui genericamente si fa riferimento a livello internazionale sono: ISO/IEC 27037 "*Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*" e ISO/IEC 27042 "*Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*". Per un approfondimento sulle procedure di *digital forensics* v. KÄVRESTAD J., *Fundamentals of Digital Forensics. Theory, Methods, and Real-Life Applications*, Springer, 2018; HASSAN N.A., *Digital Forensics Basics. A practical guide using Windows OS,* Apress, 2019; PETERSON G., SHENOI S. (a cura di*), Advances in Digital Forensics XV*, Springer, 2019; ZICCARDI G., *L'ingresso della* computer forensics *nel sistema processuale italiano*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)*, cit.

[114] TONINI P., *Considerazioni su diritto di difesa e prova scientifica*, cit., p.14.

dei divieti probatori sanzionati con l'inutilizzabilità. A sostegno di questo argomento si afferma che «quando la prova è informatica, la forma della acquisizione della prova è determinante per la sostanza dell'elemento acquisito. La qualità dell'elemento acquisito, in definitiva, dipende dal metodo impiegato: *simul stabunt, simul cadent*. Se il metodo è errato, l'elemento di prova è compromesso in modo non rimediabile nella sua possibilità di controllo».

In senso contrario, in merito al rispetto di specifiche procedure e *standard*, un orientamento giurisprudenziale[115] ritiene che il mancato rispetto delle *best practices* non determini *per se* l'inutilizzabilità delle prove, lasciando libera discrezionalità al giudice in sede di valutazione[116].

Profili di interesse presenta il caso *Vierika*, nel quale il Tribunale di Bologna ha ritenuto che fosse onere della difesa provare che la procedura utilizzata dalla polizia giudiziaria avesse alterato i dati, configurando così una vera e propria *probatio diabolica*.

Sulla stessa linea, riguardo al rispetto della catena di custodia, strumento chiave per valutare la correttezza metodologica della prova, si pone altra parte della giurisprudenza[117], ritenendo che un'eventuale violazione non determini una nullità o invalidità del sequestro, trattandosi di mere irregolarità formali, non idonee a configurare un'inutilizzabilità.

Questi orientamenti giurisprudenziali suscitano inevitabilmente delle perplessità, poiché, se da un lato riconoscono l'importanza dell'integrità della prova, al contempo, escludono che dal mancato rispetto delle previsioni possa derivare un qualunque tipo di invalidità[118].

Di fatto, in questo modo si finisce per svuotare la portata innovativa della l. 48/2008, con il rischio di pregiudicare i diritti fondamentali e, in maniera specifica, il diritto al contraddittorio e quello di difesa.

2.1.2. L'assenza di una disciplina ad hoc *e l'inquadramento negli istituti preesistenti*

[115] Tribunale Penale di Bologna, Sez. I, 21 luglio 2005, n. 1823, *Vierika*.

[116] GIUNCHEDI F., *Le* malpractices *nella* digital forensics. *Quali conseguenze sull'inutilizzabilità del dato informatico?,* in *Arch. pen*, 2013, n. 3, pp. 821-836.

[117] Cass., sez III, 16 dic 2009, n. 1993, Pirrotta; Cass., Sez. VI, 26 maggio 2011, Valente: «Riguardo al primo motivo contenuto nel ricorso presentato nell'interesse di V., si rileva che sia la mancata verbalizzazione dei modelli e degli altri elementi identificativi dei computers sequestrati, sia la mancata apposizione dei sigilli, non determinano alcuna nullità o, in genere, invalidità, del sequestro, dovendo considerarsi semplici irregolarità formali, prive di conseguenze sulla validità del provvedimento cautelare e comunque inidonee a determinarne l'inutilizzabilità».

[118] BARTOLI L., MAIOLI C., *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti,* in *Informatica e diritto*, 2015, vol. XXIV, p 139.

A fronte del mancato inquadramento della prova digitale all'interno di una categoria *ad hoc*, nella prassi si tende a ricondurla, in maniera del tutto anacronistica, agli atti tipici di indagine[119] o all'art. 189 c.p.p., in tema di prove atipiche. Quest'ultima norma consente, infatti, quando la prova richiesta non è disciplinata dalla legge, di assumerla, se idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. In tal caso, il giudice provvede all'ammissione dopo che si sia svolto il contraddittorio delle parti sulle modalità di assunzione. Eppure, in questa ipotesi, è difficile avviare un confronto delle parti sull'ammissione della prova e sulle modalità di assunzione, trattandosi di attività di indagine che spesso si svolgono in assoluta segretezza.

Ciononostante, nel corso degli anni, la giurisprudenza ha manifestato la tendenza a ricondurre all'art. 189 c.p.p. qualsiasi strumento che si discosti dal paradigma legale, privilegiando le scelte investigative a scapito della tutela dei diritti fondamentali [120].

In senso opposto, parte della dottrina[121] ritiene che non ogni tipo di prova scientifica possa ricondursi all'art. 189 c.p.p. In particolare, si esclude l'applicabilità di questa disposizione con riguardo a prove che siano espressione di istituti già codificati. Questa tesi ha, peraltro, trovato conferma nella scelta del legislatore di strutturare, all'interno di atti tipici - quali le ispezioni o le perquisizioni - specifiche modalità di acquisizione della prova, allorquando il dato sia contenuto su supporti informatici[122].

In alternativa, parallelamente al richiamo all'art. 189 c.p.p., si è fatto ampio ricorso anche alla disciplina di istituti peculiari, modellata sulle base delle circostanze specifiche.

Del tutto diverso è il caso del captatore informatico che, come è stato evidenziato, è espressamente disciplinato dall'art. 267 co. 2-*bis* c.p.p. in relazione allo svolgimento di intercettazioni. Tuttavia, attraverso l'installazione di uno *spyware* in un dispositivo portatile sono eseguibili molteplici attività, non esclusivamente riconducibili alla captazione di

---

[119] In proposito LORUSSO S., Digital evidence, cybercrime *e giustizia penale 2.0*, cit., p. 823 : «Ispezioni, perquisizioni, sequestri, intercettazioni di comunicazioni: categorie tradizionali, collocate in un preciso e rigoroso recinto, sono state piegate per comodità, pigrizia e superficialità dei *conditores* –ma forse anche per una mancata (o quantomeno insufficiente) consapevolezza della novità e della rilevanza del fenomeno da normare – allo scopo di regolamentare strumenti investigativi e probatori la cui specificità, quanto meno in ragione delle caratteristiche esclusive del dato informatico (a partire dalla sua natura immateriale), avrebbe imposto una normativa anche concettualmente *ad hoc* in grado di assorbire i connotati di tali fonti di prova e di restituirli sotto forma di coerente architettura normativa. Evitando di far insorgere problematiche e di far emergere criticità probabilmente prevedibili, a partire dalla fase investigativa – ove la maggiore fluidità del dato probatorio comporta fatalmente un maggior grado d'incidenza sui diritti fondamentali dei soggetti coinvolti, sia in chiave processuale che extraprocessuale – per giungere a quella dibattimentale, dove la dote ricevuta dal precedente stadio procedimentale è di per sé ricca di un patrimonio probatorio digitale, per sua natura formatosi in assenza di contraddittorio, spendibile per la decisione finale. Avrebbero dovuto essere sufficienti queste considerazioni a suggerire maggiore attenzione ed oculatezza ad un legislatore che, invece, sembra sia stato colto di sorpresa dalla tempesta digitale».

[120] Vedi Cass., Sez. V, 18 novembre 2020, n. 32428.

[121] MARAFIOTI L., Digital evidence *e processo penale*, in *Cass. Pen.*, 2011, p. 4511.

[122] PITTIRUTI M., Digital evidence *e procedimento penale*, cit., p. 19.

comunicazioni[123]. Si possono, infatti, menzionare l'attivazione della *webcam* o del microfono, l'esecuzione della copia dei dati (*online search*), il monitoraggio dei flussi di dati *(online surveillance*), la verifica dell'attività eseguita con le periferiche di *input* (tastiera e *mouse*) e di *output* (monitor, stampante) e molte altre attività che il legislatore ha mancato di disciplinare. Tutte queste attività investigative, non tipizzate dall'ordinamento, quando non ricondotte all'art. 189 c.p.p., in giurisprudenza[124] vengono sovente scomposte e ancorate ora alla disciplina in tema di intercettazioni di telecomunicazioni *ex* art. 266 c.p.p. (come nel caso delle *email* o di conversazioni avvenute in *chat*), ora al sequestro *ex* art. 253 c.p.p., ovvero alla perquisizione *ex* art. 247 c.p.p. o all'acquisizione di documentazione *ex* art. 243 c.p.p.

A tale riguardo, non sono mancate le critiche da parte della dottrina[125], la quale ritiene tali orientamenti «forier(i) di una mentalità che fatica a disancorarsi da una visione corporea degli elementi di prova tradizionali»[126] e che tenta di conformare «all'orizzonte digitale istituti concepiti con precipuo riferimento a realtà tangibili»[127].

In altri casi il legislatore ha invece tentato di adattare gli istituti tradizionali alle nuove tipologie investigative mediante una serie di inserimenti normativi che, tuttavia, concepiscono ancora le indagini informatiche alla stregua delle ordinarie attività investigative, dimenticando le peculiarità specifiche che le caratterizzano. Emblematica è la disciplina delle ispezioni e perquisizioni informatiche di cui sopra: in questo ambito sarebbe stato auspicabile introdurre una normativa *ad hoc,* piuttosto che prevedere peculiari modalità di esecuzione solo per lo specifico caso degli elementi digitali.

La varietà di istituti codicistici ai quali dottrina e giurisprudenza hanno fatto riferimento per l'acquisizione della prova digitale è ampia, a cominciare dalla prova documentale.

Il disposto dell'art. 234 c.p.p., che prevede l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo, va analizzato insieme all'art. 234-*bis* c.p.p[128]. Quest'ultima previsione, inserita dall'art. 2 del d.l. 18 febbraio 2015 n. 7, convertito con l. 17 aprile 2015 n. 43 in tema di contrasto al terrorismo, permette l'acquisizione di documenti

---

[123] Vedasi FILIPPI L., *Il cavallo di Troia e l'ispe-perqui-intercettazione*, in *www.penaledp.it* ,21 marzo 2022.
[124] Tra le tante Cass., sez I, 7 ottobre 2021, n. 282495; Cass., Sez. IV, 28 giugno 2016, n. 40903; Cass., Sez. I, 1 febbraio 2022, n. 3591.
[125] Cfr. SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p.120 ss.
[126] *Ibidem*, p. 123.
[127] *Ibidem*.
[128] Sulla prova documentale in relazione alle conversazioni W*hatsapp* DEL COCO R., *L'utilizzo probatorio dei dati whatsapp tra lacune normative e avanguardie giurisprudenziali,* in *Proc. Pen. Giust.*, 2018, 3, p. 532.

e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso del legittimo titolare[129]. A quest'ultimo riguardo, non è però chiaro, dal disposto normativo, se questo soggetto debba identificarsi nell'utente di un servizio o nel *provider*.

Profili di interesse presenta una pronuncia di legittimità che, con un'interpretazione ampia, lo ha individuato nella persona giuridica che può disporre dei dati o dei documenti[130], definizione ulteriormente ampliata dalla Corte di Cassazione in una successiva sentenza[131], secondo cui il titolare è «la persona giuridica che di quei documenti o di quei dati poteva disporre in forza di un legittimo titolo secondo l'ordinamento giuridico del Paese estero, identificabile non soltanto nella persona fisica e \o giuridica che procede alla trasmissione e alla conservazione dei dati, ma anche nella polizia giudiziaria, nell'autorità giudiziaria, nella persona offesa, nell'amministrazione pubblica, nella società che gestisce il servizio telefonico*, nell'internet service provider*».

Di avviso opposto altra parte della giurisprudenza, che ha escluso la possibilità di ricomprendere anche l'autorità giudiziaria – nel caso di specie straniera –, considerata «mero detentore qualificato di quei dati a fini di giustizia»[132].

Nella medesima sentenza si precisa come, in assenza del consenso legittimo, l'autorità potrà ottenere i dati solo facendo ricorso alla rogatoria o ad altro strumento di cooperazione internazionale che permetta di richiederne l'accesso.

Riguardo alla riconducibilità della prova digitale alla categoria del documento, in senso stretto o informatico, va evidenziato come la natura del documento mal si adatti alla varietà di forme che può assumere la prova digitale e alle sue caratteristiche intrinseche,

---

[129]PARODI C., *Profili tecnico-investigativi e di diritto processuale interno: dal* transborder access to data *al nuovo art. 234*-bis *c.p.p*., in *www.ilpenalista.it,* 31 maggio 2016.

[130] Cass., Sez. VI, 28 febbraio 2023, n. 8714.

In proposito PARODI C., *Profili tecnico-investigativi e di diritto processuale interno: dal* transborder access to data *al nuovo art. 234-bis c.p.p*., cit.:«una più che ragionevole alternativa – che tiene conto in termini realistici dei rapporti di forza, a livello nazionale come internazionale, tra autorità giudiziarie e operatori del settore dell'informatica e delle comunicazioni – può derivare dall'identificazione del titolare sulla base degli accordi contrattuali tra società e clienti. Un titolare quindi individuabile sulla base del contenuto degli accordi e dei contratti stipulati tra utenti e società in occasione dell'attivazione del servizio. Accordi e contratti nell'ambito dei quali i grandi *player* internazionali del settore comunicazioni ed i più diffusi *internet service provider* delineano e regolamentano il potere ed il diritto di disporre dei dati informatici degli utenti. In tale logica, indipendentemente dal soggetto materialmente inserisce dati, se il contratto prevede che il provider sia autorizzato a divulgare dati in determinate occasioni, il legittimo titolare, ai sensi dell'art. 234-*bis* c.p.p., deve essere individuato nel *provider* stesso, in quanto gestore dei dati, in quanto si tratta del soggetto al quale competono le decisioni in ordine al trattamento dei dati.Inoltre, se il consenso potesse essere prestato dal soggetto sul quale vertono le indagini- laddove quest'ultimo abbia immesso i dati e/o documenti, quando potrebbe esserci in concreto il consenso e che significato assumerebbe la norma? Si tratterebbe di una disposizione sostanzialmente priva di efficacia, specie se rapportata alle effettive ragioni (contrasto al terrorismo internazionale) per la quale la stessa è stata introdotta».

[131] Cass., Sez. I, 13 ottobre 2023, n. 6364.

[132] Cass., Sez. VI, 2 novembre 2023, n. 44154.

prima fra tutte la volatilità che impone particolari cautele al momento sia dell'estrazione del dato sia della successiva custodia.

L'art. 234-*bis* c.p.p., inoltre, trascura l'aspetto dell'integrità del dato, non essendovi garanzie che il materiale appreso sia effettivamente inalterato e rispondente a quello custodito nei *server* degli *internet service provider*.

Peraltro, dal momento che la prova è fornita da un soggetto terzo, "preconfezionata" e non direttamente appresa dalle autorità a ciò deputate, nei cui confronti potrebbero eventualmente attivarsi azioni disciplinari, mancano gli strumenti per richiedere le dovute garanzie in via preventiva o per attivare dei rimedi *ex post*. Questo determina una sorta di *probatio diabolica* a carico della difesa, non potendosi dimostrare il mancato utilizzo delle garanzie idonee considerato che, in assenza di specifiche sanzioni, difficilmente il *provider* rivelerà l'algoritmo utilizzato per la decrittazione delle informazioni[133]. Vieppiù, è necessario esaminare la nozione di documento informatico prevista dal nostro ordinamento per valutarne l'adattabilità alla prova digitale.

L'art. 491-*bis* c.p., relativo ai documenti informatici, al co. 2 qualificava come tale «qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». Il disposto è stato poi abrogato dall'art. 3 co. 1 b), della l. 48/2008; sicché, ai fini definitori si fa oggi riferimento alla disciplina amministrativa.

Ai sensi dell'art. 1 co. 1 lett. p) del d. lgs. 7 marzo 2005 n. 82 (c.d. Codice dell'amministrazione digitale)[134] per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti[135].

L'art. 20 del medesimo decreto, al co. 1-*bis* stabilisce che: «il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, […] con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore».

Sembra difficile, alla luce di quanto detto, il raccordo tra questa nozione e l'ampia casistica delle prove digitali che, seppur idonee a rappresentare fatti e atti, tuttavia non solo

---

[133] PITTIRUTI M., *L'apprensione all'estero della prova digitale*, cit., p. 205 ss.
[134] D. lgs. 7 marzo 2005 n. 82 (c.d. Codice dell'amministrazione digitale) in G.U. 16 maggio 2005 n. 112, S.O. n. 93.
[135] Cfr. COLAROCCO V., *Dal documento informatico alla pagina web*, in COLAROCCO V., GROTTO T., VACIAGO G. (a cura di), *La prova digitale*, Giuffrè Francis Lefebvre, 2020.

potrebbero non essere state create da un individuo (è il caso delle prove c.d. *machine-created*, ossia tutti i metadati autonomamente creati dai dispositivi), ma in taluni casi, ancorché create da un utente, potrebbero difettare della firma elettronica o di qualunque altra modalità che ne permetta la riconducibilità, in maniera inequivoca, a un soggetto.

Altro istituto al quale si è fatto riferimento è l'ispezione. A seguito della modifica dell'art. 244 c.p.p., operata dalla l. 48/2008, si è previsto che, anche in relazione a sistemi informatici o telematici, l'autorità giudiziaria possa disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

L'ispezione di un dispositivo tecnologico presenta caratteristiche proprie e specifiche, dal momento che le informazioni rilevanti per le indagini non sono direttamente visibili e facilmente identificabili[136].

In tal caso risulta necessario utilizzare appositi *software* di ricerca per identificare i *file* utili o, qualora non sia possibile rinvenirli immediatamente, si renderà inevitabile realizzare una copia di tutti i dati per effettuare, in un secondo momento, una ricerca basata su parole chiave. L'analisi attraverso *software* e parole chiave potrebbe, tuttavia, non portare all'identificazione dei dati utili, rendendo necessaria un'analisi approfondita di tutti i *file*.

Questa ricerca incide sul principio di proporzionalità, oltre che sul diritto alla *privacy* dei soggetti coinvolti: a tale riguardo, occorrerebbe stabilire una precisa maniera di procedere, specie in relazione all'apprensione di dati che nulla hanno a vedere con il delitto per cui si procede.

Tra i mezzi di ricerca della prova utilizzati per la prova digitale, figura anche l'istituto della perquisizione: quella perquisizione informatica, *ex* 247 co. 1-*bis* c.p.p., è stata anch'essa introdotta dalla l. 48/2008, in quella prospettiva di adattamento degli istituti già esistenti a nuove modalità operative e più affini alle prove digitali[137].

In particolare, la perquisizione informatica[138] è disposta quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al

---

[136] V. CUOMO L., GIORDANO L., *Informatica e processo penale*, in *Proc.Pen. Giust*, 2017, 4, p. 717; GIORDANO L., *L'intercettazione delle* e-mail *(già) ricevute o inviate e l'acquisizione di quelle parcheggiate nella cartella "bozze"*, in *www.ilpenalista.it*, 14 novembre 2016; PADUA G., *L'accesso alla casella* e-mail *e l'acquisizione dei contenuti: un delicato inquadramento normativo*, in *Proc. Pen. Giust.*, 2018, 3, p. 596.

[137] Sulle perquisizioni *online* effettuate tramite captatore e sull'impropria riconduzione alla fattispecie delle perquisizioni vedasi GRIFFO M., *Perquisizione informatica…e dintorni*, in *Giurisprudenza Penale Web*, 2019, 5; IOVENE F., *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. Pen. Cont.*, 2014, p. 329.

[138] Per approfondimenti CUOMO L., GIORDANO L., *Informatica e processo penale*, cit., p. 717; FILIPPI L.; *Il cavallo di Troia e l'ispe-perqui-intercettazione*, cit; GRIFFO M., *Perquisizione informatica…e dintorni*, cit., p. 5.

reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza. La norma, inoltre, prevede l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

I dati digitali possono, inoltre, essere ottenuti attraverso la richiesta di consegna, in una logica ispirata al rispetto del principio di proporzionalità. E infatti, ai sensi dell'art. 248 c.p.p. l'autorità giudiziaria, prima di procedere alla perquisizione, può chiedere la consegna di una cosa determinata. Se ciò avviene, non si procederà alla perquisizione, a meno che non si ritenga utile per la completezza delle indagini. Inoltre, l'autorità giudiziaria e gli ufficiali di polizia giudiziaria possono esaminare presso banche, atti, documenti, corrispondenza, dati, informazioni e programmi informatici.

In merito a questo mezzo di ricerca della prova, si è posto l'interrogativo se potesse essere ricondotto alla perquisizione ordinaria o se invece integrasse una tipologia autonoma di perquisizione. A favore della seconda soluzione, si è osservato che «la parziale diversità e modulazione dei diritti fondamentali lesi, la diversità dei presupposti che la legittimano, le peculiari caratteristiche dell'oggetto su cui insiste, nonché le specifiche modalità con cui deve essere effettuata inducono a ritenere che la perquisizione di un sistema informatico o telematico configuri una nuova tipologia di perquisizione»[139].

Specie in considerazione del fatto che, mentre nella perquisizione ordinaria, questa precede il sequestro, nel caso di perquisizione informatica, l'ordine è sovente invertito e solo dopo il sequestro e la copia dei dati si procede all'attività di ricerca[140]. Infatti, per svolgere le perquisizioni salvaguardando l'integrità del dato, la *digital forensics* prevede *in primis*

---

[139] SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 212.

[140] Vedasi anche TORRE M., *Indagini informatiche e principio di proporzionalità*, in *Proc. Pen. Giust*, 2019, 6, p. 1437: «La seconda caratteristica consiste nel fatto che, al contrario di ciò che avviene normalmente nel corso di indagini tradizionali, allo stato la tecnica non consiglia di limitare il sequestro informatico a specifici dati o a specifiche informazioni. In ambito di *digital evidence*, infatti, onde evitare l'alterazione degli elementi da acquisire, la perquisizione deve necessariamente seguire l'apprensione (sequestro) del bene e non, viceversa, costituire attività prodromica al successivo eventuale sequestro. Si tratta dell'unico caso in cui la perquisizione segue il sequestro (o meglio, la copia) anziché precederlo, ed il motivo è presto detto: la ricerca si traduce inevitabilmente in un'attività in grado di alterare il dato originale, sicché il suo espletamento, «ove possibile», deve avere ad oggetto la copia forense e mai l'originale, pena la violazione degli art. 247 e 352 c.p.p., così come modificati dalla legge n. 48 del 200. Questo modo di procedere, evidentemente, espone a maggior rischio la riservatezza dei soggetti interessati dal provvedimento: oggi, clonare i dati di uno *smartphone* significa accedere ai segreti più intimi di una persona. Se a ciò si aggiunge la tendenza di una certa giurisprudenza a considerare il sequestro probatorio di documenti informatici diverso concettualmente dalla propedeutica attività di estrazione di copia dei dati medesimi, con conseguente non "riesaminabilità" del provvedimento in ragione del principio di tassatività delle impugnazioni di cui all'art. 568 c.p.p., il giudizio da esprimere sul rispetto del principio di proporzionalità non può che essere negativo. Le conseguenze di queste prime due caratteristiche sono evidenti: le indagini informatiche sono sempre lesive della riservatezza delle persone coinvolte e della sicurezza dei dati contenuti nei sistemi informatici; inoltre, alto è il rischio che tali attività si trasformino in attività esplorative volte alla ricerca delle notizie di reato (c.d. indagini pro-attive: indagini ad alto contenuto tecnologico che si pongono a metà strada tra la prevenzione e la repressione)».

l'acquisizione dell'intero dispositivo e, successivamente, la creazione di una copia clone su cui poi effettuare l'attività di ricerca.

Sul punto, la dottrina[141] ha evidenziato come la linea di confine tra l'ispezione e la perquisizione, specie nel caso delle indagini digitali, non sia netta. E infatti, se la principale distinzione è da individuarsi nell'attività di mera osservazione dell'ispezione e, d'altro canto, nell'attività di ricerca della perquisizione, nel caso di un sistema informatico sarà difficile svolgere la prima senza fare una ricerca tra i file presenti, a meno che non si esaminino i soli componenti fisici dei dispositivi.

In giurisprudenza[142] si fa, inoltre, frequentemente riferimento alla normativa sui sequestri. Ai sensi degli artt. 253 e 254 co. 1 c.p.p., è previsto, presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni, il sequestro del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti e di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza anche se inoltrati per via telematica, che siano stati spediti dall'imputato o a questo diretti, o che siano relativi al reato[143].

Uno degli aspetti più controversi della disciplina riguarda la portata del sequestro: se, cioè, si debba sequestrare unicamente il dato di interesse investigativo (il singolo *file*) o l'intero dispositivo o *hard disk*, per procedere a una successiva analisi. Se, per ragioni di celerità, la seconda opzione appare preferibile, tuttavia, non sempre l'intero dispositivo costituisce corpo del reato o cosa pertinente al reato, con il rischio di addivenire a sequestri del tutto sproporzionati.

Per evitare "abusi", un ruolo fondamentale assume– come sottolineato dalla Corte di Cassazione[144] – la motivazione del decreto nella quale vanno spiegate le ragioni che conducono all'indiscriminata acquisizione dell'intero contenuto di un sistema informatico, pena l'illegittimità della misura.

---

[141] SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit. p. 206. *Ibidem*, p. 208: « Tuttavia, se qualunque attività sui dati o di controllo del contenuto di un dispositivo informatico sembra integrare più un'attività di ricerca che una mera attività di osservazione o descrizione, riesce difficile concepire una ispezione prettamente informatica, se non nei limiti in cui sia funzionale ad un'osservazione esterna, che consenta di individuare ad esempio la marca del sistema informatico o la presenza di sistemi di connessione, quali rete adsl o rete *wireless*, nonché periferiche collegate o scollegate. In questo caso, però, a ben vedere, non si tratterebbe propriamente di un'attività informatica, ma di un'attività di osservazione tout court. Per questo motivo, ragionare in termini di ispezione informatica non appare convincente, dato che si rischia di confondere l'attività con l'oggetto della medesima punto sarebbe un po' come definire musicale un'ispezione solo perché ad oggetto uno strumento musicale».

[142] Tra le tante Cass., Sez. VI, 24 ottobre 2019, n. 43556 con nota di NULLO L., *Sequestro probatorio di materiale documentativo e principi di adeguatezza e proporzionalità*, in *Proc. Pen. Giust*, 2020, 3, p. 663. Vedasi anche PITTIRUTI M., *Dalla Corte di cassazione un* vademecum *sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali* omnibus, in *www.sistemapenale.it*, 14 gennaio 2021.

[143] V. CUOMO L., GIORDANO L., *Informatica e processo penale*, cit., p. 719.

[144] Cass, Sez. VI, 2 dicembre 2020, n. 34265.

I giudici di cassazione hanno altresì riconosciuto[145] che, relativamente all'acquisizione della prova, «l'autorità giudiziaria, al fine di esaminare un'ampia massa di dati i cui contenuti sono in astratto potenzialmente rilevanti per le indagini, può disporre un sequestro dai contenuti molto estesi, provvedendo, tuttavia, nel rispetto del principio di proporzionalità e adeguatezza, alla immediata restituzione delle cose sottoposte a vincolo non appena sia decorso il tempo ragionevolmente necessario per gli accertamenti e, in caso di mancata tempestiva restituzione, l'interessato può presentare la relativa istanza e far valere le proprie ragioni, se necessario, anche mediante i rimedi impugnatori offerti dal sistema. […] Ne consegue che il Pubblico Ministero: a) non può trattenere la c.d. copia integrale dei dati appresi se non per il tempo strettamente necessario alla loro selezione; b) è tenuto a predisporre una adeguata organizzazione per compiere la selezione in questione nel tempo più breve possibile, soprattutto nel caso in cui i dati siano stati sequestrati a persone estranee al reato per cui si procede; c) compiute le operazioni di selezione, la c.d. copia – integrale deve essere restituita agli aventi diritto».

Viene in rilievo anche il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. L'art. 254-*bis* c.p.p., inserito dalla l. 48/2008, prevede il sequestro dei dati detenuti da fornitori di servizi informatici, telematici o di telecomunicazioni, compresi quelli di traffico o di ubicazione[146]. L'autorità giudiziaria può stabilire che l'acquisizione avvenga mediante copia su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.

Tenuto conto di questo, in data 19 luglio 2023 è stato presentato il d.d.l. 806[147], finalizzato a introdurre un nuovo art. 254 *ter* c.p.p. relativo al sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali.

Il legislatore si pone come necessario obiettivo la regolamentazione più specifica dell'istituto del sequestro, in relazione ai suddetti dispositivi, per garantire una tutela adeguata e il rispetto dei principi di proporzionalità, adeguatezza e gradualità. È infatti previsto che si proceda al sequestro a seguito di un decreto motivato del giudice, su richiesta

---

[145] V. anche Cass., Sez. II, 15 dicembre 2023, n. 50009.

[146] Vedasi CUOMO L., GIORDANO L., *Informatica e processo penale*, cit., p. 719: «È stato ritenuto legittimo il sequestro di sistemi informatici e telematici costituenti corpo del reato o cosa pertinente al reato con l'esame dei quali può essere dimostrato il fatto criminoso, comprese le modalità di preparazione ed esecuzione, di apparecchi del tipo "totem *internet*" per giochi d'azzardo a distanza , di dispositivi destinati a "*consolle*" per videogiochi illecitamente duplicati o scaricati abusivamente da inter net, di tablet del tipo *Ipad* o di elaboratori utilizzabili per la commissione di violazioni finanziarie, nonché di pennette USB necessarie alla prova della falsificazione di documentazione fiscale».

[147] Ddl 806, di iniziativa dei Senatori Zanetti e Bongiorno, https://www.giurisprudenzapenale.com/wp-content/uploads/2023/07/ddl-806__427387.pdf. Tra i primi commenti v. commento di MORCELLA M.T., *Ancora questioni in tema di sequestro di* smartphone, cit.; LA REGINA K., *Il sequestro dei dispositivi di archiviazione digitale*, in *www.penaledp.it*, 12 ottobre 2023.

del pubblico ministero, quando sia necessario per la prosecuzione delle indagini, nel rispetto del principio di proporzionalità. Il pubblico ministero, una volta trasmesso il decreto, potrà procedere all'esecuzione personalmente o delegando gli ufficiali di polizia giudiziaria. Nei casi di urgenza, il sequestro potrà essere disposto dall'organo di accusa con apposito decreto motivato o dagli ufficiali di polizia giudiziaria, che gli trasmetteranno il verbale entro 48 ore. Il pubblico ministero chiederà successivamente al giudice la convalida e l'emissione del decreto entro i termini previsti – 48 ore dall'esecuzione, se disposto dal pubblico ministero, o dalla trasmissione del verbale, se disposto dalla polizia giudiziaria – pena l'inefficacia dell'atto. L'esecuzione si svolgerà mediante la duplicazione dei dati su un idoneo supporto informatico, in modo da assicurare integrità, conformità e immodificabilità dei dati stessi. Effettuata la copia, il dispositivo andrà restituito all'avente diritto. Dopo l'analisi del duplicato, il pubblico ministero procederà, con decreto motivato, al sequestro dei dati, delle informazioni e dei programmi strettamente pertinenti al reato, nel rispetto dei criteri di necessità e proporzione. Nel caso di dati inerenti a comunicazioni, conversazioni o corrispondenza informativa, sarà necessario un decreto motivato di autorizzazione del giudice.

Punto di forza del d.d.l. è proprio lo svolgimento delle operazioni di selezione in contraddittorio, da svolgersi prima dell'analisi dei dati. A tal fine, entro 5 giorni dal deposito del verbale di sequestro, il pubblico ministero dovrà avvisare la persona sottoposta alle indagini, la persona alla quale la cosa è stata sequestrata o alla quale la cosa dovrebbe essere restituita, la persona offesa dal reato e i relativi difensori del giorno, dell'ora e del luogo fissato per l'affidamento dell'incarico da espletare ai sensi dell'articolo 360 c.p.p. e della facoltà di nominare consulenti tecnici. I difensori e i consulenti nominati avranno poi facoltà di partecipare al conferimento dell'incarico e alle operazioni di selezione ed estrazione dei dati.

L'acquisizione dei dati traffico è disciplinata dall'articolo 132 co. 1 del d. lgs 196/2003 (c.d. *Codice privacy*)[148].

In proposito, è legittimo domandarsi se si realizzi una qualche sovrapposizione tra la disciplina prevista da tale articolo e quella *ex* art. 254-*bis* c.p.p. Entrambe le norme, infatti, hanno ad oggetto l'acquisizione di elementi digitali presso i *provider*. Tuttavia, sembra che l'art. 254-*bis* c.p.p. sia volto unicamente a chiarire le modalità di sequestro presso i fornitori di servizi informatici, telematici e di telecomunicazioni. Infatti, la norma sarebbe finalizzata a bilanciare le finalità investigative con l'esigenza dei fornitori di servizi di non essere privati

[148] D. lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, in G.U. n.174 del 29/07/2003 - Suppl. Ordinario n. 123.

a lungo di dati ed elementi utili per il proseguimento della loro attività, prevedendo la predisposizione di una copia più che la sottrazione della strumentazione informatica e la perdita di dati essenziali per la prosecuzione del servizio.

La scelta di effettuare una copia dei dati utili sembra trovare una *ratio* nell'esigenza di non causare un *vulnus* sproporzionato ai fornitori di servizi e, al contempo, di garantire la verifica della genuinità della prova.

Inoltre, l'art. 254 c.p.p. fa riferimento ai fornitori di servizi informatici telematici e di telecomunicazioni, formula più ampia e non sovrapponibile a quella dei fornitori di servizi di telecomunicazione elettronica ai sensi dell'art. 132 *Codice privacy*.

In tal senso, nella nozione di fornitori di servizi informatici e telematici rientrerebbero non solo i soggetti che forniscono servizi consistenti nella trasmissione di segnali su rete elettroniche, ma anche quelli che forniscono tali servizi all'interno di una diversa attività d'impresa.

La possibilità di esaminare dati informatici e programmi informatici è stata introdotta dalla l. n. 48/2008, senza tuttavia che sia stato inserito un esplicito riferimento alla richiesta di consegna dei dati. Rispetto a quest'ultimo tema, vanno evidenziati taluni profili di criticità, poiché i soggetti che consegnano i dati sono soggetti privati e non anche autorità investigative. Questi, pertanto, potrebbero fornire dati che presentano errori; per evitare questo rischio, sarebbe opportuno che venissero consegnati in formato digitale, seguendo appositi *standard*, in luogo del supporto cartaceo, che non consente di effettuare un controllo sulle modifiche o sullo storico del dato.

Ultimo istituto da considerare è il dovere di esibizione: l'art. 256 c.p.p. disciplina, infatti, il dovere di consegna per i soggetti che possono eccepire il segreto professionale o di ufficio *ex* art. 200 e 201 c.p.p. In particolare, si pone in capo a tali soggetti, su richiesta dell'autorità giudiziaria, l'obbligo di esibire atti e documenti, dati, informazioni e programmi informatici, in originale o mediante copia su adeguato supporto. Nonostante il testo normativo faccia espresso riferimento ai soggetti menzionati agli artt. 200 e 201 c.p.p., la Corte Costituzionale [149]ha da tempo chiarito che tale disciplina si applica anche agli enti gestori del servizio di telefonia.

L'analisi sin qui tratteggiata, anche alla luce delle incertezze giurisprudenziali, evidenzia come gli strumenti processuali "tradizionali" – a tratti rivisitati – ai quali si fa riferimento per acquisire la prova digitale, non rispondano pienamente alle caratteristiche

[149] Corte Cost., 26 febbraio 1993, n. 81: «l'art. 256 c.p.p., il quale, nel regolare in via generale l'acquisizione di documenti coperti dal segreto professionale (o dal segreto di Stato), pone una disciplina applicabile anche all'ente gestore del servizio pubblico della telefonia».

proprie di questa tipologia di prova, contrassegnata dall'immaterialità e dalla volatilità. Come detto, il rischio – fino a quando non si interverrà con una specifica disciplina – è quello di incidere sull'affidabilità della prova medesima e sulla sua efficacia probatoria.

2.2. Data retention *e acquisizione dei dati di traffico tra normativa europea e legislazione interna*

Nel nostro sistema, la disciplina in tema di *data retention* è collocata all'interno del Codice *privacy* e*,* nello specifico, all'art. 132, norma che, dalla sua introduzione a oggi, è stata oggetto di varie interpolazioni dettate dalla necessità di adeguare il sistema agli impulsi di derivazione europea[150].

Nello specifico, tale articolo, inserito nel corpo del d. lgs. n. 196/2003[151], c.d. Codice *privacy,* prevedeva *ab origine* la conservazione di specifiche tipologie di dati da parte del fornitore del servizio per 24 mesi. Allo scadere del termine, i dati sarebbero poi stati conservati per ulteriori 24 mesi per finalità di accertamento e repressione dei delitti più gravi *ex* art. 407 co. 2 lett. a) c.p.p. e per i reati in danno di sistemi informatici e telematici.

Su questa disciplina si è innestato il d.l. 24 dicembre 2003 n. 354[152] che, ai fini dell'acquisizione probatoria, ha previsto il decreto motivato del giudice, su richiesta del pubblico ministero, dell'indagato o dell'imputato, della persona offesa o delle altre parti private. La norma è stata poi nuovamente modificata dal d.l. 27 luglio 2005, n. 144, convertito nella l. 31 luglio 2005 n. 155 (c.d. Decreto Pisanu)[153], che ha riconosciuto al pubblico ministero il potere autonomo di acquisizione dei dati presso il fornitore del servizio, anche su istanza delle altre parti[154].

Sul versante dell'accesso ai dati, è da segnalare che al difensore dell'imputato e della persona sottoposta alle indagini è stata, invece, accordata la facoltà di richiedere, direttamente al *provider*, i dati relativi alle sole utenze intestate al proprio assistito con le

---

[150] Per una cronistoria v. FILIPPI L., *Riservatezza e* data retention*: una storia infinita*, in *www.penaledp.it*, 23 giugno 2022.
[151] D. lgs.30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, in G.U. Serie Generale n.174 del 29 luglio 2003 - Suppl. Ordinario n. 123.
[152] D. l. 24 dicembre 2003, n. 354 recante "*Disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché' interventi per l'amministrazione della giustizia",* in G.U. n. 48 del 27 febbraio2 004.
[153] D.l. 27 luglio 2005, n. 144 recante "*Misure urgenti per il contrasto del terrorismo internazionale*", in G.U. n. 173 del 27 maggio 2005.
[154] Per una precisa ricostruzione cfr. ATERNO S., CAJANI F., *L'acquisizione dei dati del traffico*, in ATERNO S., CAJANI F., COSTABILE G., CURTOTTI D. (a cura di), Cyber forensics *e indagini digitali*, cit..

modalità di cui all'art. 391-*quater* c.p.p[155]. L'articolo è stato poi modificato dal d. lgs 10 agosto 2018, n. 101[156], che ha permesso l'ampliamento dei termini di *data retention* per finalità di contrasto al terrorismo e, come diremo, dal d.l. 30 settembre 2021, n. 132[157].

La definizione di dati di traffico è fornita dall'art. 1 co. 1 b) del d.lgs. 30 maggio 2008 n. 109[158], e ricalca quella precedentemente espressa dall'art. 4 co. 2 h) del d. lgs. n. 196/2003. Con tale nozione si intende qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione, ivi compresi i dati necessari per identificare l'abbonato o l'utente[159].

Tra i dati necessari per identificare l'utente, viene annoverato l'indirizzo IP univocamente assegnato quale indirizzo di protocollo (IP) che consente appunto l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica[160].

Si ricomprendono all'interno del concetto di traffico telefonico, *ex* art. 1 co. 1 d) del richiamato d.lgs., le chiamate telefoniche, incluse quelle vocali, di messaggeria vocale, in conferenza e quelle basate sulla trasmissione dati, purché fornite da un gestore di telefonia, i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata, la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve, servizi mediali avanzati e servizi multimediali.

Il riferimento alle chiamate basate sulla trasmissione dei dati, intendendosi quali dati informatici e trasmissioni telematiche, permetterebbe di includere nella nozione di traffico telefonico anche chiamate relative a sistemi quali *Voip* e *Skype*, nonché a sms[161].

Come per i dati di traffico, la definizione di dati relativi all'ubicazione, collocata alla lettera c) del medesimo articolo, ricalca quella dell'art. 4 co. 2 l) e vi ricomprende ogni dato

---

[155] Cftr. MALACARNE A., TESSITORE G., *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di Giustizia: ancora inadeguata la disciplina interna*?, in *Arch. Pen.*, 2022, 3.

[156] Tale modifica è stata introdotta dall'art. 11 del d.lgs 10 agosto 2018 n. 101 recante "*disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 abrogala direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*". In particolare, attraverso l'introduzione del nuovo co. 5-*bis* ai sensi del quale «è fatta salva la disciplina di cui all'articolo 24 della legge 20 novembre 2017, n. 167».

[157] D. l. 30 settembre 2021, n. 132 recante "*Misure urgenti in materia di giustizia e di difesa, nonché'proroghe in tema di referendum, assegno temporaneo e IRAP*", in G.U. Serie Generale m. 243 del 30 settembre 2021.

[158] D. lgs. 30 maggio 2008, n. 109, *Attuazione della direttiva 2006/24/CE riguardante la conservazione dei 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,* in G.U. Serie Generale n.141 del 18 giugno 2008.

[159] VENTURINI S., *Sequestro probatorio e fornitori di servizi telematici*, in LUPARIA L., Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè Editore, 2012, p. 116.

[160] Art. 1 co. 1 lett. g), d. lgs. 109/2008.

[161] ATERNO S., CAJANI F., *L'acquisizione dei dati del traffico*, in ATERNO S., CAJANI F., COSTABILE G., CURTOTTI D. (a cura di), Cyber forensics *e indagini digitali*, cit..

trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico, ivi compresi quelli relativi alla cella da cui una chiamata di telefonia mobile ha origine o nella quale si conclude.

Fermo restando il generico divieto di *data retention* predisposto dall'articolo 123 co. 2 del Codice *privacy*, l'art. 132 del medesimo testo prevede, a carico del fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica, un obbligo di conservazione limitato alle finalità di accertamento e repressione dei reati.

Nello specifico è prevista la conservazione di:

- dati relativi al traffico telefonico per 24 mesi dalla data della comunicazione;
- dati relativi al traffico telematico per 12 mesi dalla data della comunicazione;
- dati relativi alle chiamate senza risposta per 30 giorni.

Ci si domanda quale possa essere la *ratio* per cui il legislatore ha previsto tempi di conservazione differenti a seconda del tipo di traffico, specie in considerazione del fatto che l'esperienza ci restituisce una riduzione del traffico telefonico a fronte di un consistente aumento di quello telematico[162].

I termini di conservazione sono stati poi ulteriormente prolungati in osservanza di quanto disposto dall'art. 24 della legge 20 novembre 2017, n. 167[163] (cd. legge europea).

Si ha, dunque, un'estensione fino a 72 mesi per i reati di terrorismo *ex* art. 51 co. 3-*quater* c.p.p. e per quelli di cui all'art. 407 co. 2 a) c.p.p., in relazione a tutte le tipologie di dati sopra citati.

La principale criticità è data dal fatto che il fornitore, non avendo certezza sul se e quando l'autorità giudiziaria farà una richiesta di accesso ai dati e in relazione a quale tipologia di reato, conserverà i dati per il termine massimo di 72 mesi, salvo poi negare l'accesso qualora il delitto su cui si basa la richiesta non rientri tra quelli per i quali è prevista l'estensione. In tale scenario, è concreto il rischio di una sorta di "normalizzazione" della

[163] Legge 20 novembre 2017, n. 167, *Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017,* in G.U. Serie Generale n.277 del 27/11/2017.

conservazione generalizzata, tenuto conto che i fornitori di servizi[164] non possono, ovviamente, conoscere a priori il livello di gravità dei reati perseguiti[165].

2.2.1. Tabulati telefonici e spinte riformatrici

Sulla disciplina in tema di tabulati telefonici *post* "decreto Pisanu" è infine intervenuto il Governo, con il d.l. 30 settembre 2021, n. 132, sull'onda di alcune pronunce della Corte di Giustizia[166].

Il punto di partenza dell'*iter* giurisprudenziale è rappresentato dalla sentenza *Digital Rights Ireland* con la quale è stata dichiarata invalida la direttiva 2006/24/CE (cd. direttiva Frattini)[167] che determinava la conservazione indiscriminata dei dati in violazione del principio di proporzionalità.

Secondo la Corte: «da quanto precede deriva che la direttiva 2006/24 non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. Pertanto, è giocoforza constatare che tale direttiva comporta un'ingerenza nei suddetti diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario».

---

[164] I fornitori di servizi informatici e telematici su cui ricade l'obbligo di conservazione sono tutti quei soggetti che, pur non avendo come attività d'impresa quella di fornire reti o servizi di comunicazione elettronica, se ne avvalgono per l'impiego della loro attività.
All'interno di questa categoria possono essere inclusi istituti bancati o compagnie che offrono l'accesso a internet per usufruire dei loro servizi. Saranno, pertanto, considerati locatori dello spazio in cui un privato memorizza i propri dati e informazioni e, pertanto, detentori di dati relativi all'indagato e a terzi, che siano rilevanti per le indagini.
Si distinguono tre figure di prestatori di servizi:
- meri trasmettitori di informazioni provenienti dal destinatario del servizio (*mere conduit*);
- prestatori che trasmettono le informazioni ed effettuano una temporanea memorizzazione (*caching*),
- prestatori che memorizzano i contenuti provenienti dagli utenti(*hosting*).

V. BELLUTA H., *Oltre i confini del sequestro preventivo: vincoli "reali" e fornitori di servizi in rete,* p. 103 in LUPARIA L., Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè Editore, 2012.

[165] NADDEO G., *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "*data retention *saga" dinanzi alla Corte di Giustizia, in Freedom Security & Justice: european legal studies*, vol. 2, 2022, p. 214.

[166] Cfr. CGUE, 2 marzo 2021, C-746/18, *H. K. v Prokuratuur* con commento di ANDOLINA E., *La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di data retention*?, in *Proc. Pen. Giust.*, 2021, 5, p. 1204.

[167] 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, in G.U. L. 105 del 13 aprile 2006.

A questa ha fatto seguito la sentenza *Tele2*[168].

Nell'occasione, la Corte era stata chiamata a pronunciarsi sull'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58/CE[169] alla luce degli artt. 7 e 8 della Carta europea dei diritti fondamentali, relativi al rispetto della vita privata e familiare e alla protezione dei dati di carattere personale.

Tale sentenza ha avuto il merito di avere specificato ulteriormente la portata del principio di proporzionalità[170] in ambito di *data retention.*

Nello specifico, sono stati affermati alcuni principi di rilievo: *in primis* che la normativa comunitaria osta alla conservazione generalizzata e indifferenziata dei dati di traffico e relativi all'ubicazione, ma non alla conservazione mirata; che tale conservazione va, tuttavia, limitata alla lotta contro i reati più gravi[171] e allo stretto necessario. La Corte ha, inoltre, specificato che per circoscrivere l'accesso allo "stretto necessario", la normativa nazionale deve identificare dei criteri oggettivi per individuare le condizioni che legittimano l'accesso ai dati e l'accesso, salvo casi di urgenza debitamente giustificati, deve essere subordinato a un controllo preventivo effettuato da un giudice o da un'entità amministrativa indipendente.

Ebbene, la normativa italiana legittima, al pari della direttiva sopra citata, un fenomeno di conservazione indiscriminata e generalizzata dei dati e, per i reati di terrorismo, il termine di conservazione è stato addirittura dilatato fino ad assumere il primato del termine più lungo nel contesto europeo.

Un profilo di rilievo attiene al soggetto legittimato alla richiesta dei dati e, nello specifico, al pubblico ministero. Il tema è stato affrontato nella sentenza *H.K. / Prokuratuur* del 2021, con la quale la Corte di Giustizia è stata chiamata a rispondere al quesito se il pubblico ministero (nel caso di specie estone), che dirigeva un procedimento istruttorio

---

[168] CGUE, Grande Camera, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige* AB, con nota di POLLICINO O., BASSINI M., *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. Pen. Cont.,* 9 gennaio 2017.

[169] 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche) in G.U. L. 201 del 31 luglio 2002.

[170] Sul punto la Corte, § 94: «A questo proposito, occorre ricordare che, ai sensi dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti da quest'ultima devono essere previste dalla legge e rispettare il loro contenuto essenziale. Nel rispetto del principio di proporzionalità, possono essere apportate delle limitazioni all'esercizio dei diritti e delle libertà summenzionati soltanto qualora esse siano necessarie e rispondano effettivamente a obiettivi di interesse generale riconosciuti dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

[171] In proposito la CGUE, con sentenza del 2 ottobre 2018, C207/16, cosiddetta sentenza *Ministerio Fiscal*, ha poi operato un passo indietro, riconoscendo la possibilità della *data retention* anche per i reati non gravi, qualora l'ingerenza nella vita privata del singolo non fosse particolarmente penetrante.

penale, esercitando eventualmente l'azione penale, fosse competente ad autorizzare l'accesso ai dati di traffico e relativi all'ubicazione.

A parere della Corte, per soddisfare il requisito di indipendenza sancito dalla sentenza *Tele2,* l'autorità che esercita il controllo preventivo sull'accesso ai dati deve assumere la qualità di terzo rispetto a quella che formula la richiesta[172]. Solo in presenza di una situazione di neutralità può esservi un controllo obiettivo e imparziale; «in particolare, in ambito penale, il requisito di indipendenza implica, […] che l'autorità incaricata di tale controllo preventivo, da un lato, non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale».

In tal senso, non può considerarsi indipendente il pubblico ministero che dirige le indagini ed esercita l'azione penale. Inoltre, la circostanza che debba considerare gli elementi a carico e discarico, garantire la legittimità del procedimento istruttorio e agire secondo la legge, non gli conferisce lo *status* di soggetto terzo rispetto alle parti. Pertanto, a parere della Corte, il diritto europeo «osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale».

Pur a seguito della menzionata pronuncia, la giurisprudenza nazionale ha continuato a escludere un contrasto tra la normativa europea e quella italiana, ritenendo che i principi in quella sede affermati non potessero estendersi all'ordinamento italiano, del tutto diverso da quello estone[173].

---

[172] PALLADINI V., Data retention *e* privacy *in rete: verso una regolazione conforme al diritto UE?* , in *Riv. Italiana di Informatica e diritto,* n. 1, 2022; RESTA F., *Conservazione dei dati e diritto alla riservatezza. La Corte di Giustizia interviene sulla* data retention*. I riflessi sulla disciplina interna*, in www.giustiziainsieme.it, 6 marzo 2021.

[173] In tal senso Corte di Assise di Napoli, I Sez. penale, 16 giugno 2021: «Il pm, per il suo *status* ordinamentale è organo facente parte dell'Autorità Giudiziaria e, come tale, destinatario dei doveri di imparzialità e di rispetto della legge ed anche delle guarentigie costituzionali poste a tutela della piena autonomia della funzione […] il pm è chiamato ad acquisire non solo le prove di accusa, ma anche quelle a favore dell'indagato, essendo in suo potere richiedere l'archiviazione; la sua posizione non può, pertanto, essere assimilata a quella del corrispondente organo estone, che è autorità soggetta alla sfera di competenza del Ministro della Giustizia che partecipa alla pianificazione delle misure necessarie per la lotta e l'accertamento dei reati». Cfr. anche Trib. Milano, VII Sez. penale, ord. 22 aprile 2021, Pres. Malatesta: «Ritiene, poi, il Collegio che non possa operarsi - quantomeno alla luce delle risultanze della pronuncia richiamata - alcuna automatica assimilazione tra la figura del Pubblico Ministero estone e la corrispondente figura prevista dall'ordinamento nazionale e che neppure possano essere validamente e fondatamente trasposte, rispetto all'ordinamento italiano, le censure mosse dalla Corte di Giustizia alla disciplina estone in tema di c.d. *data retention* e acquisizione dei tabulati telefonici per finalità di giustizia. Procedendo per gradi, si evidenzia che se è vero che - come nell' ordinamento estone- il pm italiano è titolare del potere di accusa e parte del processo penale, va anche rilevato che, a dispetto di quanto si comprende valere nell'ordinamento estone, il pm. nell'ordinamento nazionale è da ricomprendersi nel concetto di Autorità Giudiziaria ed è chiamato non solo a valutare gli elementi di prova a carico e a discarico

In senso contrario, però, alcuni GIP presso il Tribunale di Roma, escludendo il carattere della terzietà in capo al pubblico ministero, hanno ritenuto che i principi pronunciati dalla Corte di Giustizia fossero applicabili anche al nostro ordinamento. A fronte di una situazione di incertezza giuridica, il Tribunale di Rieti ha sollevato una questione pregiudiziale[174] domandando se il pubblico ministero italiano potesse procedere autonomamente all'acquisizione diretta dei dati di traffico o se, essendo assimilabile al pubblico ministero estone, fosse necessario il controllo del giudice[175].

Nelle more della decisione della Corte di Giustizia, il Governo è intervenuto con il d.l. 30 settembre 2021 n. 132[176], che ha modificato l'art. 132 codice *privacy* stabilendo che i dati soggetti alla data *retention* possano essere acquisiti con decreto motivato del giudice su richiesta del pubblico ministero o su istanza del difensore dell'imputato dell'indagato, della persona offesa e delle altre parti private[177].

Presupposto per detta richiesta, sulla scorta dei principi dettati in ambito sovranazionale, è che vi siano sufficienti indizi di reato in ordine a delitti per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni e per reati di minaccia e di molestia gravi o disturbo alle persone col mezzo del telefono e che i dati siano rilevanti per la prosecuzione delle indagini.

Tuttavia, per non arrecare un grave pregiudizio alle indagini o nei casi di urgenza, e quando vi sia fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio le indagini, l'acquisizione potrà essere disposta con decreto motivato del pubblico ministero. In tal caso, il controllo del giudice dovrà avvenire entro 48 ore, con l'emanazione di un decreto motivato che disponga la convalida e l'autorizzazione.

---

dell'imputato nel corso di un processo penale, ma anche ad acquisire, in fase di indagine, e in prima persona, elementi di prova a favore dell'indagato (inclusi quelli condensati, se del caso, in eventuali tabulati telefonici) essendo in suo potere anche richiedere l'archiviazione del procedimento all'esito delle predette indagini e a nonna dell'art. 408 cpp.». Cfr. 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*, in www.sistemapenale.it 7 maggio 2021. Per ulteriori approfondimenti GIP Roma, decreto 25 aprile 2021, giud. Sabatini con commento di DELLA TORRE J., *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, *ivi*, 29 aprile 2021; MALACARNE A., *Ancora sulle ricadute interne della sentenza della Corte di Giustizia in materia di acquisizione di tabulati telefonici: il G.i.p. di Roma dichiara il "non luogo a provvedere" sulla richiesta del p.m., ivi*, 5 maggio 2021.

[174] Tribunale di Rieti, ordinanza 4 maggio 2021.

[175] Cfr. GRANOZIO L., *Corte di Giustizia sui tabulati: soluzioni contrastanti*, in www.penaledp.it, 18 maggio 2021; MALACARNE A., TESSITORE G., *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di Giustizia: ancora inadeguata la disciplina interna?,* cit.

[176] D.l. 30 settembre 2021, n. 132 recante '*Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP'* – pubblicato nella G.U. n. 234 del 30 settembre 2021.

[177] FILIPPI L., *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in www.penaledp.it, 1ottobre 2021; Id., *La disciplina italiana dei tabulati telefonici e telematici contrasta con il diritto U.E.*, in www.dirittodidifesa.eu, 20 marzo 2021. Sull'utilizzabilità dei tabulati acquisiti prima del d.l 132/ 2021 dalla polizia giudiziaria, in assenza di decreto del pm v. Cass., sez VI, 14 aprile 2023, n. 15836, dove la Corte ha escluso la legittimità dell'acquisizione effettuata dalla PG senza decreto del pm.

L'art. 132 co. 4-*ter*, inoltre, consente il congelamento dei dati di traffico telematico per un periodo non superiore a 90 giorni, per finalità relative allo svolgimento di investigazioni preventive o per l'accertamento e la repressione di specifici reati. È, tuttavia, necessario che tali provvedimenti vengano notificati entro 48 ore al pubblico ministero del luogo di esecuzione che, in presenza dei presupposti, provvederà alla convalida; la mancata convalida determina la perdita di efficacia.

Numerosi i profili di criticità evidenziati dalla dottrina riguardo alla nuova disciplina: tra questi, la carenza di gravità dei delitti, stante il riferimento al limite edittale "non inferiore nel massimo a tre anni" o ai reati di minaccia e di molestia gravi[178]. Ancora, non soddisfacente appare il presupposto dei sufficienti indizi di reato e della rilevanza per l'accertamento dei fatti, accertamenti che realizzerebbero una tutela inferiore rispetto a quella prevista per le intercettazioni, per le quali sono richiesti "gravi indizi di reato"[179].

Un ulteriore aspetto riguarda il ruolo del pubblico ministero e della difesa per l'accesso ai dati. Come già accennato, entrambi i soggetti potranno avanzare una richiesta al giudice; in ogni caso, solo il pubblico ministero potrà disporre, nei casi di urgenza, l'acquisizione con decreto, con successiva convalida da parte del giudice nelle 48 ore successive.

In questo scenario, si determina una situazione di pregiudizio per la difesa che non potrà avvalersi delle indagini difensive, ma, al fine di acquisire i dati, dovrà fare apposita istanza al giudice, essendo «deprivata del potere di "disporre" del material e acquisito, che risulterà utilizzabile anche se non introduce un elemento di prova a favore del proprio assistito»[180].

---

[178] DINACCI F. R., *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Proc. Pen. Giust.,* 2022, 2, p. 316, osserva come non sia sufficiente: «conferire la nozione di gravità ad un reato attraverso una semplice aggettivazione. Peraltro l'indeterminatezza della stessa espone la norma ad un *deficit* di tipicità e comunque, anche a voler per assurdo superare tale questione, si deve rilevare come l'attributo della gravità costituisca un segno normativo riferibile non al reato in sé ma al contesto ed alle modalità con cui lo stesso è stato realizzato. Si è in presenza di elementi extra normativi a cui si affida il potere di un'attività di indagine che limita diritti del singolo».

[179] Di tale parere DINACCI F. R., *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, cit., p. 316: «In ogni caso, richiedendosi indizi di reato e non di colpevolezza, non risulta necessario che gli indizi risultino soggettivamente orientati, potendosi giustificare l'acquisizione dei tabulati anche nell'ambito di procedimenti a carico di ignoti. Deve in ogni caso essere chiara la necessità dell'esistenza di un *fumus* che, pur non dovendo assurgere ad una specifica componente probatoria, deve comunque dare conto della serietà del progetto investigativo sulla base di elementi non equivoci. Tali dati minimali devono essere rigorosamente osservati non solo per assegnare un valore concreto alla locuzione normativa che richiede il raggiungimento di una soglia probatoria in linea, del resto, con i comandi europei, ma anche per evitare "sviamenti" operativi tendenti ad utilizzare lo strumento acquisitivo del tabulato telefonico quale momento meramente esplorativo d'indagine per una notizia di reato».

[180] *Ibidem*., p. 322.

Nella nuova normativa va ancora, segnalata una lacuna circa il dovere di conservazione del dato originale, in grado di garantire un controllo *ex* post a garanzia dell'inalterabilità dell'informazione.

L'acquisizione dei dati di traffico da parte del giudice, sin dalla modifica operata dalla l. 48/2008, è stata sovente ricondotta all'art. 254-*bis* c.p.p o all'art. 256 c.p.p., norma, quest'ultima, che legittima l'autorità giudiziaria a richiedere atti e documenti o ogni altra cosa di cui determinati soggetti siano in possesso in ragione del loro ufficio, incarico, ministero, professione o arte, ad eccezione dei casi in cui venga eccepito il segreto di Stato o inerente al loro ufficio o professione.

La l. n. 48/2008 ha espressamente ampliato la portata di tale strumento, inserendo, tra quanto può essere oggetto di richiesta anche "dati, informazioni e programmi informatici".

L'art. 254-*bis* c.p.p, prevede, invece, il sequestro presso i fornitori di servizio, ammettendo che l'acquisizione avvenga "mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità". Vi sono, tuttavia, dubbi sull'esecuzione dell'atto e sulle conseguenze una volta scaduto il termine di conservazione del dato in capo ai *provider* [181].

La consegna del tabulato può avvenire attraverso un documento stampato o un file modificabile, ma – scaduto il termine entro il quale i *provider* hanno obbligo di conservazione – verrebbe a mancare la possibilità di successivo controllo sulla genuinità della prova, con le conseguenti ricadute sul contraddittorio e sul diritto ad un equo processo.

Infatti, il disposto dell'art. 254-*bis* c.p.p. nulla dice sulla conservazione del dato originale da parte del *provider*, ma formula solamente indicazioni sulla copia, mentre l'art. 256 c.p.p. lascia alla discrezionalità dell'autorità giudiziaria la possibilità di richiedere gli originali.

---

[181] DINACCI F. R., *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, cit., p. 322: «La circostanza assume rilievo solo che si considerino i limiti temporali di conservazione del dato da cui origina il tabulato. Può quindi accadere che un tabulato acquisito nel corso delle indagini preliminari, nel momento in cui viene reso ostensibile non consenta più il controllo della fonte da cui è originato. E la situazione, come si è visto, ha ricevuto solo una potenziale tutela nel testo dell'art. 254 *bis* c.p.p. laddove si prevede che l'autorità giudiziaria "può" prescrivere che l'acquisizione dei dati di traffico telefonico e di ubicazione avvenga tramite copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti rispetto a quelli originali e la loro immodificabilità. Solo in tale evenienza «è ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali». La disposizione evidenzia come il legislatore si sia posto il problema della verifica dei dati contenuti nel tabulato ma abbia rimesso ad una decisione potestativa dell'autorità giudiziaria la possibilità di consentire *ex post* un controllo sulla genuinità dell'elemento conoscitivo. L'opzione legislativa, oltre a denotare uno scarso rispetto delle logiche confutative che presidiano e devono presidiare i metodi di conoscenza giudiziale, si pone in assoluta controtendenza rispetto a quelle diverse scelte che impongono l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione mediante una procedura che ne assicuri la rispondenza all'originale e l'immodificabilità».

Nei casi in cui la richiesta provenga dalla difesa "l'anomia legislativa è totale"[182]; peraltro, questa ha la possibilità di chiedere autonomamente i dati al *provider* solo per le utenze intestate al proprio assistito. L'impossibilità di effettuare un controllo *ex post* genera chiaramente un problema di valutazione e accertamento che pregiudica non solo il diritto di difesa, ma anche la stessa verificabilità qualora sia la difesa ad acquisire il dato, in assenza di specifiche disposizioni che regolino tale operazione.

Con riguardo alla procedura di accesso ai dati *ex*. art. 132 codice *privacy*, ci si domanda se questa sia assimilabile ai mezzi di ricerca della prova già esistenti e, nello specifico, alle intercettazioni e perquisizioni o, piuttosto, se si tratti di mera acquisizione documentale. Quest'ultimo accostamento non appare soddisfacente considerato che il documento, quale mezzo di prova precostituito, può essere poi prodotto in qualunque momento del processo, salvo il diritto delle parti di esaminarlo. Ciò stride con la disciplina della *data retention* che sanziona con l'inutilizzabilità l'acquisizione oltre i termini.

Perplessità sorgono anche rispetto all'assimilazione alla perquisizione, mancando un'attività di ricerca, sostituita invece dalla richiesta al *provider;* allo stesso modo riguardo alle intercettazioni. Seppure i dati siano strettamente connessi alle comunicazioni, le modalità di svolgimento dell'atto sono del tutto diverse.

Sulla scorta di queste considerazioni, parte della dottrina[183] ritiene che ci si trovi di fronte a un nuovo mezzo di ricerca della prova che meriterebbe di essere disciplinato all'interno del codice di rito.

2.2.2. L'acquisizione di dati da provider *con sede all'estero: il difficile equilibrio tra esigenze investigative e diritti fondamentali*

Una trattazione autonoma va fatta per i dati detenuti da *provider* con sede fuori dal territorio nazionale, in merito all'utilizzo del *cloud computing*.

Le misure previste dal nostro ordinamento, infatti, potrebbero rivelarsi inefficaci qualora un *provider* sia soggetto, in virtù della sede legale di appartenenza, alla legislazione estera. In queste ipotesi, infatti, non ci si potrà avvalere degli strumenti delle ispezioni o

[182] *Ibidem*,, cit., p. 316.
[183] MARCOLINI S., *La disciplina processuale italiana sulla* data retention, p. 44 in FLOR R., MARCOLINI S., *Dalla* data retention *alle indagini ad altro contenuto tecnologico*, G. Giappichelli Editore, 2022. Per approfondimenti v. anche FLOR R., Data retention *e art. 132 cod.* privacy: vexata quaestio?, in *Dir. Pen. Cont.*, 29 marzo 2017.

perquisizioni informatiche, né delle richieste di accesso agli atti ai sensi della normativa interna[184].

Si pone quindi l'interrogativo in merito alle modalità da seguire per l'ottenimento dei dati utili ai fini investigativi.

Nella prassi[185] è diffuso l'impiego della *voluntary disclosure*, sicché i fornitori di servizi con sede legale all'estero collaborano, efficacemente, con le autorità italiane per la consegna di *subscriber data* e *traffic data* (per un periodo variabile tra 30 e 90 giorni).

Significativo è il caso Microsoft: la società ha consentito l'accesso a *subscriber data* in relazione a caselle *email* "@hotmail.it" e anche *"@hotmail.com*" e. allo stesso modo Google, seppure solo per dati collegati a un indirizzo IP che rientrava nel *range* di Paesi membri UE. Tuttavia, non è possibile il ricorso alla *voluntary disclosure* per i dati di contenuto, richiedendosi a tal fine l'utilizzo degli strumenti di cooperazione giudiziaria[186].

Riguardo la consultazione di un *account* di posta elettronica con le credenziali di accesso e al successivo sequestro, la Corte di Cassazione ha stabilito come non sia rilevante la presenza fisica dei dati in territorio estero, quanto piuttosto il fatto che il sequestro abbia ad oggetto i dati del soggetto che dispone delle credenziali di accesso[187]. Ciò perchè «nel momento in cui viene ad essere operato il sequestro del documento informatico (nel caso che ci occupa la bozza di e*mail*) il sequestro viene operato all'utente finale, nel luogo in cui lo stesso accede digitando la *password*».

In tal modo viene privilegiato lo Stato in cui si trova il sistema informatico di accesso e dell'utente, più che quello di localizzazione dei dati; tuttavia, non va trascurato come, nel

---

[184] V. anche. CURTOTTI D., *Il sequestro*, in ATERNO S., CAJANI F., COSTABILE G., CURTOTTI D. (a cura di), Cyber forensics *e indagini digitali*, cit.

[185] V. DANIELE M., *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1282; KLEIJSSEN J., PERRI P., *Cybercrime, Evidence and Territoriality: issues and options*, in *Netherlands Yearbook of International Law* 2016, 14 dicembre 2017, p. 163; SIRIUS EU *Digital Evidence Situation Report 2022 – 4th Annual Report,* https://www.eurojust.europa.eu/publication/sirius-eu-digital-evidence-situation-report-2022., *EU Digital Evidence Situation Report 3rd Annual Report 2021*, https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_DESR_12_2021.pdf.

[186] CAJANI F., *Le richieste per finalità di giustizia agli* internet service provider *esteri*, p. 410, in ATERNO S., CAJANI F., COSTABILE G., CURTOTTI D. (a cura di), Cyber forensics *e indagini digitali*, cit.; ID, *L'acquisizione dei dati del traffico*, cit.; DANIELE M., *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1279.

[187] Cass., Sez. IV, 28 giugno 2016, n. 40903: «Chi è che "detiene" i dati quando gli stessi sono conservati (come accadeva nel caso che ci occupa per i messaggi salvati nella casella "bozze" o come potrebbe accadere per i documenti che ciascuno ha sul proprio spazio concessogli di Dropbox o di Google Drive) all'interno di uno spazio virtuale che viene concesso al singolo utente e cui lo stesso può accedere solo digitando una *password* che solo lui conosce? Secondo la (non condivisibile) tesi dei ricorrenti quei file sono nella disponibilità *dell'Internet Service Provider* (ISP), che nel caso che ci occupa è la società statunitense che gestisce le caselle (OMISSIS). E quindi, se li si va a sequestrare, occorre rispettare la disciplina prevista dall'art. 254 c.p.p., e s.s. e in particolar modo quella di cui al già ricordato art. 254-*bis* c.p.p. Ma non è così. […] Ebbene, tale potere sui messaggi nella casella "bozze" lo esercita soltanto chi è in possesso della *password* per accedere all'account di posta elettronica. […]. E quindi, correttamente, si è ritenuto essere al di fuori dell'ipotesi disciplinata normativamente dall'art. 254-*bis* c.p.p».

contesto del *cloud computing*, i dati siano soggetti a uno spostamento continuo che rende complessa l'identificazione del *server* su cui sono allocati.

Il tema dell'acquisizione dei dati provenienti da *server* esteri è tornato alla ribalta in ragione di alcuni recenti interventi della Corte di Cassazione[188] relativi all'accesso ai server di SKY ECC (sistema di produzione canadese di proprietà della società SKY Global, specializzata nella fornitura di strumenti di comunicazione sicura e protetta da un sistema di codifica dei dati) da parte di Europol.

Nello specifico, nel 2001, Europol, nel contesto di una squadra investigativa comune (SIC) che aveva coinvolto le autorità di polizia francese, belga e olandese, aveva avuto accesso ai messaggi nella disponibilità della società canadese, scambiati tra i criptofonini[189] in uso ai suoi utenti.

Le autorità italiane chiedevano la consegna dei messaggi relativi a conversazioni tra soggetti sottoposti a indagini, attraverso l'emissione da parte del pubblico ministero di un ordine di indagine europeo, ai sensi del d. lgs 21 giugno 2017 n. 108[190], indirizzato alla competente autorità francese[191].

Va specificato che sia le attività di captazione, sia quelle di decriptazione erano state eseguite dalle polizie straniere, mediante l'individuazione del necessario algoritmo utilizzato dalla società proprietaria del sistema di cifratura SKY ECC.

Come precisato, «tali sistemi di comunicazione di SKY Ecc non sono basati sulla tecnologia *pin to pin* (tipo *Blackberry*, cioè su un sistema crittografico dove le chiavi di cifratura sono collocate in un *server*), bensì sul sistema *end to end*, che prevede la cifratura delle conversazioni mediante l'utilizzo di chiavi depositate esclusivamente sui dispositivi

---

[188] Cass., Sez. IV, 7 settembre 2022, n. 32915 con commento di BARBIERI A., *I limiti di utilizzabilità dei messaggi crittografati scaricati da un* server *estero ed acquisiti mediante ordine europeo di indagine*, in *Giurisprudenza Penale Web*, 2023, 2; Cass., Sez. VI, 20 dicembre 2022, n. 4833; Cass., Sez. IV, 5 aprile 2023, n. 16345; Cass., Sez. IV, 15 febbraio 2023, n. 12140; Cass., Sez. I, 13 ottobre 2022, n. 6364; Cass., Sez. I, 13 ottobre 2022, n. 6263; Cass., Sez. I, 1 luglio 2022, n. 34059.

[189] Per approfondimenti LUDOVICI L., *I criptofonini: sistemi informatici criptati e* server *occulti*, in *www.penaledp.it,* 14 ottobre 2023.

[190] D. lgs. 21 giugno 2017, n. 108, recante "*Norme di attuazione della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale*", in G.U. Serie Generale n. 162 del 13/07/2017. In argomento v., tra i tanti, BELFIORE R., *Su alcuni aspetti del decreto di attuazione dell'ordine europeo di indagine penale*, in *Cass. Pen.*, 2018, 1, p. 400 ss.; CAIANIELLO M., *L'attuazione della direttiva sull'ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio,* in *Cass. Pen.*, 2018, 6, p. 2197 ss.; CAMALDO L., *La normativa di attuazione dell'ordine europeo di indagine penale: le modalità operative del nuovo strumento di acquisizione della prova all'estero*, in *Cass. Pen.*, 2017, 11, p. 4196 ss.; DANIELE M., *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d.lgs. n. 108 del 2017,* in *Dir. Pen. Cont.,* 28 luglio 2017; TINOCO PASTRANA A., *L'ordine europeo di indagine penale*, in *Proc. Pen Giust.*, 2017, 2.

[191] Cfr. Cass., Sez. VI, 20 dicembre 2022, n. 48330.

che colloquiano, sicché, in questa modalità, neanche il gestore del servizio è in grado di conoscere le chiavi utilizzate e, di conseguenza, il contenuto delle comunicazioni»[192].

Sul fronte della disciplina da applicare, i giudici di legittimità, hanno chiarito, in alcune pronunce [193], come l'attività di decriptazione di comunicazioni captate non sia da ricondurre all'art. 266 c.p.p., ma all'art. 234-*bis* c.p.p. relativo ai documenti informatici[194].

Nello specifico, si è operato un distinguo tra attività intercettiva e successiva attività di decriptazione, e si è ritenuto che in caso di decriptazione, la disciplina da applicare permetta l'acquisizione dei dati da parte di società o autorità estere senza necessità di garantire un controllo *ex post* sulle modalità effettuate[195].

Sul fronte, invece, delle garanzie applicabili, appare di interesse un caso [196] in cui la difesa aveva richiesto di accedere alla documentazione probatoria relativa alle attività eseguite dalla polizia francese, ma non le venivano forniti i verbali comprovanti le specifiche modalità di acquisizione e decriptazione dei dati. La motivazione era che si trattava di attività eseguite dalla polizia francese e coperte dal segreto di Stato.

---

[192] Cit. Cass., Sez. I, 13 ottobre 2022, n. 6364. Per approfondimenti v. CURTOTTI D., RIZZI V., NOCERINO W., RUSSITTO A., GILIBERTI G., SCARPA G., *Piattaforme criptate e prova penale*, in *www.sistemapenale.it*, 26 giugno 2023.

[193] Cass., Sez. IV, 15 febbraio 2023, n. 12140 e la più recente Cass., Sez. IV, 5 aprile 2023, n. 16347.

[194] Sul fronte opposto Corte Cost., 27 luglio 2023, n. 170, secondo la quale messaggi di posta elettronica, SMS e conversazioni Whatsapp non rientrano nella categoria dei documenti informatici, ma nella corrispondenza, tutelata dall'art. 15 Cost. Per approfondimenti sugli effetti di tale sentenza v. MORCELLA M.T., *Ancora questioni in tema di sequestro di* smartphone, in *www.penaledp.it*, 9 novembre 2023.

[195] *Ibidem*: «Si è già spiegato come vi siano due diversi tipi di operazione che gli inquirenti possono effettuare nello svolgimento delle indagini, rispetto alle comunicazioni a distanza:
a) quelle di captazione e registrazione del messaggio cifrato, nel momento in cui esso è in transito dall'apparecchio del mittente a quello del destinatario; tale fattispecie cade sotto la previsione dell'art. 266 *bis*, c.p.p., che estende l'applicabilità delle norme del codice di rito, relative alle "normali" intercettazioni di conversazioni o comunicazioni tra soggetti a distanza, alle intercettazioni di flussi di comunicazioni relativi a sistemi telematici ovvero intercorrenti tra più sistemi telematici, sfruttando la trasmissione dei dati in via telematica, dunque via cavo o ponti radio, ovvero per mezzo di altra analoga strumentazione tecnica (Sez. 4, n. 49896 del 15/10/2019, Brandimarte, Rv. 277949-01; Sez. 3, n. 47557 del 26/9/2019, Scognamiglio, Rv. 277990-01, 02; Sez. 3, n. 50452 del 10/11/2015, Guarnera, Rv. 265615-01);
b) ci sono poi le diverse operazioni di decriptazione del contenuto del messaggio, necessarie per trasformare mere stringhe informatiche in dati comunicativi intellegibili; per queste non operano le regole sopra richiamate; i messaggi possono essere in chiaro, oppure necessitare di apposito algoritmo (o "chiave di cifratura"); in ogni caso, esse diventano dati informatici direttamente utilizzabili a fini di prova (vedi, in motivazione, Sez. 1, n. 34059 del 1/7/2022, Moisso); allorquando si abbia a che fare con tali dati, come la stessa difesa ha rilevato, la norma disciplinante l'acquisizione di essi è quella dell'art. 234 *bis*, c.p.p.». Ed inoltre, Cass, Sez. I, 13 ottobre 2022, n. 6364: «Si tratta di disposizione applicabile anche nel caso *de quo*, in cui l'acquisizione ha riguardato non un documento cartaceo o analogico, bensì un documento inteso come "rappresentazione comunicativa incorporata in una base materiale con un metodo digitale", ovverosia dati informatici che hanno consentito di rendere intellegibile il contenuto di stringhe redatte secondo il sistema binario. Vi è stato, altresì, il consenso all'acquisizione da parte del "legittimo titolare" di quei documenti o dati conservati all'estero, da intendersi come persona giuridica che di quei documenti o di quei dati poteva disporre in forza di un legittimo titolo secondo l'ordinamento giuridico del paese estero, identificabile non soltanto nella persona fisica e/o giuridica che procede alla trasmissione e alla conservazione dei dati, ma anche nella polizia giudiziaria, nell'autorità giudiziaria, nella persona offesa, nell'amministrazione pubblica, nella società che gestisce il servizio telefonico, nell'*internet service provider*».

[196] Cass., Sez. IV, 5 aprile 2023, n. 16345.

In effetti, la polizia francese non forniva alcuna indicazione sulla modalità seguita, ma si limitava a certificare la regolarità delle procedure.

A fronte delle doglianze del ricorrente, la Corte di legittimità rispondeva che la cooperazione giudiziaria in materia penale si fonda sul principio del reciproco riconoscimento e sulla fiducia reciproca tra Stati dell'Unione; questo implica che l'OEI sia riconosciuto ed eseguito senza ulteriori formalità, come se fosse un atto disposto dall'autorità nazionale, a meno che vi siano legittimi motivi di non riconoscimento o non esecuzione o che l'esecuzione contrasti con i diritti fondamentali.

Nella sostanza, il giudice italiano «non può e non deve conoscere della regolarità degli atti di esecuzione di attività di indagine compiuta dall'autorità giudiziaria straniera (nel caso di specie francese), giacché detta l'attività investigativa è eseguita secondo la legislazione dello Stato straniero»[197].

Quanto detto vale ancor di più allorquando l'originaria attività investigativa non derivi da una richiesta del giudice italiano, ma sia stata eseguita nell'ambito di un procedimento instaurato autonomamente nello Stato estero, che abbia permesso di acquisire dei dati anteriormente all'OEI.

Sul versante del diritto di difesa, profili di interesse presenta una pronuncia di legittimità che, tuttavia, sembra porsi come isolata. Nel caso di specie, si è infatti affermata la necessità di garantire il contraddittorio sulle modalità di acquisizione, mediante ordine europeo di indagine, dei messaggi[198].

La difesa aveva formulato richiesta di accesso agli atti, chiedendo altresì l'indicazione delle modalità di acquisizione degli stessi da parte di Europol; richiesta,

---

[197] Cass., Sez. I, 13 ottobre 2022, n. 6364

[198] BARBIERI A., *I limiti di utilizzabilità dei messaggi crittografati scaricati da un* server *estero ed acquisiti mediante ordine europeo di indagine,* cit., p. 8: «L'art. 191 c.p.p. non costituisce soltanto un presidio a tutela del singolo ma anche una garanzia sulla correttezza dell'accertamento giurisdizionale, perché finalizzato a consentire il raggiungimento di un migliore risultato conoscitivo; tale prospettiva ermeneutica - si è precisato - trova conferma nell'art. 111 Cost., perché il rispetto dei principi del giusto processo è funzionale a garantire non soltanto la legittimità della prova in sé ma la legalità del procedimento di acquisizione. […] Tuttavia, la mancata partecipazione delle modalità acquisitive determina l'inutilizzabilità o il divieto d'uso del dato, perché il procedimento probatorio si è svolto in violazione del diritto al contraddittorio garantito dall'art. 111 Cost. e dall'art. 6 CEDU. […] Le disposizioni costituzionali poste a presidio dei diritti fondamentali dell'individuo sono di immediata applicazione nel processo penale per la loro natura precettiva; tra queste rientra sicuramente l'art. 111 Cost., che detta specifiche disposizioni affinché la giurisdizione sia attuata mediante il giusto processo. Il diritto al contraddittorio espressamente previsto dall'art. 111 co. 2 Cost. trova concreta attuazione attraverso la possibilità di piena partecipazione all'attività istruttoria ovvero, secondo la più ampia accezione elaborata dalla Corte Europea dei Diritti dell'Uomo in applicazione dell'art. 6 CEDU, attraverso la possibilità di controllo sul procedimento di formazione della prova quando la partecipazione non sia possibile in ragione della natura dell'attività svolta. La mancata conoscenza delle modalità acquisitive esclude in radice ogni controllo di legittimità sul procedimento probatorio ed impedisce lo svolgimento del processo penale secondo un modello di legalità di accertamento del fatto. Non va sottovalutato neppure che l'impossibilità di controllo sulle modalità acquisitive incide sulla garanzia di verifica della genuinità del dato informatico, perché ostacola, oltre che il riscontro sulla natura dell'attività investigativa concretamente svolta, anche l'accertamento della corrispondenza tra il dato originario criptato e il messaggio di testo reso intellegibile».

tuttavia, rigettata. Nell'accogliere il ricorso, la Corte ha affermato la necessità di valutare in concreto la legittimità delle modalità di acquisizione utilizzate e la conformità con i principi fondamentali dell'ordinamento. Ciò in quanto la dialettica procedimentale non può esplicarsi solo in relazione al materiale acquisito, ma va estesa anche alle relative modalità di acquisizione, nel rispetto del principio del contraddittorio, con lo scopo di rilevare eventuali profili di inutilizzabilità, non solo a «garanzia di partecipazione e assistenza in sé dell'imputato o delle altre parti, ma al *quomodo* della formazione della prova che caratterizza il processo penale secondo un modello conforme alla Costituzione e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali»[199].

Questo orientamento, se condivisibile, nella parte in cui mostra di volere privilegiare i diritti fondamentali[200], tuttavia, finisce per ridimensionare la *mutual trust* tra gli Stati membri UE, innestando un contrasto con la presunzione di legittimità delle operazioni eseguite dalle autorità di polizia estere.

Interessanti appaiono anche le conclusioni cui è pervenuta la Cassazione[201], in merito alle *chat* acquisite dai *server* di SKY-ECC.

In tal caso, si è infatti ritenuto che le *chat*, pur se decriptate dalle autorità di polizia francesi, potevano essere acquisite legittimamente ai sensi dell'art. 234-*bis* c.p.p.[202].

Con riguardo alla procedura di decriptazione, l'organo di legittimità[203] è stato chiamato a pronunciarsi anche sull'utilizzabilità dei risultati di intercettazioni di comunicazioni svolte su dispositivi BlackBerry, i cui messaggi siano stati decriptati attraverso l'ausilio della società estera.

Le comunicazioni svolte tra dispositivi BlackBerry si avvalgono di meccanismi di criptazione *pin to pin* (*person identification number*) che richiedono necessariamente l'utilizzo di un algoritmo associato a specifici codici in possesso della società produttrice. La prassi, in tale caso, consiste nel richiedere a tale società la decriptazione delle comunicazioni, acquisendole poi come documenti, ai sensi dell'art. 234 *bis* c.p.p.

---

[199] BARBIERI A., *I limiti di utilizzabilità dei messaggi crittografati scaricati da un* server *estero ed acquisiti mediante ordine europeo di indagine*, cit., p. 12. Inoltre «più precisamente, il contraddittorio nella formazione della prova non è un diritto dell'imputato strettamente inteso, ma è una regola fondamentale di svolgimento del processo penale, che lo caratterizza con specifico riguardo all'attività probatoria ; pertanto, la violazione del contraddittorio, inteso – nel caso scrutinato dalla sentenza in commento - come violazione della garanzia di possibilità di controllo sul procedimento di formazione della prova, conduce all'inutilizzabilità del risultato acquisito».

[200] Sulla necessità di garantire il contraddittorio sulle modalità di acquisizione mediante ordine europeo di indagine v. Cass., Sez. IV, 7 settembre 2022, n. 32915.

[201] Cass., Sez. I, 15 settembre 2022, n. 34059.

[202] Medesimo orientamento in Cass., Sez. I, 1 luglio 2022, n. 34059.

[203] Cass. Sez. VI, 28 febbraio 2023, n. 8714 con nota di FILIPPI L, *Quattro miti da sfatare sull'intercettazione dei cellulari BlackBerry*, in *www.penaledp.it,* 28 aprile 2023.Vedasi anche TROGU M., *Come si intercettano le* chat pin to pin *tra dispositivi Blackberry*?, in *Proc. Pen. Giust.*, 2016, 3, p. 73.

Nel caso di specie, le autorità avevano provveduto ad acquisire intercettazioni attraverso la tecnica dell'instradamento ma, per ottenere delle risultanze valutabili in dibattimento, avevano richiesto assistenza alla società estera per effettuare la decriptazione. La Corte ha ritenuto che al giudice di merito spetti solo l'apprezzamento del contenuto delle intercettazioni, escludendo la possibilità di sindacare tali prove in sede di legittimità, se non nei limiti della manifesta illogicità e irragionevolezza della motivazione, o quando la prova venga travisata[204].

Questo orientamento, certamente sbilanciato verso le istanze di persecuzione, a scapito dei diritti dell'individuo e del contradditorio, è stato oggetto di critiche da parte della dottrina[205].

In questo fluire giurisprudenziale, si inserisce una pronuncia[206] secondo cui l'assenza di chiarezza sulle modalità di decriptazione delle *chat Blackberry*, legittimamente intercettate, va qualificata quale nullità a regime intermedio *ex* artt. 178 lett. c) c.p.p. e 179 c.p.p., per violazione del diritto di difesa.

---

[204] *Ibidem*: «Secondo il costante orientamento della giurisprudenza di legittimità l'interpretazione delle conversazioni intercettate costituisce questione di fatto, rimessa all'esclusivo apprezzamento del giudice di merito, non sindacabile in sede di legittimità se non nei limiti della manifesta illogicità e irragionevolezza della motivazione (tra le tante, Sez. U, n. 22461 del 26/02/2015, Sebbar, Rv. 263715; Sez. 6, n. 9204 del 01/03/2022, Cannata + altri, non mass.) o quando l'iter argomentativo della sentenza operi un travisamento della prova indicando un contenuto difforme da quello reale e la difformità risulti decisiva e incontestabile».

[205] E invero FILIPPI L, *Quattro miti da sfatare sull'intercettazione dei cellulari BlackBerry*, cit., p. 7: «La giurisprudenza ammette la decriptazione all'estero del messaggio intercettato con un atteggiamento fideistico inammissibile nel processo penale, nel quale si deve decidere sulla responsabilità dell'imputato. Infatti, la giurisprudenza considera irrilevante che per la decriptazione dei dati identificativi associati ai codici *pin* sia necessario ricorrere alla collaborazione del produttore del sistema operativo avente sede all'estero, che trasforma, tramite l'apposito algoritmo, i dati informatici conservati all'estero in contenuti intellegibili cioè in un documento informatico che, ai sensi dell'art. 234-*bis* c.p.p., è acquisito, previo consenso del legittimo titolare, ma senza alcuna garanzia giurisdizionale e senza un contraddittorio che assicuri l'intervento della difesa e dell'accusa mediante loro consulenti tecnici». Inoltre, vedasi BARBIERI A., *I limiti di utilizzabilità dei messaggi crittografati scaricati da un* server *estero ed acquisiti mediante ordine europeo di indagine*, cit., p. 23 :«Rimane, invece, aperto (e lo dimostra la sentenza di segno contrario relativa al medesimo materiale d'indagine ritenuto acquisibile ed utilizzabile a norma dell'art. 234-*bis* cpp) il tema della necessità di superare, nell'applicazione concreta, le incertezze nella individuazione della linea di demarcazione tra l'acquisizione della messaggistica crittografata secondo lo schema procedurale previsto per i documenti e la captazione dei messaggi nell'ambito di una vera e propria attività di intercettazione dei flussi telematici generati dalla comunicazione; ciò è funzionale a garantire, con pienezza di contenuti, la libertà e segretezza delle comunicazioni e ad evitare che, attraverso lo schermo dell'acquisizione documentale, sia elusa l'applicazione delle disposizioni inderogabili in materia di intercettazioni» .

[206] Cass., Sez. IV, 15 ottobre 2019, n. 49896: «la difesa ha diritto di ottenere la versione originale e criptata dei messaggi e le chiavi di sicurezza necessarie alla decriptazione, a pena di nullità *ex* art. 178, lett. c), cpp; laddove alla difesa, non solo in sede cautelare ma in anche nel corso del giudizio di merito, fosse precluso di prendere cognizione dei flussi di comunicazioni informatiche o telematiche, nella loro versione originale ed integrale, e fosse conseguentemente impedito l'esercizio di ogni potere di controllo, sussisterebbe una nullità di ordine generale a regime intermedio, derivante dalla violazione della disciplina diretta ad assicurare l'assistenza e la rappresentanza dell'imputato in una ipotesi in cui non è obbligatoria la presenza del suo difensore».

Queste pronunce rivelano il tentativo da parte della giurisprudenza di supplire alle inerzie legislative o, comunque, all'incompletezza della disciplina vigente, la quale richiede di adeguarsi agli sviluppi delle indagini, anche a livello transnazionale[207].

Il rischio, a fronte del quadro sin qui tracciato, è che si creino indirizzi diversi che, più che risolvere un problema, aumentano l'incertezza giuridica, a scapito della tutela dei diritti fondamentali.

Ebbene, di recente è stata posta all'attenzione delle Sezioni Unite[208] la questione sulla riconducibilità delle comunicazioni decriptate, acquisite dalla polizia giudiziaria straniera attraverso ordine europeo di indagine, all'art. 234 c.p.p. o all'art. 234-*bis* c.p.p [209].

I giudici remittenti hanno analizzato i vari orientamenti interpretativi: per un verso, quello secondo cui le comunicazioni decriptate e successivamente acquisite non rispondono alla disciplina delle intercettazioni *ex* art. 266-*bis* c.p.p., trattandosi di flussi comunicativi non più in atto al momento della richiesta e del trasferimento dei dati; per altro verso, la tesi secondo cui il *discrimen* per l'applicazione dell'art. 234-*bis* c.p.p. sia la preesistenza degli elementi -«intesi come elementi informativi "dematerializzati"»[210] - rispetto all'avvio delle indagini da parte dell'autorità giudiziaria.

La stessa Corte ha, peraltro, evidenziato come ulteriori orientamenti[211] avrebbero ricondotto tali prove all'art. 234 c.p.p., considerato che l'art. 234-*bis* c.p.p. sarebbe riferibile ai casi in cui i dati sono pubblicamente accessibili o si abbia il consenso del legittimo titolare, nozione in cui non si può ricomprendere l'autorità giudiziaria.

Sulla scorta di quanto sopra, è stato chiesto alle Sezioni Unite di stabilire se le *chat* scambiate con sistema cifrato e decriptate dall'autorità giudiziaria straniera che, a seguito di richiesta, ha poi curato il trasferimento dei dati, siano disciplinare dall'art. 234 c.p.p., dall'art. 234-*bis* c.p.p. o da altra disposizione relativa all'acquisizione di prove. E, inoltre, se tale acquisizione debba essere oggetto, ai fini della utilizzabilità dei dati in tal modo versati in atti, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte dell'autorità giurisdizionale nazionale.

---

[207] In dottrina si sottolinea la necessità di uno «statuto delle prove informatiche» utile a « individuare, costruire, consolidare i riferimenti normativi di garanzia: cosa è possibile acquisire, con quali strumenti, come conservare i dati, con quali tecniche e mezzi, come si sono acquisiti, come si devono conservare, come si devono valutare, come evitare le possibili manipolazioni», SPANGHER G., *Servono regole di garanzia per la prova informatica*, in *www.penaledp.it.*, 12 ottobre 2023; v. anche CURTOTTI D., RIZZI V., NOCERINO W., RUSSITTO A., GILIBERTI G., SCARPA G., *Piattaforme criptate e prova penale*, in *www.sistemapenale,* 2023, p. 173.

[208] Cass., Sez. III, ord. 3 novembre 2023, n. 47798.

[209] DANIELE M., *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite*, in *www.sistemapenale.it*, 11 dicembre 2023.

[210] *Ibidem*.

[211] Cass., Sez. IV, 26 ottobre 2023, n. 46833.

In attesa della pronuncia, è stata rimessa alle Sezioni Unite una ulteriore questione relativa alle *chat* decriptate acquisite mediante OEI[212].

Il quesito è volto a determinare lo strumento processuale interno al quale fare riferimento per l'acquisizione, da determinarsi tra il sequestro di corrispondenza informatica (art. 254-*bis* c.p.p.) e l'acquisizione di risultanze delle intercettazioni (art. 270 c.p.p.).

I giudici, infatti, ritengono non applicabile l'art. 234-*bis* c.p.p., trattandosi di norma che – regolando l'acquisizione di documentazione proveniente da fonti aperte o con il consenso del titolare – si pone in rapporto di alternatività rispetto all'OEI o alle procedure di cooperazione giudiziaria.

La Suprema Corte si è da ultimo pronunciata[213] statuendo che l'acquisizione, a mezzo OEI, di comunicazioni scambiate attraverso criptofonini, non rientri nella disciplina dell'art. 234-*bis* c.p.p. ma in quella della circolazione di prove tra procedimenti penali. In particolare, l'attività di acquisizione probatoria di conversazioni acquisite *ex post* andrebbe ricondotta agli art.78 disp. att. c.p.p. e 238 c.p.p., relativi all'acquisizione di prove provenienti da procedimenti stranieri. Quanto, invece, alle conversazioni captate in tempo reale, il riferimento è all'art. 270 c.p.p., relativo all'utilizzo di intercettazioni in procedimenti diversi da quello di origine. In tal senso, i giudici di legittimità hanno ritenuto che l'emissione di un OEI possa provenire dal pubblico ministero, senza preventiva autorizzazione del giudice, in quanto non richiesta in situazioni analoghe, allorquando il pm voglia richiedere il contenuto di comunicazioni acquisite in altro procedimento. Il giudice, tuttavia, dovrà verificare, su richiesta delle parti interessate che ne alleghino una lesione, il rispetto dei diritti fondamentali, nello specifico il diritto di difesa e la garanzia ad un equo processo.

I giudici della Cassazione hanno, peraltro, sostenuto che l'impossibilità per la difesa di accedere all'algoritmo utilizzato per decriptare le comunicazioni non costituisca una violazione dei diritti fondamentali, escludendo ogni alterazione dei dati, dato che una chiave di decriptazione errata non permetterebbe di ottenere dei dati comprensibili.

[212] Cass., Sez. VI, ord. 15 gennaio 2024, n. 2329.
[213] Cass., Sez. Un., 14 giugno 2024, n. 23755 e 23756.

CAPITOLO III

La prova digitale nel sistema spagnolo

3.1 La Ley de Enjuiciamento Criminal: uno strumento da riformare

La *Ley de Enjuiciamento Criminal* (d'ora in avanti LECRIM), principale testo di riferimento per la disciplina del processo penale spagnolo, risale al 14 settembre 1882[214].

Questo dato, già da solo, testimonia le difficoltà degli interpreti nell'adeguare i tradizionali strumenti di indagine alle innovazioni tecnologiche.

La necessità di un intervento riformatore è stata avvertita già dall'emanazione della Costituzione spagnola[215], che ha affermato espressamente i diritti dell'individuo e ha richiesto uno sforzo interpretativo affinché gli atti di indagine già previsti dalla LECRIM - *entrada y registro en lugar cerrado*[216], *registro de libros y papeles*[217], *detención y apertura de la correspondencia escrita y telegráfica*[218]- venissero letti e applicati in conformità al disposto delle sue norme.

Proprio in relazione alla disciplina delle misure investigative, si è verificata per anni una situazione di "anemia legislativa" [219] in assenza di un quadro giuridico chiaro e ben definito, con il conseguente bisogno di un'attualizzazione delle misure previste [220].

Il *deficit* legislativo è stato colmato *in primis* dalla giurisprudenza, attraverso il ricorso all'analogia, più volte contestato dalla Corte europea dei diritti umani.

---

[214] *Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal*, pubblicata su *Gaceta de Madrid* del 17 settembre 1882, n. 260, https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036 .

[215] *Constitución Española*, pubblicata in BOE 29 dicembre 1978 n. 11, https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229 .

[216] LECRIM art. 545 ss.

[217] LECRIM art. 573 ss.

[218] LECRIM art. 579 ss.

[219] CAMPANER MUÑOZ J., PEREIRA PUIGVERT S., *Eficiencia versus garantías en la investigación penal del siglo XXI*, p. 46 in PEREIRA PUIGVERT S., ORDÓÑEZ PONZ F., PESQUEIRA ZAMORA M. J. (a cura di), *Investigación y proceso penal en el siglo XXI. Nueva tecnologías y protección de datos* , Aranzadi, 2021.

[220] Per approfondimenti BUENO DE MATA F., *Datos personales y proceso penal: diligencias de investigación y tecnologías disruptivas*, in PEREIRA PUIGVERT S., ORDÓÑEZ PONZ F., PESQUEIRA ZAMORA M. J. (a cura di), *Investigación y proceso penal en el siglo XXI. Nueva tecnologías y protección de datos*, Aranzadi, 2021, p. 494 ss.; PÉREZ GIL, J., *Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución*, in BRIGHI R., PALMIRANI M., SÁNCHEZ JORDÁN M.E. (a cura di), *Informatica giuridica e informatica forense al servizio della società della conoscenza: scritti in onore di Cesare Maioli,* Aracne Editrice, 2018, p. 187 ss.

Questa, infatti, ha condannato la Spagna nel caso *Valenzuela Contreras*[221] per la violazione dell'art. 8 della CEDU e per l'assenza di una previsione legale in grado di limitare scelte arbitrarie delle autorità. Nel caso in esame, l'autorità giudiziaria procedeva all'intercettazione delle comunicazioni del ricorrente rifacendosi all'art. 18 co. 3 della Costituzione spagnola[222], ai sensi del quale è garantito il rispetto del segreto delle comunicazioni, salvo in caso di provvedimento giudiziario. Il ricorrente, tuttavia, riteneva che tale scelta determinasse una violazione del suo diritto alla vita privata e familiare poiché la previsione di legge non era sufficientemente chiara e prevedibile. A tal proposito, la Corte, ribadendo che ogni restrizione del diritto al rispetto della vita privata e familiare deve avere una base legale chiara e precisa, in grado di fornire ai cittadini le informazioni sui presupposti e sulle condizioni di applicazione e sulle procedure per lo svolgimento, ha ritenuto che la legge spagnola non indicasse con sufficiente chiarezza i limiti al potere discrezionale delle autorità. Ha, pertanto, ritenuto non sussistente il livello minimo di tutela che deve essere garantito ai cittadini in uno Stato di diritto, con conseguente violazione dell'art. 8. CEDU.

Parallelamente alla Corte di Strasburgo, negli anni, anche le Corti nazionali hanno evidenziato l'assenza di una disciplina legislativa completa che regolasse le attività di

---

[221] CEDU, 30 luglio 1998, ricorso n. 27671/95, *Valenzuela Contreras* c. Spagna, § 60-61: « *Like the Delegate of the Commission, the Court cannot accept the Government's argument that the judge who ordered the monitoring of the applicant's telephone conversations could not have been expected to know the conditions laid down in the Kruslin and Huvig judgments five years before those judgments were delivered in 1990. It reiterates that the conditions referred to in the judgment cited by the Government concerning the quality of the law stem from the Convention itself. The requirement that the effects of the "law" be foreseeable means, in the sphere of monitoring telephone communications, that the guarantees stating the extent of the authorities' discretion and the manner in which it is to be exercised must be set out in detail in domestic law so that it has a binding force which circumscribes the judges' discretion in the application of such measures […]. Consequently, the Spanish "law" which the investigating judge had to apply should have provided those guarantees with sufficient precision. The Court further notes that at the time the order for the monitoring of the applicant's telephone line was made it had already stated, in a judgment in which it had found a violation of Article 8, that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence" (see the Malone judgment cited above, p. 32, § 67). In addition, it points out that in any event the investigating judge who ordered the monitoring of the applicant's telephone communications had himself put in place a number of guarantees which, as the Government said, did not become a requirement of the case-law until much later. In summary, Spanish law, both written and unwritten, did not indicate with sufficient clarity at the material time the extent of the authorities' discretion in the domain concerned or the way in which it should be exercised. Mr Valenzuela Contreras did not, therefore, enjoy the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society (see the Malone judgment cited above, p. 36, § 79). There has therefore been a violation of Article 8».*

[222] «***Artículo 18***

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

indagine a carattere tecnologico, sottolineando il difficile compito di colmare tali lacune e la scarsità di norme a cui fare riferimento[223].

3.2. La Ley 59/2003 e l'introduzione del "documento elettronico"

Mosso dall'esigenza di adeguare l'ordinamento all'evoluzione della società, il legislatore è intervenuto con la *Ley* 59 del 18 dicembre 2003 (*Ley* 59/2003) [224], introducendo le nozioni di firma elettronica e documento elettronico[225].

Ai sensi dell'art. 3 della richiamata Ley 59/2003, poi abrogata dalla Ley 6/2020[226], si considerava documento elettronico la informazione di qualsivoglia natura in formato elettronico, archiviata in un supporto elettronico e in un determinato formato, su cui fosse stata apposta una firma elettronica che permettesse l'identificazione dell'autore.

All'interno di questa categoria era possibile includere non soltanto documenti di testo e fogli di calcolo, bensì immagini, registrazioni, video in formato digitale o un archivio contenuto all'interno di una banca dati.

La nozione di documento è disciplinata anche dall'art. 26 del *Código penal*, che lo riconnette a ogni supporto materiale sul quale siano incorporati e che esterni dati, fatti o narrazioni con efficacia probatoria o con qualunque altro tipo di rilevanza giuridica[227].

---

[223] *Tribunal Supremo*, *Sala de lo Penal*, 18 novembre 2008, n. 776, ECLI:ES:TS:2008:6639, https://www.poderjudicial.es/search/TS/openDocument/6e949cb6e2a13f43/20081230, «*Una vez más, se echa en falta una regulación legal completa de esta compleja materia, tan novedosa y cambiante por otra parte, por lo que la jurisprudencia tiene que llevar a cabo la siempre difícil y delicada tarea de complementar el ordenamiento jurídico (art. 1.6 C. Civil), -reducido prácticamente, en nuestro caso, a los artículos 10.2, 18.3 y 96.1 CE y al art. 579.3 y 4 de la LECrim - rellenando las evidentes lagunas del mismo, habiendo acudido fundamentalmente para ello a la doctrina del Tribunal Constitucional y a la emanada del Tribunal Europeo de Derechos Humanos, hasta poder ofrecer hoy día a los operadores jurídicos un cuerpo de doctrina que llega a cubrir en buena medida las exigencias del principio de seguridad jurídica (art. 9.3 CE)*».

[224] *Ley 59/2003, de 19 de diciembre*, *de firma electrónica*, pubblicata in BOE del 20 dicembre 2003 n. 304, https://www.boe.es/buscar/act.php?id=BOE-A-2003-23399.

[225] Art. 3.5 e 3.6, *Ley 59/2003:*
«*Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable. El documento electrónico será soporte de:*
a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.
b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.
c) Documentos privados».

[226] *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza,* in BOE n. 298 del 12 novembre 2020.

[227] «*A los efectos de este Código se considera documento todo soporte material que exprese e incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica*», *Ley Orgánica*

È possibile notare una differenza tra le due norme: mentre la *Ley* 59/2003 considera documento l'informazione archiviata in un supporto, il codice penale ritiene che il documento sia proprio il supporto su cui sono incorporati dati o fatti.

Ad ogni modo, l'acquisizione al processo di tali elementi avverrà attraverso il supporto su cui i dati o le informazioni sono incorporate.

L'ingresso, all'interno del processo penale, del documento elettronico è espressamente previsto dall'art. 299.3[228] della *Ley de Enjuiciamento Civil*[229] (LEC – *Ley 58/2000*), cui si fa tutt'ora riferimento per analogia in assenza di una precisa regolamentazione in ambito penale[230].

L'utilizzo di tale mezzo di prova, pur se non espressamente regolato dal *Código penal*, è infatti legittimato, da un lato, dall'art. 24.2 della Costituzione spagnola, nella parte in cui sancisce il diritto degli individui a utilizzare i mezzi di prova pertinenti per la loro difesa[231] e, dall'altro, dall'art. 230.1 della *Ley Organica del Poder Judicial*[232] (LOPJ) che sancisce l'obbligo per giudici e i *Fiscales* di utilizzare qualunque mezzo tecnico, elettronico, informatico o telematico a loro disposizione per lo svolgimento delle proprie funzioni, con le limitazioni previste dalla legge[233].

3.3. L'intervento riformatore della Ley Orgànica 13/2015

La necessità di offrire una base giuridica alle attività di indagine a carattere tecnologico è stata colmata attraverso l'emanazione della *Ley Orgànica* del 5 ottobre 2015 n. 13 (LO 13/2015) [234], che ha recepito gli orientamenti giurisprudenziali maturati in ambito nazionale e sovranazionale.

10/1995, de 23 de noviembre, del Código Penal, pubblicata in BOE del 22 novembre 1995 n. 281, https://www.boe.es/eli/es/lo/1995/11/23/10/con .

[228] «*También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso*».

[229] *Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil*, pubblicata in BOE del 08 gennaio 2000 n. 7, https://www.boe.es/eli/es/l/2000/01/07/1/con .

[230] Art. 4 LEC: «*En defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, serán de aplicación, a todos ellos, los preceptos de la presente Ley*».

[231] Art. 24.2 *Constitución española*: «*Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia*».

[232] *Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial*, pubblicata in BOE del 02 luglio 1985 n. 157, https://www.boe.es/eli/es/lo/1985/07/01/6/con

[233] DELGADO MARTIN J., *La prueba digital. Concepto, clases, aportación al proceso y valoración,* cit.

[234] *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*, pubblicata in BOE del 06 ottobre 2015 n. 239, https://www.boe.es/eli/es/lo/2015/10/05/13. Per

Nel preambolo è chiaramente espressa l'esigenza di rafforzare i diritti in conformità al diritto comunitario e di regolare gli aspetti delle investigazioni tecnologiche in relazione al diritto all'intimità, al segreto delle comunicazioni e alla protezione dei dati personali.

Tra i principali meriti di questa legge vi è l'introduzione, all'interno della LECRIM, di un pacchetto di atti di indagine di natura tecnologica conformi ai principi costituzionali, mediante un bilanciamento tra esigenze di certezza giuridica, tutela dei diritti e innovazione tecnologica.

Nello specifico, all'interno del Titolo VIII della LECRIM[235] relativo agli atti di indagine che incidono sui diritti sanciti dall'art. 18 della Costituzione, sono stati introdotti sette nuovi capitoli:

- Capitolo IV "Disposizioni comuni alle intercettazioni di comunicazioni telefoniche e telematiche, captazione e registrazione di comunicazioni orali attraverso dispositivi elettronici, utilizzo di dispositivi tecnici per la ripresa di immagini, sorveglianza e localizzazione, perquisizione di dispositivi di archiviazione di informazioni e perquisizioni a distanza di dispositivi informatici" [236].
- Capitolo V "Intercettazioni di comunicazioni telefoniche e telematiche" [237].
- Capitolo VI "Captazione e registrazione di comunicazioni orali attraverso dispositivi elettronici" [238].
- Capitolo VII "Utilizzo di dispositivi tecnici per la ripresa di immagini, sorveglianza e localizzazione[239].
- Capitolo VIII "Perquisizione di dispositivi di archiviazione di massa[240].

---

approfondimenti CEDEÑO HERNÁN, M. (a cura di), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, 2017; PÉREZ GIL, J., *Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución*, in BRIGHI R., PALMIRANI M., SÁNCHEZ JORDÁN M.E. (a cura di), *Informatica giuridica e informatica forense al servizio della società della conoscenza: scritti in onore di Cesare Maioli,* Aracne Editrice, 2018, p. 187; RAYÓN BALLESTEROS M. C., *Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015*, in *Anuario Jurídico y Económico Escurialense*, 2019, 52, p. 197.

[235] «*De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*».

[236] «*Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos*». LECRIM, art. 588 *bis* a) ss.

[237] «*La interceptación de las comunicaciones telefónicas y telemáticas*», LECRIM, art. 588 *ter* a) ss.

[238] «*Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos*», LECRIM, art. 588 *quater* a) ss.

[239] «*Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización»,* LECRIM, art. 588 *quinquies* a) ss.

[240] «*Registro de dispositivos de almacenamiento masivo de información*», LECRIM, art. 588 *sexies* a) ss. Per approfondimenti FERNÁNDEZ RODRÍGUEZ A.P., *Algunas consideraciones a partir de la regulación del registro de dispositivos de almacenamiento masivo de la información*, in *Diario La Ley* , 2019, 9433.

- Capitolo IX "Perquisizione a distanza di dispositivi informatici"[241].
- Capitolo X "Misure di garanzia" [242] .

In tal modo, il legislatore è intervenuto su aspetti strettamente correlati ai diritti dell'individuo, fino a quel momento lasciati alla discrezione del formante giurisprudenziale, in ragione dell'assenza di un quadro giuridico chiaro.

Di rilievo è l'affermazione, per tutte le misure, della riserva di giurisdizione, in virtù della quale l'adozione è vincolata alla previa autorizzazione giudiziaria, mediante un'ordinanza motivata, che può essere adottata d'ufficio o su richiesta del *Fiscal* o della polizia giudiziaria.

Trasponendo, inoltre, gli orientamenti giurisprudenziali[243], il legislatore ha vincolato l'adozione di tali misure al rispetto dei principi di specialità, idoneità, eccezionalità, necessità e proporzionalità[244], dei quali occorrerà dare conto in relazione al singolo caso.

In merito al principio di proporzionalità, questo implica un giudizio di ponderazione che include la verifica di tre requisiti: idoneità, ovvero se la misura è adeguata a raggiungere l'obiettivo perseguito; necessità, se lo svolgimento di questa è essenziale e non esista altra misura meno gravosa ma ugualmente valida a raggiungere il risultato perseguito;

---

[241] «*Registros remotos sobre equipos informáticos*», LECRIM, art. 588 *septies* a) ss.
[242] «*Medidas de aseguramiento*», LECRIM, art. 588 *octies*.
[243] Sentencia del Tribunal Constitucional (STC) 23 febbraio 1991 n. 50, ECLI:ES:TC:1995:50; STC 8 maggio 1995 n. 1995, ECLI:ES:TC:1995:66; STC 16 dicembre 1996 n. 207, ECLI:ES:TC:1996:207; STC 22 marzo 1999 n. 44, ECLI:ES:TC:1999:44; STC 3 aprile 2002 n. 70, ECLI:ES:TC:2002:70; STC 28 ottobre 2014 n. 145, ECLI:ES:TC:2014:145. V. BLANCO A.E., *La jurisprudencia del Tribunal Constitucional español sobre el principio de proporcionalidad en el proceso penal*, in *Anuario de derecho penal y ciencias penales*, 2021, 1, p. 707.
[244] LECRIM, art. 588 *bis* a) «*2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.*
3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.
4. En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:
a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o
b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.
5. Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho».

proporzionalità "in senso stretto"[245], se il rapporto tra i benefici perseguiti e i beni o valori pregiudicati sia bilanciato[246].

Bisogna evidenziare come il legislatore non abbia inserito un catalogo di delitti che legittima l'adozione di tali mezzi d'indagine; per questa ragione *la Fiscalía General*, nella Circolare 5/2019[247], ha ritenuto che sia compito del giudice giustificare la misura nel caso concreto, tenendo conto non solo della gravità del delitto, ma anche del bene giuridico protetto.

Il decidente, pertanto, sarà chiamato a vagliare la gravità del fatto, l'ambito tecnologico di produzione, l'intensità degli indizi esistenti e la rilevanza del risultato perseguito in relazione alla restrizione dei diritti in causa.

Il legislatore ha poi disciplinato ulteriori aspetti, stabilendo periodi di durata massima delle misure e delle eventuali proroghe e ha altresì tenuto conto dei diritti dei terzi coinvolti, in modo da non lasciare eccessivi margini alla discrezionalità degli operatori, in ragione dell'esigenza di un adeguato bilanciamento tra istanze di persecuzione e tutela dei diritti, in special modo quelli sanciti dall'art. 18 della Costituzione (il diritto all'intimità personale e familiare, il diritto alla propria immagine, l'inviolabilità del domicilio, il diritto al segreto delle comunicazioni e il diritto all'autodeterminazione in ambito informatico).

Preme, tuttavia, sottolineare come la LO 13/2015, pur avendo disciplinato in maniera precisa i nuovi atti di indagine, non abbia introdotto nell'ordinamento spagnolo una nozione di prova digitale.

Per molti aspetti è, tutt'ora, necessario fare riferimento *alla Ley de Enjuiciamento Civil* (LEC) e l'introduzione della prova digitale nel processo penale, come si dirà di qui a poco, avviene sulla scorta della disciplina dettata per i mezzi di prova già esistenti, in base alle esigenze del caso concreto.

3.3.1 L'acquisizione di dati elettronici

La *Ley* 13/2015 assume altresì rilievo per avere inserito, nella LECRIM, una definizione di "dati elettronici", seppur esclusivamente riferita ai dati di traffico o associati e, pertanto, unicamente riconducibili allo svolgimento di comunicazioni.

---

[245] Per approfondimenti NAVARRO FRIAS I., *El principio de proporcionalidad en sentido estricto: ¿principio de proporcionalidad entre el delito y la pena o balance global de costes y beneficios?,* in *InDret,* 2010, 2.
[246] SÀNCHEZ RUBIO A., *El principio de proporcionalidad en las medidas de investigación tecnológica*, p.62 in PEREIRA PUIGVERT S., ORDÓÑEZ PONZ F., PESQUEIRA ZAMORA M. J. (a cura di), *Investigación y proceso penal en el siglo XXI. Nuevas tecnologías y protección de datos,* Aranzadi, 2021.
[247] *Circular 5/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre sobre registro de dispositivos y equipos informáticos*, pubblicata in BOE del 20 marzo 2019 n. 70, https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4244 .

In particolare, l'art. 588 *ter* b) indica come dati elettronici di traffico o associati tutti i dati generati dallo svolgimento di una comunicazione attraverso reti di comunicazione elettronica o dall'utilizzo di servizi di società di informazione o comunicazione telematica di natura similare[248].

Tuttavia, già con la *Ley* 25 del 18 ottobre 2007 (*Ley* 27/2007) [249] il legislatore aveva disciplinato la conservazione dei dati relativi a comunicazioni elettroniche e a reti pubbliche di comunicazione in relazione alla persecuzione dei reati.

L'art. 1 di questa legge prevede espressamente che i dati possano essere consegnati solo ai soggetti autorizzati, in virtù di un'autorizzazione giudiziaria e ai soli fini della individuazione, investigazione e persecuzione dei delitti gravi, ovvero puniti con le pene gravi stabilite dall'art. 33.2[250] del *Código penal* e tra le quali, in relazione alla reclusione, si individuano l'ergastolo e la reclusione superiore a 5 anni.

Il legislatore ha, inoltre, elencato alcune tipologie di dati utili per le indagini e di cui era richiesta la conservazione ai prestatori di servizi di comunicazione elettronica.

L'art. 3 della suddetta legge distingue come "*dato objetos de conservación*" i dati necessari a:

- tracciare e identificare l'origine di una comunicazione (numero di telefono, nome ed indirizzo dell'utente a cui è assegnato un determinato numero o un indirizzo IP);
- identificare il destinatario di una comunicazione (numero telefonico dei destinatari di una chiamata, nome ed indirizzo degli utenti registrati e l'identificazione del destinatario di una comunicazione);

---

[248] «*A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga*».

[249] *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones,* pubblicata in BOE del 19 ottobre 2007 n. 251, https://www.boe.es/eli/es/l/2007/10/18/25/con.

[250] «*Son penas graves:*
a) La prisión permanente revisable.
b) La prisión superior a cinco años.
c) La inhabilitación absoluta.
d) Las inhabilitaciones especiales por tiempo superior a cinco años.
e) La suspensión de empleo o cargo público por tiempo superior a cinco años.
f) La privación del derecho a conducir vehículos a motor y ciclomotores por tiempo superior a ocho años.
g) La privación del derecho a la tenencia y porte de armas por tiempo superior a ocho años.
h) La privación del derecho a residir en determinados lugares o acudir a ellos, por tiempo superior a cinco años.
i) La prohibición de aproximarse a la víctima o a aquellos de sus familiares u otras personas que determine el juez o tribunal, por tiempo superior a cinco años.
j) La prohibición de comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el juez o tribunal, por tiempo superior a cinco años.
k) La privación de la patria potestad».

- determinare data, ora e durata (data e ora dell'inizio e della fine di una chiamata, dell'accesso a *internet* e della disconnessione, indirizzo IP, e identificazione dell'utente, *log in* e *log out* del servizio di posta);
- identificare il tipo di comunicazione (servizio utilizzato, tipo di chiamata, servizi di messaggistica o di invio di file multimediali);
- identificare il dispositivo di comunicazione degli utenti (numero di telefono di origine e destinazione della comunicazione, numero IMSI o IMEI del chiamante, IMSI del destinatario, data e ora dell'attivazione di un servizio prepagato e cella a cui si è agganciato il soggetto per attivare il servizio);
- localizzare il dispositivo utilizzato (identificazione della cella).

Con l'introduzione del Capitolo V del Titolo VIII della LECRIM, è stato poi disciplinato l'accesso ai dati elettronici attraverso nuove misure.

L'acquisizione dei dati di traffico e associati è regolata da un doppio binario, il cui *discrimen* è dato dalla connessione con il diritto alla segretezza delle comunicazioni. In caso di interferenza con tale diritto, infatti, le norme prevedono la necessità di un'autorizzazione del giudice.

La *Ley* 13/2015 permette, anzitutto, di distinguere tra:

- acquisizione dei dati in connessione con lo svolgimento dell'attività di intercettazione;
- acquisizione dei dati in modalità indipendente dall'attività di intercettazione, di cui è possibile fare un'ulteriore distinzione tra:
  - dati connessi ad una comunicazione,
  - dati non connessi ad una comunicazione.

I principali atti che permettono di ottenere dati elettronici sono: l'acquisizione in connessione con lo svolgimento di intercettazioni[251], l'acquisizione di dati relativi allo svolgimento di comunicazioni, conservati dai prestatori di servizi[252], l'accesso a dati necessari per l'identificazione a partire dall'indirizzo IP[253], l'identificazione di dispositivi e apparecchiature a partire dal codice IMSI e IMEI[254].

[251] LECRIM, Art. 588 *ter* a) e b).
[252] LECRIM, Art. 588 *ter* j).
[253] LECRIM, Art. 588 *ter* k).
[254] LECRIM, Art. 588 *ter* l) e m).

L'acquisizione di dati contestualmente allo svolgimento delle intercettazioni deve essere disposta dal giudice nell'ordinanza di autorizzazione, indicando espressamente quali dati in concreto siano necessari[255].

La *Fiscalía General*, nella Circolare 2/2019, ha precisato che questo "ampliamento" del contenuto delle intercettazioni richiede una specifica motivazione e giustificazione in ragione della rispondenza ai principi di idoneità, necessità, eccezionalità e proporzionalità.

Il disposto della norma mirava a contrastare un fenomeno ampiamente diffuso che consisteva nell'inclusione sistematica, negli atti autorizzativi delle intercettazioni, di tutti i dati di traffico o associati che potevano essere reperiti dall'operatore telefonico, senza alcun fondamento legittimo che giustificasse tale ingerenza[256].

Quanto ai dati conservati negli archivi dei prestatori di servizio, la loro acquisizione riguarda elementi connessi allo svolgimento di comunicazioni e che siano stati mantenuti per adempiere alla normativa di conservazione dei dati, per fini di natura commerciale o di altro tipo.

Trattandosi di comunicazioni, questi dati potranno essere richiesti previa autorizzazione giudiziaria, quando risultino indispensabili per le indagini, purché sia specificata la tipologia di dati richiesti e le ragioni che ne giustifichino la domanda.

L'art. 588 *ter* k) disciplina, invece, l'identificazione di un utente allorquando, nell'esercizio delle proprie funzioni, gli agenti di polizia giudiziaria entrino in possesso di un indirizzo IP utilizzato per la commissione di un delitto e questo non permetta di accedere alla localizzazione del dispositivo né ai dati personali dell'utente.

In questo caso, la polizia giudiziaria può rivolgersi al *Juez de Instrucciòn* affinché chieda la cessione dei dati ai prestatori di servizio e alle persone fisiche soggette al dovere di collaborazione, *ex* art. 588 *ter* e), per localizzare il dispositivo in uso e identificare il sospettato.

A parere della *Fiscalía General*, quando è possibile risalire all'indirizzo IP senza il supporto del *provider*, non sarà necessaria alcuna autorizzazione giudiziaria.

Questa sarà, invece, necessaria allorquando si debba richiedere la collaborazione del prestatore di servizi per ricollegarvi l'identità di un soggetto o un dispositivo. L'indirizzo IP,

---

[255] LECRIM, art. 588 *ter* d), 2 d).

[256] Vedasi anche *Sentencia del Tribunal Supremo (STS), Sala de lo penal*, 06 aprile 2011, n. 316, ECLI:ES:TS:2011:2659 : «*Toda decisión judicial que acuerde, además de las escuchas telefónicas de los sospechosos, el control por la policía de otros datos generados durante la conversación, pero con incidencia sustantiva en el ámbito definido por el art. 18 de la CE, ha de motivar, con el mismo nivel de exigencia que venimos imponiendo para validar las escuchas, las razones que explican y legitiman el sacrificio añadido de otros aspectos íntimamente ligados a la privacidad*».

infatti, non è in grado *per se* di identificare un soggetto, conformemente a quanto già espresso dal *Tribunal Supremo*[257].

La giurisprudenza ha, peraltro, chiarito più volte che non è necessaria l'autorizzazione giudiziaria per accedere ad un indirizzo IP, specialmente quando sia accessibile pubblicamente; sarà invece necessario richiederla per collegarlo a dati personali dell'utente utili all'identificazione, attraverso il supporto del prestatore di servizi[258], come evidenziato dalla Sentenza del *Tribunal Supremo* 680/2010 del14/07/2010 [259].

Così come per l'indirizzo IP, la polizia può, inoltre, avvalersi di artifici tecnici per conoscere i codici IMSI o IMEI dei dispositivi da cui il soggetto ha effettuato l'accesso alla rete. Per l'ottenimento di tali codici, in ossequio all'art. 588 *ter* l), non è richiesta l'autorizzazione del giudice, dal momento che non si ha una restrizione del diritto al segreto delle comunicazioni, né una significativa ingerenza nei diritti individuali.

Questa sarà necessaria, come nel caso dell'indirizzo IP, qualora si voglia avere dai fornitori di servizi un riscontro sull'identità dell'utente e sui dispositivi in uso[260].

---

[257]Cfr. STS 28 maggio 2008, n. 292, ECLI:ES:TS:2008:3346 e STS, 18 novembre 2008, n. 776, ECLI:ES:TS:2008:6639.

[258] STS 9 maggio 2008, n. 236, ECLI:ES:TS:2008:1932: «*Visto el panorama jurisprudencial y legislativo y trasponiéndolo al caso que nos ocupa se puede concluir lo siguiente: los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IPS (Internet protocols) que habían accedido a los "hash" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada - como puntualiza con razón el Mº Fiscal - queda registrada siempre y ello lo sabe el usuario*».

[259] STS , 14 luglio 2009, n. 680, ECLI:ES:TS:2010:3944:
«*a) los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IPS (Internet protocols) que habían accedido a los "hush" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada queda registrada siempre y ello lo sabe el usuario. b) entender que conforme a la legalidad antes citada (...) se hace preciso, sin embargo, acudir a la autorización del juez instructor para desvelar la identidad de la terminal, teléfono o titular del contrato de un determinado IP, en salvaguarda del derecho a la intimidad personal (habeas data)*».

[260] *Circular* 2/2019 della *Fiscalía General:* «*En este proceso, al igual que ocurría con la dirección IP, pueden distinguirse dos momentos; uno, cuando se recogen los datos técnicos de identificación por medio del escáner y, otro, cuando esos datos técnicos, después de ser cruzados con los conservados por las operadoras de telefonía, permiten identificar una línea telefónica y el resto de los datos que ello conlleva. Pues bien, nuevamente aquí, el precepto lo que realmente regula es la posibilidad de que la Policía Judicial pueda obtener los datos técnicos por medio del escáner sin necesidad de recabar previamente autorización judicial. Su fundamento es el mismo que antes se exponía: esos datos técnicos –fundamentalmente el IMSI y el IMEI-, no permiten la identificación de persona alguna. Solo el trámite posterior con la operadora será lo que posibilite esa identificación y de ahí que la autorización judicial sea necesaria STS n.º 249/2008, de 20 de mayo, señalando la Circular 1/2013: «El TS tiene declarada la legitimidad de que sea la propia Policía la que los obtenga –los datos técnicos, concretamente, el IMSI y el IMEI– por sí misma y por sus medios técnicos en la medida que con ellos se desconoce incluso el número telefónico concernido, y las llamadas que pudieran recibirse y efectuarse, y, por supuesto se desconoce igualmente las conversaciones (SSTS n.º 1115/2011, de 17 de noviembre, 79/2011, de 15 de febrero; 249/2008, de 20 de mayo; 776/2008, de 18 de noviembre). Sin embargo, no puede la Policía solicitar tal información de las operadoras», recordando más adelante el contenido de la STS 249/2008, cuando señalaba que «así como la recogida o captación técnica del IMSI no necesita autorización judicial, sin embargo, la obtención de su plena funcionalidad, mediante la cesión de los*

A partire da tali numeri, sarà poi possibile richiedere l'autorizzazione per lo svolgimento delle intercettazioni, specificando nella richiesta attraverso quali mezzi è stato identificato il numero IMSI o IMEI, al fine di garantire un maggior controllo da parte del giudice ed una maggior trasparenza.

La *Fiscalía General* precisa che tale articolo disciplina i casi in cui, a partire dai codici si voglia effettuare un'intercettazione, e non invece la circostanza in cui si voglia semplicemente identificare un dispositivo, disciplinata dall'art. 588 *ter* m).

Tale ultimo articolo, invece, disciplina il caso in cui il *Fiscal* o la Polizia giudiziaria richiedano ai prestatori di servizio l'accesso ai dati utili a identificare un utente, a partire dal numero di telefono o da un codice riconducibile ad ogni tipo di dispositivo.

In proposito, la Corte di Giustizia[261] ha affermato che «l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dai suddetti articoli della Carta, che non presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave».

La previsione, inoltre non si considera limitata ai dati che riguardano la titolarità di un numero di telefono o, viceversa, il conseguimento di un numero di telefono a partire dai dati di un soggetto. Deve, infatti, considerarsi estesa ad ogni tipo di dato che permetta di identificare un utente o un dispositivo di comunicazione, ad eccezione di quelli connessi allo svolgimento di comunicazioni.

Come precedentemente esposto, pertanto, rientrano nell'ambito di applicazione di tale norma le richieste del numero IMSI associato a un determinato dispositivo, in vista della determinazione dell'utente.

Secondo quanto precisato dalla *Fiscalía General*, questa circostanza si è verificata più volte nei casi di furto di telefoni cellulari, per identificare il soggetto in possesso del dispositivo attraverso il numero IMSI della scheda SIM utilizzata dopo il furto.

Il numero IMSI non può, quindi, essere considerato come un dato di traffico e, pertanto, connesso a un processo di comunicazione, essendo semplicemente un codice di identificazione di ogni dispositivo di telefonia mobile.

---

datos que obran en los ficheros de la operadora, sí impondrá el control jurisdiccional de su procedencia». para el segundo momento del proceso, pero no para el primero».

[261] CGUE, 2 ottobre 2018, C-207/16, *Ministerio Fiscal.*

Da qui scaturirebbe la principale differenza con l'art. 588 *ter* l), finalizzato allo svolgimento delle intercettazioni[262].

Vieppiù, tale richiesta, conformemente all'orientamento della CGUE, potrà essere effettuata per qualunque delitto, purché nel rispetto dei principi di specialità, idoneità eccezionalità, necessità e proporzionalità.

3.3.2 L'applicabilità della disciplina generale delle intercettazioni all'acquisizione dei dati di traffico

La riforma del 2015, come detto, ha strutturato un apposito capitolo della LECRIM per enucleare le disposizioni comuni e i principi da seguire per lo svolgimento degli atti di indagine tecnologica, tra questi, spicca la previsione della necessaria autorizzazione giudiziaria (art. 588-*bis* a).

Allo stesso modo, l'obbligatorietà di tale autorizzazione è ribadita nuovamente all'art. 588-*ter* a), relativo alle intercettazioni telefoniche.

Tuttavia, questa condizione non sembra applicabile anche ai casi di accesso a dati non vincolati ad una comunicazione, poiché non vi sarebbe violazione del diritto al segreto delle comunicazioni *ex* art. 18.3 della Costituzione e, d'altronde, le stesse misure previste dagli art. 588-*ter* l) e 588-*ter* m) non prevedono un'autorizzazione del giudice.

Allorquando l'acquisizione dei dati non sia connessa ad un'attività di intercettazione, infatti, sarà possibile adottare una disciplina distinta in relazione alla connessione ad un'attività di comunicazione.

Nel primo caso sarà, pertanto, necessaria un'autorizzazione giudiziaria, a tutela del segreto delle comunicazioni.

---

[262] *Circular* 2/2019 della *Fiscalía General*: «*Se incluirían aquí, por ejemplo, los supuestos de solicitud del IMSI que aparece asociado a un determinado dispositivo electrónico, con el fin de determinar quién es el usuario de ese dispositivo electrónico. Este supuesto se ha venido planteando con cierta frecuencia en los casos de sustracción de teléfonos móviles con el fin de identificar a la persona que lo tenía en su poder mediante la identificación del IMSI de la tarjeta SIM que estaba siendo utilizada por el usuario del teléfono. El IMSI, en estos casos, no puede ser considerado como un dato de tráfico y, por lo tanto, vinculado a un proceso de comunicación, pues no se genera como consecuencia de una comunicación concreta, sino que se trata, en palabras de la STS n.º 249/2008, de 20 de mayo, de un código de identificación de cada dispositivo de telefonía móvil que sirve para posibilitar esa identificación a través de las redes GSM y UMTS; en consecuencia, puede fácilmente encuadrarse en el concepto de «dato identificativo de un medio de comunicación», que utiliza el art. 588 ter m. Se trata, por lo tanto, de un supuesto diferente al que regula el art. 588 ter l en el que, como antes se analizaba, será necesario recabar autorización judicial para relacionar ese IMSI con otros datos que posibiliten la identificación del usuario».*

Come già anticipato, nella sua circolare 2/2019 [263], la *Fiscalia General* ha ritenuto che l'art. 588-*bis* a) non sia applicabile neppure per la parte in cui stabilisce che le misure possano essere adottate solo in relazione ai delitti previsti dall'art. 579 1 LECRIM[264], ovvero:

- delitti dolosi puniti con limite massimo di almeno 3 anni di reclusione,
- delitti commessi in seno a gruppi o organizzazioni criminali, delitti di terrorismo,
- delitti commessi attraverso strumenti informatici o tecnologie di informazione o comunicazione[265].

Tale disposizione, tuttavia, sembrerebbe porsi in contrasto con la *Ley* 25/2007 che, nel disciplinare l'accesso ai dati, prevede, all'art. 1, questa possibilità solo in relazione ai delitti gravi.

Stando al disposto di tale articolo, pertanto, la disciplina delle intercettazioni, permesse anche per reati informatici non rientranti nel catalogo dei delitti gravi, determinerebbe un livello di tutela inferiore rispetto a quello approntato per la cessione dei dati di traffico, nonostante il maggior livello di intrusione e la violazione del diritto alla segretezza delle comunicazioni.

Contrariamente a questa interpretazione, secondo la *Fiscalía General*, i dati non connessi ad una comunicazione potrebbero essere richiesti anche al di fuori dei delitti indicati dall'art. 588-*bis* a) e in assenza di autorizzazione del giudice[266].

---

[263] *Circular 2/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas*, in BOE del 22 marzo 2019 n.70, https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4241.

[264] «**Artículo 579. De la correspondencia escrita o telegráfica.**
1. El juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes delitos:
1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
2.º Delitos cometidos en el seno de un grupo u organización criminal.
3.º Delitos de terrorismo».”

[265] ARRABAL PLATERO P., *Algunas cuestiones controvertidas sobre la obtención de datos de tráfico*, in ARRABAL PLATERO P., CONDE FUENTES J., GARCIA MOLINA P., SERRANO HOYO G., *La justicia digital en España y la Unión Europea,* Atelier Libros, 2019, p. 317.

[266] *Circular* 2/2019: «*Por otro lado, la regulación contenida en la Ley 25/2007 referente a la cesión de tales datos «a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales» (art. 1), debe entenderse superada por la contenida ahora en la LECrim cuando se trate de una medida de interceptación de comunicaciones, con lo que desaparecen todas las dudas interpretativas que se habían venido planteado, tales como el alcance de la gravedad del delito, el derecho fundamental afectado o la autoridad competente para requerir los datos. […] La incorporación al procedimiento de datos, tanto los vinculados como los no vinculados a un proceso de comunicación, podrá acordarse en relación con cualquier comportamiento delictivo, siempre que la medida aparezca justificada por la ponderación de los principios rectores en el caso concreto*».

A sostegno di tale tesi interpretativa, il *Tribunal Supremo*[267] aveva precedentemente stabilito che le prescrizioni della *Ley* 25/2007 si considerano sostituite dalle disposizioni sopravvenute con la *Ley Organica 13/2015*.

Pertanto, seguendo l'impostazione della LECRIM, si profilano due categorie di dati: quelli connessi allo svolgimento di una comunicazione, disciplinati dall'art. 588 *ter* j)[268] e tutti gli altri dati di traffico, di cui il legislatore ha regolamentato i codici IMSI ed IMEI – i dati che permettono di identificare il soggetto titolare di un numero di telefono o il numero di telefono di uno specifico soggetto, attraverso gli articoli 588 *ter* l) ed m).

Il disposto della LECRIM evidenzia come, per i dati connessi ad una comunicazione, sia necessaria l'autorizzazione del giudice, secondo il sistema della *Ley* 25/2007.

Tuttavia, non tutti i dati indicati dall'art. 3 di tale legge – relativo ai *datos objetos de conservaciòn* – sono specificatamente connessi a comunicazioni concrete, ragion per la quale il legislatore ha preferito disciplinare espressamente i casi in cui non ritenga necessaria l'autorizzazione del giudice e slegarli da tale disciplina.

Conseguentemente, secondo quando chiarito dalla *Fiscalía General,* sarà necessaria l'autorizzazione per tutti i dati indicati dalla *Ley* 25/2007, a eccezione di quelli espressamente disciplinati dagli art. 588-*ter* j) ed m) della LECRIM.

3.3.3. Il dovere di collaborazione dei provider

Gli articoli 588-*ter* e) e 588-*septie*s b) LECRIM disciplinano il dovere di collaborazione dei *provider* in relazione, rispettivamente, alle intercettazioni di comunicazioni e alla perquisizione informatica a distanza[269]. In entrambi i casi, tale collaborazione sarà vincolata all'esistenza dei presupposti prescritti dalla legge e alla sussistenza di uno dei delitti indicati per ciascuna delle misure in questione[270].

L'articolo 588 *ter* e) stabilisce il dovere di collaborazione dei prestatori di servizi di telecomunicazione, di accesso a una rete di telecomunicazioni o di servizi, delle società di

[267] STS*,* 07 luglio 2017, 52372017, ECLI:ES:TS:2017:2968.

[268] Ad eccezione del caso previsto dall'art. 588-*ter* k) in relazione all'indirizzo IP.

[269] LARO GONZALÈZ M. E., *Prueba electrónica: situación actual en el proceso penal y perspectivas en el futuro,* p. 246 ss., in ARRABAL PLATERO P., CONDE FUENTES J., GARCIA MOLINA P., SERRANO HOYO G., *La justicia digital en España y la Unión Europea*, cit.

[270] Nel caso del *registro remoto*: delitti commessi in rapporto ad organizzazioni criminali, delitti di terrorismo, delitti commessi contro minori o persone con disabilità, delitti contro la costituzione di tradimento e relativi alla difesa nazionale, delitti commessi attraverso strumenti informatici o altre tecnologie dell'informazione o della comunicazione o servizio di comunicazione.

informazioni[271], e di ogni persona che per qualunque motivo contribuisca a rendere possibili le comunicazioni attraverso un telefono o qualunque altro mezzo o sistema di comunicazione telematica logica o virtuale.

Tali soggetti sono obbligati a fornire al giudice, al *Fiscal* e agli agenti di Polizia la loro assistenza e collaborazione per permettere il compimento degli atti di intercettazione e a mantenere il segreto sull'attività che gli viene richiesta.

Come precedentemente esposto, i dati elettronici che siano correlati ai processi di comunicazione potranno essere ceduti solo attraverso un'autorizzazione giudiziaria.

Conformemente all'art. 2.4[272] della *Ley* 34/2002, i prestatori di servizi sono soggetti alle obbligazioni imposte dall'ordinamento spagnolo quando siano stabiliti nel territorio spagnolo, secondo i criteri stabiliti dall'art. 2[273].

Tale disposizione permette di individuare due criteri per determinare se un prestatore di servizi abbia uno stabilimento in Spagna: quando la sede fisica in cui ha luogo la gestione amministrativa centrale si trovi in territorio spagnolo o quando, pur avendo sede legale in un altro Stato, vi sia nel territorio spagnolo una sede fisica, abituale o continuativa, in cui si realizza l'attività, tutta o in parte. Si presume, inoltre, che il *provider* sia stabilito in Spagna quando è iscritto nel *Registro Mercantil* o in un altro registro pubblico spagnolo necessario per ottenere la personalità giuridica.

L'art. 588-*septies* b) è collocato all'interno del capitolo IX, che riguarda perquisizioni a distanza su dispositivi informatici (*registro remoto*[274]), e sancisce il dovere di collaborazione degli stessi soggetti già indicati all'articolo 588-*ter* e) e dei proprietari o responsabili di un sistema informatico o di una banca dati che siano oggetto di una perquisizione.

---

[271] *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*, pubblicata in BOE del 12 febbraio 22 n. 166. L'esposizione dei motivi nella legge, nel suo paragrafo, chiarisce che questa adotta un concetto ampio di servizi della società di informazione, che comprende servizi di contrattazione di beni e servizi per via elettronica, somministrazione di informazioni per via elettronica, attività di intermediazione per l'accesso alla rete, trasmissione di dati attraverso reti di telecomunicazioni, realizzazione di copie temporanee di pagine Internet richieste dagli utenti, allocazione nei propri server di informazioni, servizi o applicazioni o messa a disposizione di strumenti di ricerca o di collegamenti ad altri siti Internet, così come qualunque altro servizio che si presti alle richieste individuali degli utenti, purché rappresenti un'attività economica per il *provider*. Questi servizi sono offerti dagli operatori di telecomunicazioni, i *provider* di accesso a Internet, i portali, i motori di ricerca o qualunque altro soggetto che disponga di un sito Internet attraverso il quale realizzare alcune delle attività indicate, incluso il commercio elettronico.

[272] «*Los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización*».

[273] *Ley 34/2002.*

[274] Per un approfondimento BACHMAIER WINTER L., *Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015*, in *Boletìn del Ministerio de Justicia*, 2017, n. 2195.

Questi soggetti sono obbligati a collaborare con gli agenti di polizia per lo svolgimento della perquisizione e l'accesso al sistema informatico e dovranno fornire l'assistenza necessaria affinché i dati e le informazioni raccolte possano essere successivamente visualizzati ed esaminati[275].

Nei casi di delitti di minor gravità e/o di dati indipendenti dall'attività di intercettazione o in possesso dei prestatori di servizio, il dovere di collaborazione è invece disciplinato dagli artt. 588-*ter* j) e 588 *ter* m).

Nel primo caso, previa autorizzazione giudiziaria, quando risulti indispensabile per le indagini, si potranno richiedere ai *provider* le informazioni da questi conservati.

Invece, *ex* art. 588-*ter* m), anche in assenza di autorizzazione giudiziaria, sarà possibile richiedere agli stessi i dati utili per indentificare utenti o dispositivi. I *provider* dovranno collaborare per non incorrere nel delitto di disobbedienza.

Per ottenere dati conservati nel *cloud*, le autorità potrebbero ricorrere al *registro remoto* richiedendo una collaborazione ai sensi dell'art. 588 *septies* b).

Tale misura, tuttavia, è prevista solo per specifiche tipologie di delitti:

- criminalità organizzata,
- terrorismo,
- delitti commessi contro minori o persone con capacità ridotta,
- delitti contro la Costituzione, di tradimento o relativi alla sicurezza nazionale.
- delitti commessi attraverso dispositivi informatici o altri tipi di tecnologie informatiche o telematiche o servizi di comunicazione.

Nel caso di dati appartenenti ad un sistema di *Internet of Things*, come Amazon Alexa, anziché richiedere la collaborazione dei *provider*, si può ricorrere alla disciplina della perquisizione *ex* art. 588 *sexies* a)[276] .

---

[275] LECRIM, art. 588 *septies* b) co. 1 e 2: «*Los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización. Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia*».

[276] «***Artículo 588 sexies a. Necesidad de motivación individualizada.***

1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente».

Nello specifico, quando durante una perquisizione nel domicilio la polizia entri in possesso di un dispositivo, potrà richiedere un ampliamento dell'autorizzazione del giudice per accedere al contenuto dell'apparecchio.

Nel caso di Alexa, si potrebbe così accedere alle registrazioni effettuate dai dispositivi, che sono disponibili all'interno dell'*app* scaricata nello *smartphone*.

Qualora, invece, le autorità non siamo in possesso del dispositivo o non possano svolgere una perquisizione a distanza attraverso *malware*, l'unica opzione è la richiesta al *provider*, dovendosi tuttavia valutare i profili che permettano di richiedere tali dati, specialmente quando il soggetto obbligato abbia sede legale in un altro Stato[277].

Non si può, tuttavia, sottovalutare il riflesso di tali indagini nella protezione dei diritti umani e le ricadute sul principio di proporzionalità, in relazione ai dati da acquisire. E infatti, come sottolinea parte della dottrina[278], le modalità con cui si ottengono i dati di un sistema informatico non permettono di individuare agevolmente quelli rilevanti, ma prevedono un'acquisizione indiscriminata di tutto il contenuto.

3.4. L'introduzione della prova digitale nel processo

Ai sensi dell'art. 311 LECRIM[279], il *Juez de Instrucción* si occuperà, nella fase di istruzione, dello svolgimento degli atti di indagine proposti dal *Ministerio Fiscal* o dalle parti, sempre che non siano irrilevanti o pregiudizievoli.

Al momento del dibattimento, il *Ministerio Fiscal* e le parti proporranno le prove da acquisire negli *escritos de califición provisional*, i cosiddetti *escritos de acusación y defensa*[280], nel quale verranno inseriti gli elenchi dei testimoni e periti ed ulteriori prove richieste. Il Giudice potrà ammettere o rifiutare le prove, con apposito "*auto judicial*".

Si può, inoltre, fare riferimento alle disposizioni della LEC che si applicano in via sussidiaria. L'art. 299.2 LEC[281] stabilisce, infatti, che saranno ammessi i mezzi di

---

[277] RODRIGUEZ ÁLVAREZ A., *Alexa, ¿quién es el culpable? El uso de altavoces inteligentes como prueba en el proceso penal*, in PEREIRA PUIGVERT S., ORDÓÑEZ PONZ F., PESQUEIRA ZAMORA M. J. (a cura di), *Investigación y proceso penal en el siglo XXI. Nueva tecnologías y protección de datos*, Aranzadi, 2021, p. 192.

[278] BACHMAIER WINTER L., *Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica* 13/2015, cit., p. 28 ss.

[279] «*El Juez que instruya el sumario practicará las diligencias que le propusieran el Ministerio Fiscal o cualquiera de las partes personadas si no las considera inútiles o perjudiciales*».

[280] LECRIM, art. 626 co. 1:« *El Ministerio Fiscal y las partes manifestarán en sus respectivos escritos de calificación las pruebas de que intenten valerse, presentando listas de peritos y testigos que hayan de declarar a su instancia*».

[281] «*También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos,*

riproduzione di parole suoni e immagini e gli strumenti che permettono di archiviare o riprodurre parole, dati, numeri, o operazioni effettuate e rilevanti per il processo.

L'introduzione nel processo della prova digitale può avvenire attraverso più strumenti, tra loro cumulabili: la prova documentale (su supporto cartaceo o quale documento elettronico[282]), l'esame delle parti o la testimonianza, l'atto notarile, la perizia e il *reconocimiento judicia* o *inspección ocular* [283].

In quest'ultimo caso, il giudice – *Juez de instrucciòn* o il giudice del *juicio oral*, a seconda della fase – può accedere personalmente e in maniera diretta alla prova che la parte vuole introdurre, per esempio visionando in prima persona una pagina *web*.

Considerato, tuttavia, il rischio di alterazione di quanto estrapolato dal *web*, sarà possibile fare certificare anche attraverso un atto notarile il contenuto della pagina, così da dare contezza di eventuali modifiche e garantire che la pagina sia rimasta inalterata.

In merito alla prova documentale, il legislatore non ha previsto una lista dei supporti ammessi, anche se l'art. 26 del *Código Penal* rimanda a tutti i supporti materiali che incorporino dati, fatti o narrazioni con efficacia probatoria o qualunque altro tipo di rilevanza giuridica.

Riguardo alla prova digitale, il Tribunal Supremo[284] ha sancito la riconducibilità delle email alla prova documentale, ma un orientamento giurisprudenziale minoritario sostiene che questa non possa essere considerata una prova documentale e ciò, non solo per le varie modalità con cui una prova digitale può essere apportata al procedimento, ma anche in relazione al sistema di valutazione che, per i nuovi mezzi di prova, risponde al criterio della libera valutazione del giudice e alla sana critica.

Inoltre, si specifica come non si possa fare solo riferimento alla prova documentale qualificando la prova come documento elettronico, in quanto, la *Ley* 59/2003 stabilisce che

---

cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso».

[282]In questo caso il regime applicabile sarà quello della prova di strumenti elettronici disciplinato dall'articolo 299.2 LEC.

[283] Art. 326 LECRIM relativamente alla fase di "*instrucción*": «*Cuando el delito que se persiga haya dejado vestigios o pruebas materiales de su perpetración, el Juez instructor o el que haga sus veces ordenará que se recojan y conserven para el juicio oral si fuere posible, procediendo al efecto a la inspección ocular y a la descripción de todo aquello que pueda tener relación con la existencia y naturaleza del hecho*» e art. 727 LECRIM relativamente allá fase del *juicio oral*: «*Para la prueba de inspección ocular que no se haya practicado antes de la apertura de las sesiones, si el lugar que deba ser inspeccionado se hallase en la capital, se constituirá en él el Tribunal con las partes, y el Secretario extenderá diligencia expresiva del lugar o cosa inspeccionada, haciendo constar en ella las observaciones de las partes y demás incidentes que ocurran. Si el lugar estuviere fuera de la capital, se constituirá en él con las partes el individuo del Tribunal que el Presidente designe, practicándose las diligencias en la forma establecida en el párrafo anterior.*
En todo lo demás se estará, en cuanto fuere necesario, a lo dispuesto en el título V, capítulo I del libro II».

[284] STS, 23 luglio 2020, 706, ECLI:ES:TS:2020:2925.

un documento elettronico viene considerato tale solo quando vi sia apposta una firma elettronica.

Qualora la difesa impugni la prova digitale, esponendone i motivi nello scritto di difesa, l'accusa sarà obbligata a presentare una prova periziale informatica a sostegno della veridicità del contenuto dei messaggi, dei dati presentati e della mancata alterazione[285].

Ciò permetterà il rispetto di garanzie essenziali quali l'immediatezza, l'autenticità, l'integrità e il rispetto della catena di custodia, a tutela della veridicità della prova e dell'assenza di manipolazioni.

La mancanza di uno di questi o una falla nella catena di custodia, potrebbe infatti avere risvolti sull'affidabilità della prova. Tuttavia, ciò non impedirebbe di valutarla insieme alle altre prove, come le dichiarazioni testimoniali, dalle quali potrebbe essere completata o rafforzata.

Di fatto sembra che, nell'ordinamento spagnolo, al pari di quanto succede in altri sistemi, in assenza di un quadro preciso si utilizzino istituti talvolta datati per consentire l'acquisizione al processo della prova digitale.

Laddove, invece, come chiaramente evidenziato da parte della dottrina[286], sarebbe più opportuno disegnare una disciplina *ad hoc* che si adatti alle caratteristiche della prova digitale ed alle varie casistiche di acquisizione, valorizzandone le potenzialità.

---

[285] STS, *Sala de lo Penal,* 22 novembre 2021, 121, ECLI:ES:TS:2021:16734° : «*En los casos que la defensa impugne esta "prueba digital" en el escrito de defensa motiva y obliga a la acusación a proponer prueba pericial informática acerca de la veracidad del contenido de estos mensajes y que estos no han sido alterados*».

[286] MAGRO SERVET V., *¿Cómo aportar la prueba digital en el proceso penal*?, in *Diario La Ley*, n. 9824, *Secciòn Doctrina*, 7 de Abril, 2021, Wolters Kluwer: «*Porque hoy en día lo que estamos haciendo en el derecho probatorio es buscar un encaje en medios de prueba ya existentes para comprobar si podemos ponerle a la prueba digital el traje de otro medio de prueba donde pueda tener un cierto encaje forzado, cuando lo correcto desde el punto de vista de la corrección jurídica adaptada a los tiempos es crearle a la prueba digital un traje propio con el que se pueda vestir para acudir con un adecuado lenguaje procesal ad hoc al propio escenario del proceso penal bien vestida y con la verdadera autonomía que exige y merece la prueba reina que se está aportando en muchos procedimientos sin tener los operadores jurídicos la seguridad de cómo se aporta, en qué condiciones, plazos de preclusión, momentos procesales de su aportación, y lo que es más importante, cómo reproducirla en el juicio oral*».

CAPITOLO IV

Prova digitale e cooperazione giudiziaria: verso una nuova disciplina

La cooperazione giudiziaria in materia penale, nel corso degli anni, si è evoluta al fine di assicurare una più efficace repressione e persecuzione dei reati, al di là dei confini nazionali[287]. E invero, l'espansione della criminalità organizzata oltreconfine ha richiesto agli attori coinvolti nell'attività di contrasto di instaurare nuove modalità di collaborazione. Un processo che si è reso ancora più necessario in conseguenza dello sviluppo delle nuove tecnologie anche come strumenti per la commissione di attività criminose[288].

Nello specifico ambito della prova digitale, numerosi sono gli istituti ai quali si può fare ricorso per ottenere i dati in possesso dei *provider.*
Tra questi, è possibile menzionare: la *voluntary disclosure*; la rogatoria "tradizionale", per il tramite dell'autorità ministeriale; la rogatoria con trasmissione diretta, basata su accordi internazionali di *mutual legal assistance* (MLA); gli strumenti delineati dalla *Convenzione di Budapest*, tra i quali i "*production orders*" (*ex* art. 18) e il "*direct transborder access*" (art. 32); l'ordine europeo di indagine penale, regolato dalla direttiva 2014/41/UE, implementata in Italia dal d. lgs. n. 108/2017.

Come si avrà modo di meglio analizzare, nuovi "spazi di manovra" si profilano per merito del Secondo Protocollo della Convenzione di Budapest e del Regolamento sugli ordini europei di produzione e conservazione delle prove elettroniche.

Per meglio comprendere le criticità e le possibilità legate all'acquisizione della prova digitale in ambito transnazionale, sembra utile tracciare il percorso dei meccanismi di cooperazione giudiziaria riconducibili al Consiglio d'Europa e all'Unione europea, iniziando dalla c.d. "grande Europa".

---

[287] Per approfondimenti v. BELFIORE R., *La prova penale "raccolta" all'estero*, Aracne editrice, 2014; DELGADO MARTÍN J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer, 2016, p. 498; GERACI R. M., *Il mutuo riconoscimento nella cooperazione processuale: genesi, sviluppi, morfologiche*, Cacucci Editore, 2020; KOSTORIS E.R., *Manuale di procedura penale europea*, Giuffrè, 2019.
[288] Cfr. SPIEZIA F., *Cooperazione internazionale e tutela delle vittime nel cyberspazio*, in *Dir. Pen. Proc.*, 2022, 9, p. 1137

4.1. L'impulso del Consiglio d'Europa: dall'assistenza giudiziaria in materia penale al Secondo Protocollo della Convenzione di Budapest

4.1.1. La Convenzione di assistenza giudiziaria in maniera penale

Nell'ambito del Consiglio d'Europa, il primo strumento di rilievo è costituito dalla Convenzione di Strasburgo, firmata il 20 aprile 1959[289] dai 47 Stati membri del Consiglio d'Europa e da Cile, Israele e Repubblica di Corea, adottata con l'obiettivo di attuare un'unione più stretta tra i Paesi membri del Consiglio d'Europa.

Questa ha costituito la base dell'assistenza giudiziaria in materia penale ed ha, inoltre, rappresentato il prototipo per i successivi strumenti di assistenza, nonché per quelli di mutuo riconoscimento adottati nell'ambito dell'UE.

Il trattato, all'art. 1, dispone che le parti abbiano il dovere di «accordarsi reciprocamente l'assistenza giudiziaria più ampia possibile in qualsiasi procedura concernente reati, la cui repressione, al momento in cui l'assistenza giudiziaria è domandata, è di competenza delle autorità giudiziarie della Parte richiedente». È prevista un'eccezione al principio di reciprocità qualora i reati in questione vengano qualificati dal Paese richiesto come reati politici, connessi a reati politici, o reati fiscali e, inoltre, quando l'assistenza determini un *vulnus* alla sovranità, alla sicurezza, all'ordine pubblico o ad altri interessi essenziali dell'ordinamento dello Stato cui la richiesta è inoltrata (art. 2).

Al centro di questo sistema si pone la commissione rogatoria, intesa quale richiesta trasmessa dal Ministero di Giustizia del Paese richiedente al Ministero del Paese dal quale si voglia ottenere l'assistenza. Questa è, dunque, soggetta al filtro del potere esecutivo e, solo nei casi di urgenza, è previsto un contatto diretto tra le autorità giudiziarie.

Il principio adottato per lo svolgimento degli atti richiesti è quello del *locus regit actum* (art. 3), ai sensi del quale l'esecuzione dell'atto verrà effettuata secondo la legge dello Stato richiesto.

L'art. 26 della Convenzione prevede che «le Parti Contraenti potranno concludere fra esse accordi bilaterali o multilaterali relativi all'assistenza giudiziaria in materia penale soltanto per completare le disposizioni della presente Convenzione e per agevolare

[289] Convenzione europea di assistenza giudiziaria in materia penale, firmata a Strasburgo il 20 aprile 1959, consultata su https://rm.coe.int/1680065702 .

l'applicazione dei principi contenuti nella medesima». Tale sistema si è, tuttavia, rivelato inefficiente e non del tutto in grado di adattarsi alle nuove tecnologie, il cui utilizzo ha richiesto un ripensamento dei meccanismi di cooperazione in chiave di maggior rapidità e flessibilità.

L'evoluzione della cooperazione ha, infatti, determinato l'imporsi di nuovi principi guida quali il rapporto diretto tra autorità giudiziarie non mediato da autorità politiche, la celerità nelle procedure di cooperazione e l'assenza di formalità.

Tali principi, certamente, contrastano con la procedura definita dalla Convenzione.

Nello specifico, se l'autorità giudiziaria italiana volesse ottenere dei dati digitali utilizzando gli strumenti di mutua assistenza, dovrà anzitutto individuare lo Stato competente in relazione alla localizzazione dei *server* presso cui sono archiviati i dati[290].

Una volta individuato lo Stato – che dev'essere firmatario della Convenzione o comunque soggetto con il quale si ha un accordo bilaterale – seguirà l'invio di una rogatoria da parte del Ministro della Giustizia italiano all'omologo straniero; quest'ultimo, dopo aver esaminato la richiesta valuterà se sottoporla all'autorità giudiziaria.

A quel punto, l'autorità giudiziaria procederà all'acquisizione e alla successiva comunicazione degli esiti al Ministro di Giustizia, che rimetterà al suo omologo italiano, il quale a sua volta fornirà i dati all'autorità giudiziaria nazionale.

Già da questo breve quadro emergono alcune criticità: in primo luogo, risulta difficile, soprattutto con l'avvento del *cloud computing*, individuare con certezza il *server* e lo Stato in cui sono localizzati i dati. Occorre, infatti, considerare che a causa dello spostamento continuo dei dati operato dai *provider*, le autorità giudiziarie o di polizia si scontrano con la difficoltà di identificare in concreto il luogo in cui si colloca il dato[291].

Il procedimento si snoda, poi, attraverso una procedura particolarmente dispendiosa in termini di tempo, che varia tra 6 e 24 mesi, difficilmente conciliabile con la facile volatilità dei dati elettronici e, a volte, con i termini di *data retention* di un Paese[292].

---

[290] DE BUSSER E., *The digital unfitness of mutual legal assistance*, in *Security and human rights*, vol. 2017, 28, 1, p. 161.

[291] MAILLART J. B., *The limits of subjective territorial jurisdiction in the context of cybercrime*, in *ERA Forum*, 2018, 18: « *However, the problem lies in the fact that metadata are very often held by service providers outside the territory of the investigating law enforcement agency and therefore outside its jurisdiction and that, as detailed below, traditional cooperation mechanisms – direct transborder access and mutual legal assistance – are unfit to access and secure data stored in foreign jurisdictions in an effective and timely manner. To this must be added the fact that computer data are increasingly stored 'in the cloud' where the location of the data may be very difficult to determine at any point in time and that such cooperation mechanisms cannot be used in these circumstances».*

[292] DE BUSSER E., *The digital unfitness of mutual legal assistance*, cit., p. 163: «*Still, it seems as if the traditional mechanism of mla is losing ground quickly because of its slow and cumbersome way of working. With surveys showing that it takes authorities an average of ten months to react to a request for mla3 – in some cases, no reaction is received at all by the requesting authority – individual states, as well as the EU*

Le lunghe tempistiche, inoltre, complicano non solo l'ottenimento del dato, ma anche lo svolgimento di tutte le indagini connesse.

L'utilizzo della *lex loci* come parametro per l'acquisizione può, peraltro, generare casi di *forum shopping* allorquando possano essere individuati più Stati di esecuzione e quello richiedente decida di scegliere lo Stato che offre minori tutele sul versante dei diritti.

Ai sensi dell'art. 5 della Convenzione, inoltre, l'esecuzione della richiesta può essere soggetta al requisito della doppia incriminazione, determinando così un rifiuto in caso di variazioni relative alle fattispecie tra uno Stato e l'altro[293].

4.1.2. La Convenzione sul Cybercrime

La Convenzione sul *cybercrime*[294], firmata a Budapest il 23 novembre 2001, nasce dalla necessità di dover fronteggiare nuove modalità di realizzazione dei crimini che traggono vantaggio e forza dall'evanescenza del mondo digitale[295].

Il Consiglio d'Europa, nel *report*[296] esplicativo della Convenzione, specifica come il facile accesso e lo scambio di informazioni abbiano determinato cambi sociali ed economici senza precedenti.

Mentre i criminali si trovano in Paesi diversi da quelli in cui le loro azioni hanno effetto, le leggi nazionali sono generalmente confinate in uno specifico territorio[297].

---

institutions, have sought faster alternatives. Ten months is slow in any criminal investigation – even in a domestic setting – but it is unworkably slow when the evidence is digital rather than tangible».

[293] «*The majority of the challenges in cybercrime cases relate to the execution of mutual legal assistance (MLA) requests: slow execution of MLA requests due to a lack of coordination between jurisdictions affected by the criminality, or refusal of execution because of conflicting national interests and/or pending criminal proceedings at national level. The current MLA process is perceived as a slow and cumbersome method of gathering and sharing volatile electronic data, for example due to the reasons relating to lack of coordination between different jurisdictions affected by the criminality.*», EUROJUST, *Overview Report- Challenges and best practices from Eurojust's casework in the area of cybercrime*, November 2020, p. 4, https://www.eurojust.europa.eu/sites/default/files/assets/2020_11_cybercrime_report.pdf. In dottrina v. DE LA CHAPELLE B., FEHLINGER P., *Jurisdiction on the Internet: from legal arms race to transnational cooperation*, in *Oxford Handbook of Online Intermediary Liability*, 2020, p. 10; MAILLART J. B., *The limits of subjective territorial jurisdiction in the context of cybercrime,* cit.: «*Second of all, the admissibility of MLA requests is traditionally subject to the dual criminality principle. Yet, with respect to cybercrimes, the problem is that the definition and scope of cybercrimes may vary considerably from one state to another, which may then result in a refusal of the MLA request*».

[294] V. ALIMONTI V., *Evaluando el nuevo Protocolo al Convenio sobre la Ciberdelincuencia en América Latina: Preocupaciones, consideraciones respecto a los derechos humanos y estrategias de mitigación*, *Electronic Frontier Foundation*, 2022; ILARDA G., MARULLO G. (a cura di), Cybercrime Conferenza *Internazionale: la Convenzione Del Consiglio d'Europa sulla criminalità informatica. Osservatorio permanente sulla criminalità organizzata,* cit.

[295] Per approfondimenti CAJANI F., *La cooperazione internazionale nelle indagini digitali*, in ATERNO S., CAJANI F., COSTABILE G., CURTOTTI D. (a cura di), *Cyber Forensics e indagini digitali*, cit., p. 249 ss.

[296] *Explanatory Report to the Convention on Cybercrime*, consultato su https://rm.coe.int/16800cce5b.

[297] *Explanatory Report to the Cybercrime Convention*, cit., p. 2, :«*The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer*

I lavori preparatori della Convenzione sono stati avviati da un comitato di esperti sul crimine nel cyberspazio nell'aprile del 1997[298] e hanno portato ad una prima bozza nell'aprile 2000, per giungere alle successive elaborazioni e all'approvazione nel giugno 2001; atti ai quali è seguito l'invio al Comitato dei ministri per l'adozione e l'apertura alla firma.

Obiettivi principali della Convenzione sono l'armonizzazione delle fattispecie di diritto penale in relazione al *cybercrime,* l'elaborazione di un idoneo apparato di diritto processuale per indagare e perseguire tali delitti ed altri commessi attraverso l'utilizzo di un sistema informatico e la definizione di un rapido ed efficace regime di cooperazione internazionale.

Questa si struttura in tre parti:

- la prima riguarda le disposizioni per l'armonizzazione internazionale delle leggi penali in relazione alla tipizzazione di determinati atti ed elementi;
- la seconda contiene disposizioni processuali per la regolamentazione dei mezzi di indagine e conservazione delle prove;
- la terza riguarda i principi che devono reggere la cooperazione internazionale tra gli Stati membri, inclusa la necessità di designare un punto di contatto che funzioni 24 ore al giorno tutti i giorni.

Ci soffermeremo, ai fini della presente ricerca, sulle misure disposte alla sezione II del capitolo II, relative al diritto processuale penale e al rapporto con i *service provider*.

Ai sensi dell'art. 1 lett. c) si definisce *service provider* qualunque ente pubblico o privato che mette a disposizione dei suoi utenti la possibilità di comunicare attraverso un sistema informatico e ogni altro ente che processa o immagazzina dati informatici per conto di un servizio di comunicazione o per gli utenti di tale servizio.

L'art. 14 espressamente chiarisce che le disposizioni procedurali saranno applicate in relazione alle fattispecie penali delineate dalla Convenzione, agli altri reati commessi attraverso un sistema informatico e alla raccolta di prove in formato elettronico. Pertanto, la portata delle disposizioni non è limitata ai delitti informatici, ma ricomprende qualunque altro delitto per cui si richiede l'acquisizione di dati informatici.

Le garanzie previste dalla Convenzione si allineano al rispetto dei diritti umani e delle libertà secondo quanto stabilito dalla Convenzione europea dei diritti umani[299], dal

---

boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory».

[298] *The Committee of Experts on Crime in Cyber-space* (PC-CY).

[299] Convenzione europea dei diritti dell'uomo (CEDU), (STE n. 005) firmata a Roma il 4 novembre 1950, entrata in vigore il 3 settembre 1953, consultata su https://rm.coe.int/1680a6eabb .

Patto internazionale sui diritti civili e politici delle Nazioni Unite[300] e dagli altri strumenti di diritto internazionale applicabili. Viene inoltre fatto esplicito riferimento al principio di proporzionalità, in quanto principio guida per l'esecuzione delle misure disposte.

Sul versante degli strumenti introdotti sono da considerare, soprattutto, l'ordine di produzione, previsto dall'art. 18, e l'accesso transnazionale ai dati immagazzinati in un computer, con il consenso del proprietario o quando pubblicamente disponibili, *ex* art. 32.

L'art.18 prevede che le Parti adottino le misure legislative o di altro tipo per dare alle autorità competenti il potere di:

- ordinare ad una persona nel suo territorio di inoltrare specifici dati informatici in suo possesso o controllo, archiviati in un sistema informatico o di archiviazione;
- ordinare ad un *service provider* che offre i suoi servizi nel territorio della Parte di inoltrare informazioni sull'utente (*subscriber information*) in suo possesso o controllo.

Questa misura permette l'emanazione di ordini svincolati dal principio di territorialità e dalla necessità di attivare una procedura nello Stato in cui il *provider* abbia sede legale[301].

La Convenzione circoscrive, inoltre, i limiti del concetto di *subscriber information* quale informazione contenuta in formato informatico o in qualunque altro formato detenuta dal *service provider*, in relazione agli utenti dei suoi servizi.

Tale informazione viene determinata in via residuale rispetto ai dati di traffico e di contenuto, ma si definisce tale in quanto in grado di precisare il tipo di servizio di comunicazione utilizzato, il periodo del servizio, l'identità dell'utente, l'indirizzo, il numero di telefono o altri numeri di accesso, i conti e le informazioni sui pagamenti, o ogni altra informazione disponibile sulla base del contratto di servizio[302].

---

[300] Patto internazionale sui diritti civili e politici, adottato in data 16 dicembre 1966 dall'Assemblea Generale delle Nazioni Unite con Risoluzione 2200°(XXI), entrato in vigore il 23 marzo 1976.

[301] *Cour de Cassation Belgique*, 01 dicembre 2015, P.13.2082.N., *Yahoo! Case*. A tal proposito, è opportuno precisare che il Belgio ha implementato l'art. 18 attraverso l'art. 46 del codice di procedura penale, stabilendo un dovere di cooperazione per *l'online service provider*, e in tal senso la Corte Suprema belga ha avuto modo di precisare che un ordine indirizzato a dei *provider* stranieri non eccede la giurisdizione delle competenti autorità giudiziarie.
Allo stesso modo in Spagna è stabilito un dovere di collaborazione sancito dall'art. 351 LECRIM.

[302] **Art. 18, Production order**, co. 3: « *For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement*».

Due i principali limiti di questa disposizione: da una parte, la circostanza che il *provider* debba trovarsi nel territorio della Parte o ivi offrire i suoi servizi e, dall'altra, la sua estensione ai soli *subscriber data*, tralasciando ogni altro tipo di dato che, seppur con le dovute garanzie, potrebbe essere utilizzato all'interno di un procedimento penale.

L'articolo 32 ha, invece, ad oggetto l'accesso transfrontaliero ai dati immagazzinati in un *computer* da parte di uno Stato quando:

- i dati siano pubblicamente disponibili, indipendentemente dalla loro localizzazione geografica, pur in assenza dell'autorizzazione dello Stato parte in cui si trovino;
- vi sia il consenso legittimo e volontario della persona che ha il potere di divulgare i dati attraverso il sistema informatico[303], pur se localizzati nel territorio di un'altra Parte.

Uno dei principali dubbi ha riguardato l'individuazione del soggetto al quale ricondurre "il legittimo potere di divulgare i dati". A tale riguardo, è da evidenziare che la giurisprudenza di legittimità ha precisato che tale soggetto debba essere individuato nella persona giuridica che di quei documenti o dati può disporre[304].

Entrambe le misure sembrano però inadeguate nei casi in cui non sia possibile identificare con certezza il luogo dove sono localizzati i dati o quando lo Stato in cui si trovi non sia Parte della Convenzione.

Per evitare, dunque, eventuali rifiuti da parte delle autorità e per usufruire di una procedura rapida, le autorità di polizia, di frequente, si rivolgono ai *provider* attivando forme di cooperazione volontaria.

I *provider*, anche per tutelare i propri interessi economici, sono soliti cooperare e favorire la *voluntary disclosure*, salvo che ciò determini un conflitto con la legge dello Stato presso cui hanno la sede legale.

Per rendere più veloce ed efficace la cooperazione, inoltre, la Convenzione ha disposto la creazione delle Reti 24/7[305]: punti di contatto costantemente disponibili per

---

[303] «**Article 32 – Trans-border access to stored computer data with consent or where publicly available:** *A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system*».

[304] Cass., Sez. VI, 28 febbraio 2023, n. 8714.

[305] «**Article 35 – 24/7 Network**

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-daya-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

assicurare assistenza immediata in caso di indagini o procedimenti penali relativi a sistemi informatici e dati, o per la raccolta di prove elettroniche di un reato. L'assistenza include l'agevolazione o, se lo Stato di appartenenza lo permette, lo svolgimento delle seguenti misure:

- suggerimenti tecnici,
- conservazione dei dati *ex* art. 29 e 30 della Convenzione,
- raccolta di prove, offerta di informazioni legali e localizzazione dei sospettati.

4.1.3 Il Secondo Protocollo alla Convenzione di Budapest

Se, già al momento della firma della seconda convenzione di Budapest, si aveva consapevolezza della portata dirompente delle innovazioni digitali, il passare del tempo ha soltanto amplificato questo dato.

Come dimostra l'esperienza applicativa, gli strumenti predisposti sono diventati obsoleti di fronte a quella che è stata definita la quarta rivoluzione[306].

L'avvento del *cloud computing* e dell'I*nternet of things* ha, in più, amplificato l'inadeguatezza degli strumenti di cooperazione, ancorati al principio della territorialità.

E invero, proprio i meccanismi connessi a queste tecnologie invalidano il principio di territorialità e indeboliscono la repressione dei crimini, allorquando non sia possibile identificare lo Stato al quale chiedere collaborazione o quando, invece, gli Stati coinvolti siano più di uno.

---

a) the provision of technical advice;
b) the preservation of data pursuant to Articles 29 and 30;
c) the collection of evidence, the provision of legal information, and locating of suspects.

2
a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network».

306 Cit. FLORIDI L., *La quarta rivoluzione. Come l'infosfera sa trasformando il mondo*, Raffaello Cortina Editore, 2017. Per approfondimenti: ALLEN S., *Enforcing criminal jurisdiction in the clouds and international law's enduring commitmet to territoriality*, in *The Oxford Handbook of Jurisdiction in International Law*, 2019; DANIELE M., *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit.; DASKAL J., *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, in *www.jnslp.com*, 2016; DE LA CHAPELLE B., FEHLINGER P., *Jurisdiction on the Internet: from legal arms race to transnational cooperation*, in *Oxford Handbook of Online Intermediary Liability*, 2020.

Nel 2012 la *Cybercrime Convention Committee* ha definito un nuovo "*Subgroup on jurisdiction and transborder access to data"* (cd. *Transborder group*) e nel 2015 un *working gro*up su "*Criminal Justice Access to Evidence stored in the cloud, including through mutual legal assistance*" (cd. *Cloud evidence group*).

Le principali sfide individuate nel 2016 dal *Cloud evidence group* riguardavano il rapporto tra *cloud computing* e principio territorialità, e le attuali difficoltà connesse alla raccolta delle prove digitali[307].

Sulla scorta di tali conclusioni, le Parti della Convenzione sul *cybercrime* hanno ritenuto che non fosse necessario modificarla o adottare nuove disposizioni di diritto penale sostanziale ma che, invece, fossero necessarie misure addizionali per sviluppare la cooperazione e la capacità delle autorità di ottenere prove digitali, attraverso un secondo protocollo addizionale.

La bozza del Secondo Protocollo alla Convenzione di Budapest è stata approvata durante una riunione del *Cybercrime Convention Committee* in data 28 maggio 2001 per essere poi sottoposta al Comitato dei ministri per la sua adozione.

Il Protocollo, firmato in data 12 maggio 2022 da 22 Stati[308], ha ad oggi 36 stati firmatari[309].

Il preambolo chiarisce che il fine è la promozione della cooperazione diretta – in materia di *cybercrime* – tra le autorità, i *service provider* e altri soggetti in possesso di informazioni pertinenti e, anche, la raccolta di prove elettroniche in relazione ad ogni tipo di reato ai fini dei procedimenti giudiziari.

All'art. 2 viene sancito il rispetto del principio di specificità[310], in virtù del quale le misure predisposte non potranno essere utilizzate a fini preventivi o in via generale, ma soltanto per specifici procedimenti penali e indagini, in relazione a reati informatici, raccolta

---

[307] Cfr. *Transborder access and jurisdiction: What are the options? - Report of the Transborder Group adopted by the T-CY*, 6 dicembre 2012, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8 .

[308] Austria, Belgio Bulgaria, Cile, Colombia, Estonia, Finlandia, Islanda, Italia, Giappone, Lituania, Lussemburgo, Montenegro, Marocco, Paesi Bassi, Macedonia del nord, Portogallo, Romania, Serbia, Spagna, Svezia e Stati Uniti d'America.

[309] Cfr. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 .

[310] Art. 2: «*the measures described in this Protocol shall be applied […]:*

a) to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence, and

b) *[…] to specific criminal investigations or proceedings concerning criminal offences established pursuant to the First Protocol*».

di prove digitali o, per gli Stati firmatari del Primo Protocollo[311], per reati da quest'ultimo stabiliti.

In merito alle definizioni fornite dall'art. 3, assume particolare importanza la nozione di autorità competente, intesa quale: autorità giudiziaria, amministrativa o di polizia a cui la legge nazionale conferisca il potere di ordinare, autorizzare o intraprendere l'esecuzione delle misure previste dal Protocollo per la raccolta o produzione di prove, in relazione a specifici procedimenti penali o indagini[312].

Il capitolo II, relativo alle misure per la cooperazione rafforzata, è a sua volta diviso nelle seguenti sezioni:

1. principi generali,
2. procedure che promuovono la cooperazione diretta con i *provider* ed enti di altre Parti,
3. procedure che promuovono la cooperazione internazionale con altre Parti per la rapida produzione di *subscriber data* e *traffic data,*
4. procedure di assistenza reciproca in caso di emergenza,
5. procedure di cooperazione in assenza di accordi internazionali applicabili.

Il protocollo prevede che le Parti adottino, per adempiere agli obblighi assunti, ogni misura legislativa o di altro tipo, lasciando così a queste la discrezionalità sulla possibilità di adottare norme specifiche o di rimuovere gli ostacoli alla cooperazione.

Sarà, pertanto, possibile la rimozione di ogni previsione legale che impedisca ai *provider* di rispondere a un ordine dell'autorità di un altro Stato parte, così come la creazione di un apposito obbligo di adempiere a tali ordini.

Sarà obbligo di ogni Stato assicurare che i *service provider* possano rispondere a tali ordini in maniera legittima e in un regime di certezza giuridica, senza incorrere in una responsabilità legale per il solo fatto di avere consegnato dei dati in buona fede, in risposta ad un ordine legittimamente emanato. Questo non preclude, tuttavia, la possibilità di incorrere in responsabilità legale per ragioni diverse.

Le misure previste agli articoli 6, 7 e 8 del Protocollo pongono le basi per ottenere dati in possesso o controllo degli *internet service provider* per specifiche indagini o procedimenti penali. Ciò avviene richiedendo agli Stati di adottare misure legislative o di

---

311 Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici (STE no. 189), firmato a Strasburgo il 28 gennaio 2003, entrato in vigore l'1 marzo 2006.

312 Art. 3 co. 2 lett. b): «*competent authority" means a judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings*».

altro tipo idonee a permettere a tali soggetti la legittima *disclosure* alle autorità competenti di un altro Stato che ne facciano richiesta.

La cooperazione diretta con i *service provider* o enti di altre Parti è regolata dagli artt. 6, *request for domain name registration information* e 7, *disclosure of subscriber information*, mentre l'art. 8– g*iving effect to orders from another Party for expedited production of subscriber information and traffic data* – prevede la cooperazione tra autorità per dare effetto all'ordine di cui all'art. 7.

Tali articoli si concentrano sui domini registrati, su *subscriber information* e sui dati di traffico, spesso fondamentali per le indagini ma difficili da ottenere tramite le procedure di assistenza giudiziaria, che non permettono di ottenere risposta in tempi rapidi e utili per le indagini. In più, si rischia di incorrere in un sovraccarico a causa della mole di indagini e dati richiesti.

In tal modo, il Protocollo ha inteso creare una struttura più rapida ed efficace per ovviare alle suddette problematiche e permettere la rapida prosecuzione delle indagini.

L'art. 6 è incentrato sulla richiesta di informazioni relative alla registrazione di un dominio[313] e prevede che le Parti debbano adottare ogni misura legislativa o di altro tipo per permettere alle autorità competenti, in relazione a specifici procedimenti penali o indagini, di inviare una richiesta ad un ente che fornisca un servizio di registrazione di dominio[314] nel territorio di un'altra Parte, per ottenere informazioni in suo possesso o controllo, finalizzate all'identificazione o contatto del *registrant* di un dominio[315]. Nello specifico, nome, indirizzo fisico o *email* e numero telefonico del soggetto che registra il dominio.

---

[313] *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, Strasburgo, 12 maggio 2022, https://rm.coe.int/1680a49c9d , § 75: « *Domain name registration information is held by entities providing domain name registration services. These include organisations that sell domain names to the public ("registrars") as well as regional or national registry operators which keep authoritative databases ("registries") of all domain names registered for a top level domain and which accept registration requests. In certain cases, such information may be personal data and may be protected under data protection regulations in the Party where the respective entity providing domain name registration services (the registrar or registry) is located or where the person to whom the data relates is located*».

[314] *L'Explanatory report* specifica come il termine utilizzato, "*entity providing domain name registration service*" possa riferisci sia a *registrars* che *registries* e che, inoltre, possa essere adattato a vari modelli economici e all'architettura di *internet*, che può subire frequenti cambi. Cfr. Explanatory Report, cit., § 79: «*An "entity providing domain name registration services" currently refers to registrars and registries. To take the present situation into account and at the same time permit adaptation as business models and the architecture of the internet may change over time, this article uses the more generic term of an "entity providing domain name registration service*s».

[315] *Explanatory Report*: «74. *Many forms of cybercrime are facilitated by offenders creating and exploiting domains for malicious and illicit purposes. For example, a domain name may be used as a platform for the spreading of malware, botnets, phishing and similar activities, fraud, distribution of child abuse materials and for other criminal purposes. Access to information on the legal or natural person who registered a domain (the "registrant") is therefore critical to identify a suspect in a specific criminal investigation or proceeding. Whereas domain name registration data were historically publicly available, access to some of the information is now restricted, which affects judicial and law-enforcement authorities in their public policy tasks*».

Queste informazioni possono essere considerate alla stregua di *subscriber data*, secondo quanto stabilito dall'art. 18 della Convenzione di Budapest. Peraltro, la richiesta di questa tipologia di dati è considerata meno intrusiva rispetto ad altre, dal momento che non permette di tracciare precise conclusioni sulla vita di un soggetto o sulle sue abitudini.

Il Protocollo prevede che, proprio per garantire la reciprocità della cooperazione, le Parti non solo adottino le misure idonee a permettere l'invio della richiesta ma, al contempo, permettano al soggetto presente nel territorio nazionale di divulgare le informazioni richieste.

A queste è lasciata ampia flessibilità in relazione alle formalità procedurali richieste per l'emissione dell'ordine, dipendendo dalle considerazioni legali e politiche di ciascuno di essi, non è tuttavia previsto che abbia portata vincolante per il *provider*[316] e non saranno pregiudicate eventuali forme di collaborazione volontaria.

Lo Stato può, inoltre, condizionare la risposta dei *provider* al rispetto di specifiche disposizioni nazionali e, tra queste, quelle in tema di *data protection*.

La richiesta delle autorità competenti dovrà includere:

- la data di invio della richiesta, l'identità e i dettagli di contatto dell'autorità compente che la effettua;
- il dominio di cui si richiedono informazioni e una lista specifica delle informazioni richieste,
- la dichiarazione che la richiesta è effettuata secondo quanto stabilito dal Protocollo, che le informazioni richieste sono necessarie e rilevanti per specifici procedimenti penali o indagini e che, pertanto, verranno utilizzate solo in relazione a questi;
- il termine ed il modo in cui ottenere la *disclosure* e ogni ulteriore e speciale richiesta sulla procedura.

Qualora il soggetto interpellato decida di non cooperare con le autorità, queste potranno chiedere di offrire una giustificazione, in modo da valutarla e trovare un ragionevole compromesso per ottenere i dati. Potranno, inoltre, avviare una consultazione con lo Stato su cui sia localizzato *il provider* per verificare come ottenere le informazioni.

Le autorità incaricate per la consultazione verranno stabilite delle Parti e comunicate al Segretario Generale del Consiglio d'Europa, che ne terrà nota in un apposito registro con i dati e dettagli delle autorità designate.

---

316 *Explanatory report*: «77. *Paragraph 1 gives Parties flexibility regarding the format in which requests are made, since the format depends on the Parties' respective legal and policy considerations. A Party can use procedures available under its domestic law, including issuance of an order; however, for the purposes of Article 6, such an order is treated as a nonbinding request*».

L'art. 7 non prevede, invece, l'invio di una richiesta ma di un ordine emanato dall'autorità competente di uno Stato parte e diretto a un *provider* presente nel territorio di un'altra Parte. La norma nasce dalla necessità di definire un meccanismo complementare all'art. 18 della Convenzione di Budapest, fortemente limitato, *in primis,* dall'esigenza di localizzare i dati da ottenere e, *in secundis,* dalla necessità che il *provider* che li detiene sia ubicato nel territorio dello Stato che effettua la richiesta.

Infatti, l'art. 18 della Convenzione si applica quando un *service provider* è nel territorio dello Stato che emette la richiesta o ivi offra i suoi servizi; l'art. 7, invece, riguarda i casi in cui il *provider* si trovi in un altro Stato parte[317].

Tale ordine sarà finalizzato all'ottenimento di specifiche *subscriber information*, già conservate dal *provider* (*stored*) e in suo possesso o controllo, qualora necessarie per specifici procedimenti penali o indagini.

Sebbene questi ordini, impartiti in via diretta ai *provider,* presentino dei vantaggi sul piano della speditezza della procedura, non dovrebbe, tuttavia, essere consentito alla Parte utilizzare tutti i meccanismi coercitivi di cui dispone nella legge domestica[318].

Per la definizione di *subscriber information* si fa riferimento proprio all'art. 18 della Convenzione, ovvero ogni informazione detenuta in forma di dato informatico o sotto altra forma da un fornitore di servizi e relativa agli abbonati ad un proprio servizio e diversa dai dati relativi al traffico o al contenuto e attraverso la quale è possibile stabilire:

a) il tipo di servizio di comunicazione utilizzato, le disposizioni tecniche prese a tale riguardo e il periodo del servizio;
b) l'identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento, disponibili sulla base degli accordi o del contratto di fornitura del servizio;
c) ogni altra informazione sul luogo di installazione dell'apparecchiatura della comunicazione, disponibile sulla base degli accordi o del contratto di fornitura del servizio.

---

[317] V. SPIEZIA F., *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: Il ruolo di Eurojust*, cit.

[318] *Explanatory Report*, cit.*, § 94: «The Parties recognised that although such direct orders from authorities of one Party to service providers located in another Party are desirable for rapid and effective access to information, a Party should not be permitted to use all enforcement mechanisms available under its domestic law for enforcement of these orders. For that reason, enforcement of these orders in cases where the provider does not disclose the specified subscriber information is limited in the manner set forth in paragraph 7 of Article 7. This procedure provides for safeguards to take account of the unique requirements arising from a direct co-operation between authorities of one Party with service providers located in another Party*». Cfr. BUCCARELLA M., *Il secondo protocollo addizionale alla Convenzione di Budapest alla luce del diritto internazionale e dei trattati*, in *Dir. Pen. Proc*., 2022, 9, p. 1160.

Tra le informazioni utili a identificare l'abbonato vi è certamente l'indirizzo IP.

Come già anticipato, se in alcuni Stati questo può essere inquadrato nell'ambito dei *subscriber data*, in altri, invece, è trattato alla stregua di un dato di traffico, in ragione del suo collegamento con lo svolgimento di una comunicazione. In ragione di questa difformità tra gli ordinamenti nazionali, il Protocollo prevede che ogni Parte possa formulare una riserva su determinate categorie di dati, in tal modo impedendo ai *provider* di effettuarne la *disclosure*. L'art. 7 co. 9 del Protocollo, infatti, dà alle Parti il diritto di non applicare questo articolo *in toto* o in relazione a specifici numeri di accesso qualora ciò non rispetti i principi fondamentali dell'ordinamento.

Secondo quanto già previsto all'art. 6, gli Stati potranno prevedere l'applicazione di tale norma utilizzando apposite misure legislative o di altro tipo, per permettere sia l'emanazione dell'ordine, sia la rimozione di ogni impedimento alla legittima *disclosure* da parte del *provider*.

Viene, inoltre, previsto che, al momento della firma o della ratifica, la Parte possa stabilire che l'ordine debba essere emanato da o sotto la supervisione di un pubblico ministero o altra autorità giudiziaria, o essere altrimenti emanato sotto la supervisione di un'autorità indipendente.

L'ordine dovrà specificare:

- l'autorità che lo emana e la relativa data,
- la dichiarazione che l'ordine è stato emanato secondo il Protocollo,
- il nome e la direzione del *service provider* interpellato,
- il reato per cui si procede o indaga,
- l'autorità che richiede gli specifici dati dell'utente, se non è l'autorità emanante,
- una dettagliata descrizione delle informazioni richieste.

Inoltre, potrà essere accompagnato da alcune informazioni supplementari, quali:

- la base legale che legittima l'autorità all'emanazione dell'ordine,
- un riferimento alle disposizioni legali e alle sanzioni applicabili per il reato sul quale si indaga o procede,
- le informazioni di contatto dell'autorità a cui il *provider* dovrà consegnare i dati e a cui potrà richiedere informazioni ulteriori,
- il periodo e il modo di consegna delle informazioni,
- le informazioni su eventuali anteriori richieste di conservazione dei dati, inclusa la data di conservazione e ogni altro numero di riferimento,

- ogni specifica richiesta sulla procedura (tra cui la confidenzialità),
- se *applicabile*, la dichiarazione che sono state fatte delle notificazioni allo Stato parte in cui si trovi il provider,
- ogni altra informazione che può essere utile per ottenere la *disclosure* delle informazioni.

Ogni Parte può dichiarare[319] al Segretario Generale del Consiglio d'Europa che al momento dell'emanazione di un ordine ad un *service provider* nel suo territorio, le venga inviata una notifica con informazioni supplementari e un sunto dei fatti relativi all'emanazione dell'ordine.

La Parte può, inoltre, chiedere di essere consultata. Tali richieste di notifica o consultazione possono riguardare tutti i casi in cui venga emanato un ordine o solo specifiche circostanze da questa definite. Ciò al fine di effettuare un'analisi della richiesta, per poter eventualmente impedire al *provider* la *disclosure* qualora ciò possa pregiudicare indagini o procedimenti penali nazionali, o nel caso in cui siano applicabili condizioni di rifiuto secondo gli artt. 25 co. 4 [320]e 27 co. 4[321] della Convenzione.

Le autorità potranno, inoltre, sollecitare informazioni addizionali alle autorità richiedenti e dovranno prontamente informarle qualora abbiano intimato al *provider* di non consegnare i dati, specificandone le ragioni.

Le autorità designate per la notifica e la consultazione andranno comunicate al Segretario Generale per la redazione di un apposito registro in cui segnare anche i dettagli di contatto.

Qualora il *provider* dichiari di non voler consegnare le informazioni o non risponda alla richiesta nel termine di 30 giorni, l'autorità competente della Parte richiedente potrà richiedere la ragione del rifiuto e far rispettare l'ordine solamente utilizzando l'art. 8 o misure di *mutual legal assistance*, dal momento che in nessun modo è previsto il ricorso alla coercizione da parte dello Stato richiedente.

---

[319] Art. 50 co. 5 lett. a), prevede che la dichiarazione della Parte avvenga al momento della firma o del deposito degli strumenti di ratifica, accettazione o approvazione.

[320] «*Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence*».

[321] «*The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b) it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests*».

In questa ipotesi, la cooperazione non si realizza tra l'autorità e il *provider*, ma tra le autorità nazionali degli Stati interessati: lo Stato richiesto, infatti, dovrà compiere ogni ragionevole sforzo per obbligare il *provider* localizzato nel suo territorio a consegnare le informazioni richieste (*subscriber* o *traffic data*) nel più breve tempo possibile o, comunque, nei termini previsti nella Convenzione[322].

Sia nel caso della richiesta *ex* art. 6 sia dell'ordine *ex* art. 7, qualora il soggetto privato lo accetti, la richiesta potrà essere trasmessa in formato elettronico, secondo appropriati standard di sicurezza e autenticazione. Inoltre, ai sensi dell'art. 4, le richieste, gli ordini o le informazioni supplementari dovrebbero essere formulati:

- nella lingua dell'altra Parte, accettata dal *provider* o dall'ente privato in relazione a simili procedure domestiche;
- in un'altra lingua accettata dal *provider* o dall'ente privato,
- accompagnati da una traduzione in una delle lingue di cui alle voci precedenti.

La Parte potrà opporre una riserva per non permettere l'esecuzione di ordini provenienti da altre Parti. Per effetto di tale riserva, tuttavia, non potrà emettere ordini di tal tipo nei confronti di *provider* di altre Parti.

L'art. 8 è rubricato "*Giving effect to orders from another Party for expedited production of subscriber information and traffic data*".

Nello specifico, prevede che le autorità di ogni Parte abbiano il potere di dare effetto all'ordine[323] emanato da un'altra Parte, per obbligare un *service provider* nel territorio nazionale a produrre specifici *subscriber information* e *traffic data* conservati e in suo possesso o controllo, per specifici procedimenti penali o indagini.

Le Parti dovranno adottare ogni misura legislativa o di altro tipo per permettere l'emanazione di tale ordine e, inoltre, affinché sia dato effetto alla richiesta.

---

[322] In tal senso SPIEZIA F., *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: Il ruolo di Eurojust*, cit.

[323] *L'Explanatory Report* specifica che con il termine "*order*" si intende ogni tipo di strumento idoneo ad obbligare un *provider* a fornire *subscriber information* o *traffic data*. § 126: «*The "order" referred to in Article 8 is any legal process that is intended to compel a service provider to provide subscriber information or traffic data. For example, it can be implemented by a production order, a subpoena or other mechanism that is authorised in law and that can be issued for the purpose of compelling the production of subscriber information or traffic data*». Inoltre, l'espressione "*giving effect*" dà la possibilità allo Stato interpellato di obbligare il *provider* utilizzando un meccanismo a sua scelta. Cfr. *Explanatory Report*, cit., § 129: «*For example, a requested Party may give effect to a requesting Party's order by accepting it as equivalent to domestic orders, by endorsing it to give it the same effect as a domestic order or by issuing its own production order. Any such mechanism will be subject to the terms of the law of the requested Party, since the requested Party's procedures will control it. Therefore, the requested Party can ensure that its own law, including constitutional and human rights requirements, is satisfied, especially in relation to any additional safeguards including those necessary for the production of traffic data*».

L'ordine dovrà contenere le informazioni previste dall'art. 7 e, inoltre, eventuali informazioni addizionali o specifiche istruzioni sulla procedura richiesta.

Le informazioni supplementari dovranno specificare:

- la base legale che autorizza l'autorità ad emanare l'ordine,
- le disposizioni legali e le sanzioni applicabili per i reati per cui si procede o indaga,
- la ragione per cui la parte richiedente crede che il *service provider* sia in possesso o abbia il controllo dei dati,
- un sunto dei fatti relativi alle indagini o al procedimento,
- indicazioni sulla rilevanza delle informazioni o dei dati per le indagini e il procedimento,
- le informazioni di contatto di un'autorità o delle autorità che potrebbero dare ulteriori informazioni,
- se è stata già richiesta la conservazione dei dati la data di conservazione e ogni altro numero di riferimento,
- se l'informazione o i dati sono stati già richiesti in altri modi e, in caso di risposta affermativa, in quali.

La Parte può, inoltre, richiedere che le informazioni addizionali siano sempre necessarie per dare effetto all'ordine. Come per le disposizioni precedenti, è prevista la possibilità di inoltrare la richiesta in formato elettronico per semplificare la procedura. Non è specificato attraverso quale canale o forma; dovrà, tuttavia, essere garantito un adeguato livello di sicurezza e autenticazione.

La Parte a cui è richiesta la cooperazione dovrà fare ogni ragionevole sforzo per interpellare il *service provider* entro 45 giorni dalla ricezione di tutte le informazioni, e dovrà ordinare la consegna delle informazioni richieste non oltre 20 giorni se si tratta di *subscriber information* e 45 per i dati di traffico.

In seguito, procederà alla trasmissione dei dati alla Parte richiedente senza ulteriori ritardi. Nel caso di specifiche richieste sulla procedura da eseguire, qualora queste non siano eseguibili secondo la legge dello Stato di esecuzione, la Parte richiedente verrà prontamente informata. Saranno, inoltre, specificate le condizioni necessarie per il compimento dell'atto, permettendo di scegliere se proseguire con l'esecuzione o meno [324].

[324] Cfr. *Explanatory Report*, cit., § 140: «*The Parties acknowledged that some special procedural instructions from the requesting Party may also cause delays in the processing of orders, if the instructions require additional domestic processes in order to give effect to the special procedural instructions. The requested Party may also require additional information from the requesting Party in order to support any applications for supplementary orders, such as confidentiality orders (non-disclosure orders). Some procedural instructions may not be available under the requested Party's law, in which case paragraph 7 provides that it shall promptly inform the requesting Party and specify any conditions under which it could comply, giving the requesting Party the ability to determine whether or not it wishes to continue with the request*».

La Parte interpellata può rifiutarsi di eseguire una richiesta in conformità agli artt. 25 co. 4 o 27 co. 4 della Convenzione oppure imporre le condizioni che ritenga necessarie per permettere l'esecuzione di una richiesta. Nello specifico, avrà inoltre la possibilità di rigettare la richiesta qualora vi siano motivi di rifiuto contemplati in trattati di assistenza giudiziaria o in leggi nazionali, nel rispetto delle garanzie per i diritti delle persone ubicate nello Stato di esecuzione. Inoltre, in ossequio al paragrafo 268 dell'*Explanatory Report* della Convenzione di Budapest, si potrà opporre il rifiuto qualora l'esecuzione causi un pregiudizio alla sovranità statale, sicurezza, ordine pubblico o altri interessi fondamentali.

Lo Stato potrà, inoltre, posporre l'esecuzione dell'atto. In entrambi i casi, rifiuto o ritardo, dovrà notificare le ragioni poste alla base di tale scelta.

Le autorità incaricate di emanare o ricevere un ordine ai sensi dell'art. 8 verranno scelte dalle Parti e comunicate al Segretario Generale al momento della firma, del deposito degli atti di ratifica, accettazione o approvazione; potranno, inoltre, richiedere che l'ordine dalle altre Parti sia emanato dall'autorità centrale o da altre autorità reciprocamente determinate tra le parti. Il Segretario terrà nota di tali informazioni in apposito registro.

Le Parti potranno, inoltre, riservarsi il diritto di non applicare tale articolo.

Al momento della redazione del Protocollo si era affrontata la necessità di prevedere forme agevolate di cooperazione in situazioni di emergenza, quali attacchi informatici, terroristici o in caso di sequestro di persona.

A tal fine, l'art. 9 stabilisce che sia data ai punti di contatto della Rete 24/7 la possibilità di trasmettere e ricevere richieste per ottenere assistenza immediata finalizzata all'ottenimento di specifici dati conservati dai *service provider* presenti nel territorio di un'altra Parte, senza passare attraverso una richiesta di assistenza giudiziaria.

Ai sensi dell'art. 3 co. 2 lett. c), per emergenza deve intendersi una situazione in cui c'è un significativo e imminente rischio per la vita o la sicurezza di ogni persona fisica. Il termine utilizzato per i dati da richiedere è "*specified stored computer data*", così da includere ogni tipo di dato informatico, secondo quanto definito dall'art. 1 della Convenzione, ovvero qualunque rappresentazione di fatti, informazioni o concetti in una forma che si presta a elaborazione informatica, inclusi i programmi che permettono a un sistema informatico di svolgere una funzione. Tale definizione permette di includere non solo le *subscriber information*, ma anche dati di traffico e di contenuto, che richiederebbero una previa richiesta di assistenza giudiziaria.

Questa tipologia di dati presenta livelli di intrusività particolarmente incisivi e ciò giustifica la scelta di limitarne l'accesso alle sole situazioni di emergenza.

L'utilizzo dei canali di cooperazione della Rete 24/7 permette di agevolare lo scambio senza le lungaggini connesse alla redazione di una richiesta di assistenza giudiziaria. I vantaggi che derivano dall'utilizzo della Rete 24/7 sono molteplici: si riducono i tempi per l'acquisizione delle informazioni; è possibile avviare forme di cooperazione ulteriore non limitate alla richiesta di *subscriber data* e, inoltre, potrebbe essere più semplice autenticare le prove ottenute attraverso tali canali[325].

La richiesta dovrà specificare:

- l'autorità competente che richiede i dati e la data in cui la richiesta è stata effettuata,
- la dichiarazione che la richiesta è emanata conformemente al Protocollo,
- il nome e l'indirizzo del *service provider* in possesso o controllo dei dati richiesti,
- il reato alla base delle indagini o del procedimento penale e il riferimento alle previsioni legali e alle sanzioni applicabili,
- sufficienti indicazioni che consentano di dimostrare l'esistenza di una situazione di emergenza e come i dati richiesti vi siano legati,
- una dettagliata descrizione dei dati richiesti,
- specifiche richieste sulla procedura,
- ogni altra informazione che possa essere utile nell'ottenimento dei dati richiesti.

La richiesta potrà essere inviata in formato elettronico. In ogni caso, la Parte può anche accettarla quando sia trasmessa oralmente e sollecitare una conferma in formato elettronico, previa garanzia di appropriati livelli di sicurezza e autenticazione. Ogni Parte potrà prevedere l'utilizzo di specifici format o appositi canali per inoltrare la richiesta.

---

[325] Cfr. *Explanatory Report* cit., § 152: «*Using the channel established in this article may have advantages over the emergency mutual assistance channel set forth in Article 10. For example, this channel has the advantage that no mutual assistance request need be prepared in advance. Considerable time may be needed to prepare a prior mutual assistance request, have it translated and pass it through domestic channels to the requesting Party's central authority for mutual assistance, which would not be required under Article 9. In addition, once the requested Party has received the request, if it must obtain supplemental information before it can grant assistance, the additional time that may be needed for a mutual assistance request is more likely to slow execution of the request. In the mutual assistance context, requested Parties often require that the supplemental information be provided in a written and more detailed form, whereas the 24/7 channel operates using real-time exchange of information. On the other hand, the emergency mutual assistance channel offers advantages in certain situations. For example, (i) little or no time may be lost by using that channel if there are particularly close working relations between the central authorities concerned; (ii) emergency mutual assistance may be used to obtain additional forms of co-operation beyond computer data held by providers; and (iii) it may be easier to authenticate evidence obtained via mutual assistance. It is up to the Parties, based on their accumulated experience and the specific legal and factual circumstances at hand, to decide which is the best channel to use in a particular case*».

Il capitolo III si occupa, invece, di stabilire le condizioni e garanzie.

In particolare, prevede che ogni Parte, nell' implementare e applicare il Protocollo, rispetti le garanzie previste dalle leggi nazionali, che devono assicurare un'adeguata protezione dei diritti umani e delle libertà.

Una specifica disposizione è dedicata alla protezione dei dati personali: l'art. 14 stabilisce, infatti, che ogni Parte dovrà processare i dati personali che riceve nel rispetto di precise garanzie.

In primis, saranno applicati eventuali accordi internazionali tra gli Stati che stabiliscono un quadro generale per la protezione dei dati personali, applicabile al trasferimento dei dati per ragioni di prevenzione e persecuzione di reati, e che prevedano disposizioni *ad hoc* per il trattamento di tali dati. In assenza di un accordo, tuttavia, le Parti possono stabilire reciprocamente che il trasferimento dei dati personali abbia luogo sulla base di altri accordi o patti tra le stesse. Rimane ferma la possibilità di applicare delle garanzie più elevate per il trasferimento dei dati personali.

I dati sensibili – relativi a origini etniche o razziali, opinioni politiche o religiose o altri tipi di opinioni, dati genetici, biometrici o dati personali relativi alla salute o alla vita sessuale – saranno trasferiti nel rispetto di adeguate tutele che prevengano il rischio di pregiudizi, come illegittime discriminazioni, derivanti dall'uso di tali dati.

Le Parti dovranno, inoltre, detenere i dati per lo stretto necessario in relazione ai fini per cui sono stati richiesti.

L'articolo 14 co. 13 prevede, ancora, che ogni Parte disponga di un rimedio giudiziario o non giudiziario, purché effettivo, a fronte di violazioni in tema di protezione dei dati personali.

Ancorché la norma sia apprezzabile, è da domandarsi se il Protocollo non avrebbe dovuto prevedere dei rimedi per eventuali violazioni dei diritti fondamentali che si verifichino nel caso di richiesta diretta ai *provider* o, ancora, nel caso di richiesta *ex* art. 9, che, come anticipato, non include i soli *subscriber data*, ma anche categorie soggette ad una maggiore intrusività, quali *traffic data* e *content data*.

Quanto sin qui rassegnato rende evidente come la principale sfida sia quella di permettere l'accesso legittimo ai dati in tempi rapidi ed efficienti per lo sviluppo delle indagini e la prosecuzione dei procedimenti penali. Allo stesso tempo, però, non bisogna sottovalutare la necessità di proteggere i diritti fondamentali e la libertà degli individui.

Seppure il Protocollo non manchi di porre alla base delle misure il principio di specificità e il rispetto di diritti fondamentali e delle libertà, nonché la protezione dei dati personali, bisogna capire se e come questi valori potranno essere tutelati.

Nello specifico, mentre l'art. 8 richiama alcune delle garanzie previste dal sistema di *mutual legal assistance*, maggiori dubbi si concentrano sulle misure previste dagli artt. 6 e 7.

Anzitutto, se non espressamente disposto dalla Parte, l'ordine potrà essere emesso senza alcun tipo di supervisione da parte dell'autorità giudiziaria o di un'autorità indipendente. Nella sostanza, saranno i *provider* a compiere la relativa valutazione, con il rischio che omettano di verificare il rispetto dei diritti fondamentali. Ciò in conseguenza, per lo più, dell'assenza delle necessarie competenze, specie nel caso di piccole imprese che non dispongano delle adeguate risorse umane e di tutte le informazioni necessarie per valutare la conformità con i diritti fondamentali[326]; un altro elemento potrebbe essere quello della tutela dei propri interessi economici.

Un ulteriore fattore di rischio nella tutela dei diritti fondamentali è legato alla nozione di autorità competente. Infatti, come detto, nella definizione vi rientra un'autorità giudiziaria o amministrativa o di polizia a cui l'ordinamento nazionale dia il potere di emettere una delle misure in oggetto. Conseguentemente, la richiesta di dominio o di un ordine per ottenere informazioni dal *provider* potrebbe non essere soggetta al controllo di un'autorità giudiziaria o di altre autorità indipendenti. Il timore è quella di ottenere informazioni in un altro Stato, con minori tutele rispetto a quelle a cui sarebbe sottoposta la richiesta proveniente dalle autorità nazionali in un altro Stato parte.

Seppur al co. 2 lett. b) dell'art. 7 sia previsto che una Parte possa dichiarare che l'ordine inoltrato ad un *provider* nel suo territorio sia emanato da un pubblico ministero o altra autorità giudiziaria o sotto la sua supervisione o di un'autorità indipendente, ciò lascia ampia discrezionalità agli Stati.

---

[326] Cfr. ALIMONTI V., *Evaluando el nuevo Protocolo al Convenio sobre la Ciberdelincuencia en América Latina: Preocupaciones, consideraciones respecto a los derechos humanos y estrategias de mitigación*, cit., p. 11: «*Los requerimientos a los proveedores de servicios en virtud del apartado 1 del artículo 7 se presentan en el texto del Protocolo como "órdenes" ("orders" en el texto inglés original), que son vinculantes a nivel nacional, aunque no son directamente ejecutables por las autoridades extranjeras requirentes, dada su aplicación transfronteriza. En principio, los proveedores de servicios siguen teniendo margen para rechazar estos requerimientos directos, pero el hecho de que su cumplimiento puede ser ejecutado mediante procedimientos para obligar a la presentación de la información ("dar efecto a una orden") establecidos en el artículo 8, u por otra forma de asistencia mutua, 13 probablemente disuadirá a los proveedores de rechazar dichos requerimientos. De hecho, en virtud del artículo 7, los proveedores de servicios ni siquiera reciben suficiente información para evaluar o procesar adecuadamente un requerimiento para identificar las circunstancias que son incompatibles con los derechos humanos y las libertades fundamentales*».

Nel caso in cui l'ordine sia emesso da un pubblico ministero, per quanto questi risponda alla legge e possa operare in maniera indipendente nello svolgimento delle indagini, non si può tuttavia ritenere che la figura risponda al requisito di imparzialità. Questa tesi è stata, peraltro, avallata dalla Corte di giustizia, come precedentemente detto, nella sentenza *Prokuratuur*. Si può ritenere, inoltre, che i meccanismi di notificazione e consultazione possano non sortire alcun effetto, essendo facoltativi.

E peraltro, in assenza di questi meccanismi, spetterà al *provider* valutare la proporzionalità, la necessità, la specificità e l'eventuale mancato rispetto dei diritti umani degli interessati.

Uno dei metodi attraverso i quali si potrebbe garantire una maggior salvaguardia dei diritti fondamentali potrebbe essere quello di applicare le riserve previste e le maggiori salvaguardie quali, per esempio:

- richiedere che l'ordine venga emesso da un pubblico ministero e da o sotto il controllo di un'autorità giudiziaria o indipendente[327] (pur se come esposto, ciò non garantisce la assoluta indipendenza dell'autorità emanante, come nel caso del pubblico ministero),
- stabilire meccanismi di notifica e consultazione obbligatori[328],
- designare un'autorità giudiziaria indipendente per ricevere le comunicazioni *ex* art. 7 co. 5,
- decidere di non applicare l'art. 7 per determinati tipi di dati, quali l'indirizzo IP.

Queste raccomandazioni sono arrivate da parte dello *European data protection supervisor*[329], che ha sottolineato come alcune categorie di dati vengano considerate *subscriber information* secondo la Convenzione di Budapest e *traffic data* secondo la normativa comunitaria.

Per tale ragione, si raccomanda agli Stati membri di:

---

[327] Cfr. *EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime,* https://rm.coe.int/euroispa-s-comments-to-draft-provisions-2nd-add-protocol-final/168098bcab.

[328] Cfr. EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, cit., p.3:« *EuroISPA demands that the competent authorities in the receiving party shall be notified in all circumstances as this would provide more legal certainty whereas preference is given to notification already by the requesting party to the receiving party, in order to avoid additional burden for the service provider. Authorities in the receiving state should be involved as to ensure that rule of law in the receiving state is applied».*

[329] *European Data Protection Supervisor, Opinion 1/2022 on the two Proposals for Council Decisions authorising Member States to sign and to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, 20 gennaio, 2022, https://edps.europa.eu/system/files/2022-04/22_01_20_opinion_en.pdf .

- riservarsi il diritto di non applicare l'art. 7 in relazione a specifici tipi di numeri di accesso,
- di richiedere la notifica simultanea dell'ordine, *ex*. art. 7 co. 5, e di designare un'autorità giudiziaria indipendente a tal fine.

Anche la Commissione ha proposto agli Stati membri di applicare la riserva prevista per l'art. 7, per intero o in relazione a specifici tipi di numeri di accesso, e li ha incoraggiati a riservarsi il diritto di non applicare l'art. 8 in relazione ai *traffic data*. Ha inoltre raccomandato di indicare quale autorità designata per ricevere la notifica quella giudiziaria o altra autorità indipendente[330].

4.2. Il percorso nell'ambito dell'Unione europea: dall'Accordo di Schengen agli strumenti di mutuo riconoscimento

In ambito europeo, dopo l'Accordo di Schengen[331], l'abolizione delle frontiere ha contribuito ad ampliare le opportunità di sviluppo delle organizzazioni criminali, rendendo necessario un rafforzamento della cooperazione tra forze di polizia e autorità giudiziarie attraverso la Convenzione di applicazione dell'accordo stesso (CAAS)[332].

L'art. 48 del testo chiarisce che le disposizioni sono complementari a quelle della Convenzione europea di mutua assistenza giudiziaria penale del 1959 e che non è pregiudicata l'applicazione di norme più favorevoli contenute in accordi bilaterali tra le Parti contraenti. Tuttavia, la CAAS ha segnato un rilevante cambio di passo: sul versante specifico della cooperazione, si è attuata la «giurisdizionalizzazione delle procedure di assistenza a scapito della loro usuale connotazione politica»[333], sostituendo la trasmissione ministeriale

[330] Cfr. *European Digital Rights (EDRI), Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention*, https://edri.org/wp-content/uploads/2022/04/EDRi-Position-Ratification-EU-Member-States-Cybercrime-Second-Additional-Protocol.pdf .
[331] Accordo fra i Governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni, aperto alla firma il 14 giugno 1985. L'accordo è completato dalla Convenzione di applicazione, firmata il 19 giugno 1990 ed entrata in vigore il 26 marzo 1995, in L-239 del 22 settembre 2000. Accordo e Convenzione costituiscono *l'acquis* di Schengen e sono, inoltre, ricompresi all'interno *dell'acquis* comunitario. L'Accordo nasce dalla consapevolezza che «l'Unione sempre più stretta fra i popoli degli Stati membri delle Comunità europee deve trovare la propria espressione nella libertà di attraversamento delle frontiere interne da parte di tutti i cittadini degli Stati membri e nella libera circolazione delle merci e dei servizi» e che la libera circolazione tra le frontiere comuni sia il mezzo per rafforzare la solidarietà tra i popoli.
[332] Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i Governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni, in G.U.U.E., L-239 del 22 settembre 2000.
[333] BELFIORE R., *La prova penale "raccolta" all'estero*, cit., p. 139.

con un rapporto diretto tra le autorità giudiziarie interessate, pur mantenendo la possibilità di utilizzare i canali ministeriali come punti di riferimento per l'invio delle domande[334].

Una tappa importante nei rapporti tra i Paesi dell'UE è stata segnata dalla stipula della Convenzione di assistenza giudiziaria in materia penale tra gli Stati membri UE[335], firmata a Bruxelles il 29 maggio 2000.

Tale convenzione si ispira a quella di Strasburgo del 1959 e integra le disposizioni precedenti e i relativi protocolli, che rimangono in vigore per questioni da questa non regolate[336].

Anche questo strumento ha attuato la giurisdizionalizzazione delle procedure, lasciando impregiudicata la facoltà di coinvolgere le autorità centrali o, in caso di urgenza, l'INTERPOL o qualsiasi organo competente secondo il Trattato dell'Unione europea.

Sul versante probatorio, allo Stato di emissione è consentito richiedere l'adozione di specifiche formalità per il compimento degli atti, qualora risultino di fondamentale importanza per la successiva spendibilità dell'atto nell'ordinamento interno. Queste richieste dovranno essere rispettate dallo Stato di esecuzione, a meno che non contrastino con i principi fondamentali dell'ordinamento[337]. In caso di difficoltà, è previsto uno scambio di comunicazioni tra le autorità coinvolte, in modo da chiarire quali condizioni devono trovare attuazione.

Riguardo ai tempi di esecuzione, le richieste andranno eseguite «il più rapidamente possibile»,[338] tenendo eventualmente conto di specifici termini – giustificati sulla base di specifiche necessità – indicati dallo Stato richiedente.

È prevista un'estensione dell'ambito di applicazione rispetto alla Convenzione di Strasburgo e all'Accordo di Schengen.

E, infatti, l'assistenza giudiziaria potrà essere prestata non solo per i procedimenti penali, ma anche per:

- quelli relativi ad atti che, in base al diritto nazionale dello Stato membro richiedente o dello Stato membro richiesto, o ad entrambi, sono punibili a titolo di infrazioni a norme di diritto, promossi da autorità amministrative e contro la decisione delle

[334] Cfr. Art. 53 CAAS: «1. Le domande di assistenza giudiziaria possono essere fatte direttamente tra le autorità giudiziarie e nello stesso modo possono essere rinviate le risposte. 2. Le disposizioni del paragrafo 1 lasciano impregiudicata la facoltà di inviare e rinviare domande da un Ministero della giustizia all'altro o per il tramite degli uffici centrali nazionali dell'Organizzazione internazionale di polizia criminale».
[335] Atto del Consiglio che stabilisce, conformemente all'articolo 34 del trattato sull'Unione europea, la convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea, firmato il 29 maggio 2000 a Bruxelles, in G.U.U.E., C-197, 12 luglio 2000.
[336] Art. 1, "Rapporti con altre convenzioni in materia di assistenza giudiziaria".
[337] Art. 4, co. 1.
[338] Art. 4, co. 2.

quali possa essere proposto ricorso dinanzi a una giurisdizione competente, in particolare, in materia penale;

- procedimenti penali e procedimenti di cui sopra, relativi a reati o infrazioni per cui nello Stato richiedente possa essere fatta valere la responsabilità di una persona giuridica (art. 3).

La Convenzione promuove, inoltre, il principio di disponibilità[339], poiché prevede che le autorità degli Stati membri si scambino spontaneamente informazioni anche in assenza di un'apposita richiesta e che possa essere consentito il loro utilizzo nel rispetto di specifiche condizioni (art. 7).

4.2.1. Il principio del mutuo riconoscimento: da alternativa al ravvicinamento delle legislazioni a pilastro della cooperazione giudiziaria

Il principio del mutuo riconoscimento è stato originariamente concepito in relazione alla libera circolazione delle merci, come testimonia la nota sentenza *Cassis de Dijon* [340] . Nella decisione in questione, infatti, il mutuo riconoscimento è stato indicato quale elemento propulsore del mercato comune, in assenza di misure di armonizzazione del diritto interno[341].

---

[339] Il principio di disponibilità è posto alla base della cooperazione delle forze di polizia e prevede lo scambio di informazioni all'interno dello spazio europeo. È stato consacrato dal c.d. "Programma dell'Aja" adottato dal Consiglio europeo del 4 e 5 novembre 2004. Vedasi Consiglio europeo di Bruxelles, 4-5 novembre 2004: «ciò significa che, in tutta l'Unione, un ufficiale di un servizio di contrasto di uno Stato membro che ha bisogno di informazioni nell'esercizio delle sue funzioni può ottenere tali informazioni da un altro Stato membro, e che il servizio di contrasto nell'altro Stato membro che dispone di tali informazioni è tenuto a trasmettergliele per i fini dichiarati, tenendo conto dei requisiti relativi alle indagini in corso nel suddetto Stato». SÁNCHEZ BARRIOS M.I., *Análisis sobre la protección de datos personales y el principio de disponibilidad en el ámbito de la cooperación judicial penal en la Union Europea* in FONTESTAD PORTALÈS L., JIMÈNEZ LÓPEZ M. de las Nieves (a cura di), *A vueltas con la transformación digital de la cooperación jurídica penal internacional,* Aranzadi, 2022.

[340] CGUE, 20 febbraio 1979, C-120/78, *Rewe- Zentral AG c. Bundesmonopolverwaltung für Branntwein*. Nel caso particolare, la parte attrice intendeva importare in Germania dalla Francia una partita del liquore fruttato *Cassis de Dijon*. Le veniva, tuttavia, negata l'autorizzazione per importarlo dall'Amministrazione del monopolio dell'alcol (*Bundesmonopolverwaltung*). Le ragioni poste alla base del diniego consistevano nel fatto che il prodotto non possedesse i requisiti necessari per essere commerciato in Germania, presentando un tasso alcolico del 15-20% a fronte del 25% richiesto dalla legge tedesca per commerciare liquori fruttati. Il tribunale finanziario dell'Assia ha sottoposto la questione alla Corte di giustizia, che ha statuito che le difformità delle legislazioni nazionali sulla produzione e sul commercio dei prodotti non possono ostacolare la libera circolazione delle merci, tranne in caso di esigenze imperative quali l'efficacia dei controlli fiscali, la protezione della salute pubblica, la lealtà dei negozi commerciali e la difesa dei consumatori. Pertanto, le prescrizioni nazionali che non perseguono uno scopo di interesse generale non possono prevalere sulla libera circolazione delle merci, in quanto principio fondamentale della Comunità europea.

[341] V. GERACI R. M., *Il mutuo riconoscimento nella cooperazione processuale: genesi, sviluppi, morfologiche,* cit., p. 66: «Un'attenta analisi della portata e del funzionamento del criterio in esame evidenzia come esso, più che costituire veicolo di efficacia *ultra moenia* degli interessi pubblici nazionali, sia piuttosto

I suoi confini, dapprima circoscritti alle questioni relative al mercato comune, sono stati successivamente estesi in maniera progressiva fino a ricomprendere anche l'ambito della cooperazione giudiziaria. Ciò anche in ragione delle spinte di Paesi, quali Regno Unito e Finlandia, che lo vedevano come una valida alternativa all'armonizzazione delle legislazioni nazionali, da questi fortemente osteggiata.

«Preso atto delle pressoché insormontabili difficoltà incontrate dalle politiche di omogeneizzazione normativa all'uopo avviate, si è individuata quale opzione sostitutiva l'espansione dell'ambito di validità dei provvedimenti giurisdizionali nazionali, vagheggiandone una libera circolazione all'incirca analoga a quella dei fattori produttivi nell'ambito del mercato interno»[342].

«Il principio del mutuo riconoscimento comporta una sorta di ultra territorialità dell'applicazione delle legislazioni degli Stati membri, conferendo una potenzialità espansiva straordinaria al *corpus* del diritto dell'Unione europea. L'estrema funzionalità del principio consiste nell'ovviare alle divergenze normative esistenti fra gli Stati membri, vincolandoli alla presunzione di rispetto del diritto dell'Unione da parte di ogni altro Stato membro»[343].

Tale concetto è stato ulteriormente rilanciato in occasione del Consiglio europeo di Cardiff[344] del 15 e 16 giugno 1998, in cui per la prima volta il principio è riferito alla cooperazione giudiziaria in ambito civile e penale.

La spinta in avanti è provenuta proprio dal Governo britannico, fermo oppositore dell'armonizzazione delle legislazioni nazionali e sostenitore, di contro, del mutuo riconoscimento in quanto alternativa al processo di omogeneizzazione legislativa.

---

il mezzo attraverso cui l'ordinamento comunitario conforma agli interessi nazionali a quelli sovraordinati, limitando i casi in cui il conseguimento di questi ultimi può essere ostacolato. Da questo punto di vista, il mutuo riconoscimento opera, infatti, come strumento di matrice eminentemente semplificatoria che, disattendendo le pretese "protezionistiche" dei Paesi membri, supporta le istituzioni comunitarie nel perseguimento degli obiettivi fondamentali dell'integrazione europea, consentendo l'abbattimento delle barriere legislative ostacolanti l'accesso ai mercati nazionali».

342 GERACI R. M., *Il mutuo riconoscimento nella cooperazione processuale: genesi, sviluppi, morfologiche*, cit., p. 72. Ed inoltre, p. 66 : «L'idea di fondo, in sostanza, era quella di *bypassare* gli ostacoli derivanti dalla « politicamente titanica opera di armonizzazione delle legislazioni penali, sia sostanziali che processuali», mettendo al contempo al riparo i Paesi membri da « ogni pretesa di intervento europeo mirante a modificare il diritto interno nella sostanza»: se, infatti, ciascuno Stato della Comunità avesse riconosciuto la validità delle decisioni emesse dalle autorità giudiziarie degli altri Paesi europei, dandovi esecuzione e facendole, così, circolare liberamente, si sarebbe arginata la produzione normativa di matrice sovraordinata, affrancando gli ordinamenti nazionali dalle conseguenti ingerenze interne».

343 GIORGI E., *Il principio del mutuo riconoscimento nell'ordinamento dell'Unione europea*, cit., p. 13 ss.

344 Consiglio europeo di Cardiff, 15 e 16 giugno 1998, Conclusioni della Presidenza, SN 15071/, § 39: «Il Consiglio europeo sottolinea l'importanza di un'efficace cooperazione giudiziaria nella lotta contro la criminalità transnazionale. Esso riconosce che occorre potenziare la capacità dei sistemi giuridici nazionali di operare in stretto contatto e chiede al Consiglio di determinare in quale misura si debba estendere il riconoscimento reciproco delle decisioni dei rispettivi tribunali».

Dello stesso orientamento anche la Finlandia, incaricata dell'organizzazione del successivo vertice di Tampere del 1999 del 15 e 16 ottobre 1999.

E proprio nelle conclusioni del Consiglio di Tampere[345] viene dedicato ampio spazio al principio del reciproco riconoscimento delle decisioni giudiziarie e delle sentenze - identificato quale «pietra angolare»[346] della cooperazione giudiziaria - ritenendolo fondamentale per la cooperazione delle autorità, al pari del ravvicinamento delle legislazioni nazionali e della tutela giudiziaria dei diritti dei singoli[347]. Nelle stesse conclusioni il Consiglio europeo aveva, inoltre, invitato il Consiglio e la Commissione ad adottare, entro dicembre 2000, un programma di misure per l'attuazione del principio.

Nel luglio 2000 la Commissione inviava la sua comunicazione[348] al Consiglio e al Parlamento europeo in cui stabiliva che il riconoscimento reciproco comportava l'automatico riconoscimento – da parte di uno Stato membro – di un atto adottato da un giudice di un altro Stato membro nell'esercizio dei suoi poteri ufficiali, esplicando effetti identici o analoghi.

E inoltre:

«si considera che il riconoscimento reciproco sia un principio basato sull'idea che, nonostante un altro Stato possa non trattare una specifica questione in maniera uguale o simile a quella dello Stato stesso, la decisione adottata sarà tale da essere accettata come equivalente alla decisione che avrebbe adottato lo Stato interessato. La reciproca fiducia, non solo nell'adeguatezza della normativa dei propri partner, bensì anche nella corretta applicazione di tale normativa, è un fattore importante del riconoscimento reciproco. […] Riconoscere una decisione estera in materia penale significa attribuire a tale decisione effetti al di fuori dello Stato in cui è stata adottata, sia attribuendole gli effetti giuridici stabiliti dal diritto penale dello Stato estero, sia tenendone conto affinché esplichi gli effetti stabiliti dal diritto penale dello Stato che ha riconosciuto tale decisione»[349].

La Commissione si occupa, inoltre, di definire il rapporto tra mutuo riconoscimento e armonizzazione, ritenendo che i due concetti procedano «spesso, ma non sempre, di pari passo»[350] e che se, da un lato, l'armonizzazione può permettere una più agevole accettazione

---

[345] Consiglio europeo di Tampere, Conclusioni della Presidenza, SN 200/99.
[346] *Ibidem*. Nella versione inglese «*The European Council therefore endorses the principle of mutual recognition which, in its view, should become the cornerstone of judicial co-operation in both civil and criminal matters within the Union. The principle should apply both to judgements and to other decisions of judicial authorities*».
[347] *Ibidem*, § 33 ss.
[348] Comunicazione della Commissione al Consiglio e al Parlamento europeo sul riconoscimento reciproco delle decisioni definitive in materia penale, 26 luglio 2000, COM /2000/0495.
[349] *Ibidem*.
[350] *Ibidem*.

degli atti svolti in un altro Stato, dall'altro, può essere vanificata dal reciproco riconoscimento.

Per una più efficace applicazione del principio, viene, inoltre, ritenuto imprescindibile il rafforzamento delle tutele dei diritti e la fissazione di norme minime comuni. In tal senso, snodo fondamentale è la consapevolezza che, per raggiungere le priorità stabilite, il riconoscimento reciproco non possa interamente sostituire il ravvicinamento delle legislazioni, ma che i due sistemi dovrebbero coesistere[351].

Il principio veniva, nuovamente, richiamato tra le priorità dell'Unione per il quinquennio 2010-2014 nel c.d. Programma di Stoccolma[352], in cui veniva ribadita la necessità di potenziare la cooperazione tra le autorità giudiziarie e il riconoscimento reciproco delle sentenze, in materia civile e penale.

La svolta decisiva è giunta, successivamente, con il Trattato di Lisbona[353] che ha conferito priorità alla costituzione di uno spazio giudiziario europeo. Il principio del riconoscimento reciproco è stato sancito dall'art. 67 TFUE [354] co. 3 e 4 e, così, inserito tra i principi di diritto primario dell'UE. La norma prevede che: «L'Unione si adopera per garantire un livello elevato di sicurezza attraverso misure di prevenzione e di lotta contro la criminalità, il razzismo e la xenofobia, attraverso misure di coordinamento e cooperazione tra forze di polizia e autorità giudiziarie e altre autorità competenti, nonché tramite il riconoscimento reciproco delle decisioni giudiziarie penali e, se necessario, il ravvicinamento delle legislazioni penali. L'Unione facilita l'accesso alla giustizia, in particolare attraverso il principio di riconoscimento reciproco delle decisioni giudiziarie ed extragiudiziali in materia civile».

---

[351] V. GRANDI C., *Il mutuo riconoscimento dei provvedimenti di confisca alla luce del Regolamento (UE) 2018/1805*, in *www.lalegislazionepenale.eu*, 2021, p. 12: «Il principio del mutuo riconoscimento è chiamato ad operare proprio laddove l'armonizzazione sia imperfetta, lubrificando i meccanismi della cooperazione transnazionale che rischiano di incepparsi dinanzi alle incongruenze tra le regole nazionali; semprechè, beninteso, al netto delle incongruenze sulle regole, tra i partner vi sia condivisione di principi e valori di fondo in misura sufficiente da giustificare la fiducia reciproca. Per altro verso, quindi, il mutuo riconoscimento richiede e presuppone una certa quota di armonizzazione, con il minimo comune denominatore del rispetto dei diritti fondamentali quale nutriente indispensabile per la *mutual trust*».

[352] Programma di Stoccolma – Un'Europa aperta e sicura al servizio e a tutela dei cittadini, G.U.U.E. C-115 del 4 maggio 2010.

[353] Trattato di Lisbona che modifica il trattato sull'Unione europea e il trattato che istituisce la Comunità europea, firmato a Lisbona il 13 dicembre 2007, entrato in vigore il 1° dicembre 2019, in G.U. C 306 del 17 dicembre 2007.

[354] Trattato sul funzionamento dell'Unione europea (versione consolidata 2016), in G.U.U.E. C 202, del 7 giugno 2016, p. 47 ss., come modificato dal Trattato di Lisbona che modifica il trattato sull'Unione europea e il trattato che istituisce la Comunità europea, firmato a Lisbona il 13 dicembre 2007, in G.U.U.E. C 306, del 17 dicembre 2007, p. 1 ss.

Il principio è stato collocato alla base della cooperazione giudiziaria in materia penale[355], stabilendo inoltre che Parlamento e Consiglio possano dettare norme comuni adottando direttive secondo la procedura legislativa ordinaria, tenendo conto delle tradizioni giuridiche differenti degli Stati membri.

Sotto l'egida dell'art. 82 TFUE è stato così avviato un processo di armonizzazione delle legislazioni nazionali attraverso una serie di direttive volte a creare un livello *standard* di tutela, quale presupposto base per la reciproca fiducia.

Gli ambiti di intervento individuati sono:

- l'ammissibilità reciproca delle prove,
- i diritti della persona nella procedura penale,
- i diritti delle vittime,
- ulteriori elementi che il Consiglio potrà individuare tramite una decisione, deliberando all'unanimità previa approvazione del Parlamento europeo.

La giurisprudenza è poi intervenuta delineandone ulteriormente i confini. A tale riguardo, vanno richiamate le sentenze della Corte di Giustizia, *N.S.*[356] , *Melloni*[357] e *Aranyosi e Căldăraru*[358]. In queste pronunce è costante l'affermazione secondo cui il "mutuo riconoscimento" impone di ritenere, tranne in circostanze eccezionali, che tutti gli

---

[355] Art. 82 TFUE, co. 1: «La cooperazione giudiziaria in materia penale nell'Unione è fondata sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e include il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri nei settori di cui al paragrafo 2 e all'articolo 83. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, adottano le misure intese a:
a) definire norme e procedure per assicurare il riconoscimento in tutta l'Unione di qualsiasi tipo di sentenza e di decisione giudiziaria;
b) prevenire e risolvere i conflitti di giurisdizione tra gli Stati membri;
c) sostenere la formazione dei magistrati e degli operatori giudiziari;
d) facilitare la cooperazione tra le autorità giudiziarie o autorità omologhe degli Stati membri in relazione all'azione penale e all'esecuzione delle decisioni».

[356] CGUE, 21 dicembre 2011, C-411/10 e C-493/10, *N. S.* : « Risulta dall'esame dei testi che istituiscono il sistema europeo comune di asilo che quest'ultimo è stato concepito in un contesto che permette di supporre che l'insieme degli Stati partecipanti, siano essi Stati membri o Paesi terzi, rispetti i diritti fondamentali, compresi i diritti che trovano fondamento nella Convenzione di Ginevra e nel Protocollo del 1967, nonché nella CEDU, e che gli Stati membri possono fidarsi reciprocamente a tale riguardo. […] Ne va, infatti, della ragion d'essere dell'Unione e della realizzazione dello spazio di libertà, di sicurezza e di giustizia e, più in particolare, del sistema europeo comune di asilo, fondato sulla fiducia reciproca e su una presunzione di osservanza, da parte degli altri Stati membri, del diritto dell'Unione, segnatamente dei diritti fondamentali».

[357] CGUE, 26 febbraio 2013, C-399/11, *Melloni*.

[358] CGUE, 5 aprile 2016, C-404//15 e C-659/15, *Aranyosi e Căldăraru*, § 77 ss.: «Il principio del mutuo riconoscimento su cui si fonda il sistema del mandato d'arresto europeo si basa esso stesso sulla fiducia reciproca tra gli Stati membri circa il fatto che i rispettivi ordinamenti giuridici nazionali sono in grado di fornire una tutela equivalente ed effettiva dei diritti fondamentali, riconosciuti a livello dell'Unione, in particolare nella Carta […] Tanto il principio della fiducia reciproca tra gli Stati membri quanto il principio del mutuo riconoscimento, nel diritto dell'Unione, rivestono un'importanza fondamentale, dato che consentono la creazione e il mantenimento di uno spazio senza frontiere interne. Più specificamente, il principio della fiducia reciproca impone a ciascuno di detti Stati, segnatamente per quanto riguarda lo spazio di libertà, di sicurezza e di giustizia, di ritenere, tranne in circostanze eccezionali, che tutti gli altri Stati membri rispettino il diritto dell'Unione e, più in particolare, i diritti fondamentali riconosciuti da quest'ultimo».

altri Stati membri rispettano il diritto dell'Unione e i diritti fondamentali riconosciuti da quest'ultimo. In tal senso, il rispetto dei diritti fondamentali, nell'attuazione del diritto dell'Unione, è presunto.

Ciò preclude ad ogni Stato di esigere da un altro Stato membro un livello di tutela nazionale dei diritti più elevato di quello garantito dal diritto dell'Unione, ma anche, salvo casi eccezionali, quella di verificare se in un caso concreto, siano stati effettivamente rispettati i diritti fondamentali garantiti dall'Unione[359].

Tra gli strumenti più significativi di mutuo riconoscimento adottati in ambito europeo e rilevanti nel settore che riguarda le prove si possono richiamare:

- la decisione quadro 2003/577/GAI relativa ai provvedimenti di blocco e sequestro dei beni[360],
- il mandato europeo di ricerca delle prove[361],
- l'ordine europeo di indagine.

4.2.2. I provvedimenti di blocco e sequestro dei beni

La Decisione quadro 2003/577/GAI ha applicato il mutuo riconoscimento alle decisioni di blocco e sequestro[362] dei beni emesse ai fini probatori o per la successiva confisca, permettendone l'esecuzione all'interno degli Stati membri senza la previsione di un riesame o di specifiche formalità.

---

[359] CGUE, parere 18 dicembre 2014, n. 2/13, *Adhésion de l'Union à la CEDH*, § 191 - 192: «In secondo luogo, occorre ricordare che il principio della fiducia reciproca tra gli Stati membri riveste, nel diritto dell'Unione, un'importanza fondamentale, dato che consente la creazione e il mantenimento di uno spazio senza frontiere interne. Orbene, tale principio impone a ciascuno di detti Stati, segnatamente per quanto riguarda lo spazio di libertà, di sicurezza e di giustizia, di ritenere, tranne in circostanze eccezionali, che tutti gli altri Stati membri rispettano il diritto dell'Unione e, più in particolare, i diritti fondamentali riconosciuti da quest'ultimo. Allorché attuano il diritto dell'Unione, gli Stati membri possono quindi essere tenuti, in forza di quest'ultimo, a presumere il rispetto dei diritti fondamentali da parte degli altri Stati membri, sicché risulta ad essi preclusa non soltanto la possibilità di esigere da un altro Stato membro un livello di tutela nazionale dei diritti fondamentali più elevato di quello garantito dal diritto dell'Unione, ma anche, salvo casi eccezionali, quella di verificare se tale altro Stato membro abbia effettivamente rispettato, in un caso concreto, i diritti fondamentali garantiti dall'Unione».

[360] Decisione quadro 2003/577/GAI del Consiglio, del 22 luglio 2003, relativa all'esecuzione nell'Unione europea dei provvedimenti di blocco o di sequestro probatorio, in G.U.U.E. L/196 del 02 agosto 2003.

[361] Decisione quadro 2008/978/GAI del Consiglio, del 18 dicembre 2008, relativa al mandato europeo di ricerca delle prove diretto all'acquisizione di oggetti, documenti e dati da utilizzare nei procedimenti penali, in G.U. L/350 del 30 dicembre 2008.

[362] Ai sensi dell'art. 2 c): «qualsiasi provvedimento adottato da un'autorità giudiziaria competente dello Stato di emissione per impedire provvisoriamente ogni operazione volta a distruggere, trasformare, spostare, trasferire o alienare beni che potrebbero essere oggetto di confisca o costituire una prova».

In tal modo, in seguito all'emissione di un certificato *standard* da parte dello Stato di emissione, lo Stato destinatario di tale richiesta riconosceva ed eseguiva i provvedimenti alla stregua di un atto interno (art. 5).

La trasmissione del modulo *standard* avveniva tra le autorità giudiziarie dei Paesi membri ed era seguita, dopo il riconoscimento, dall'esecuzione immediata, previa osservanza del requisito della doppia incriminazione, ad accezione di un *numerus clausus* di reati (art. 3 co. 2).

La decisione era finalizzata ad evitare la distruzione, la trasformazione, lo spostamento o l'alienazione di beni che potessero costituire elementi probatori. A tale scopo, poteva anche essere richiesto il rispetto di specifiche modalità procedurali in ossequio alla *lex fori*, per poter poi garantire che le prove acquisite fossero utilizzabili all'interno di un processo. Tali richieste, tuttavia, non potevano contrastare con i principi fondamentali dello Stato di esecuzione.

La portata di tale decisione era, tuttavia, depotenziata dal fatto che, pur potendosi inserire nel modulo una richiesta di trasferimento delle prove, il passaggio successivo richiedeva comunque l'attivazione di un'apposita rogatoria.

A causa della mancanza di un'applicazione uniforme della disciplina, il legislatore europeo ha, quindi, optato, per l'emanazione del Regolamento 2018/1805/UE[363], che ha abrogato la decisione 2003/577/GAI, per la parte sul congelamento, e la decisione 2006/783/GAI[364] in relazione alla confisca.

4.2.3. Il mandato europeo di ricerca delle prove

Il primo tentativo di applicazione del mutuo riconoscimento in materia di raccolta e acquisizione delle prove all'estero è stato fatto con il mandato europeo di ricerca delle prove (MER), adottato con la Decisione quadro 2008/978/GAI, strumento rivelatosi del tutto inefficace[365].

Nello specifico, il mandato – espressione del principio del reciproco riconoscimento – era da considerare quale «decisione giudiziaria emessa da un'autorità competente di uno

[363] Regolamento 2018/1805/UE del 14 novembre 2018 relativo al riconoscimento reciproco dei provvedimenti di congelamento e di confisca in G.U.U.E L 303/1 del 28 novembre 2018.
[364] Decisione Quadro 2006/783/GAI del Consiglio del 6 ottobre 2006 relativa all'applicazione del principio del reciproco riconoscimento delle decisioni di confisca, in G.U.U.E. L 328/59 del 24 novembre 2006.
[365] AGUILERA MORALES M., *El Exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas*, in *Boletín del Ministerio de Justicia*, 2021, 2145, p. 5; DE AMICIS G., *Limiti e prospettive del mandato europeo di ricerca della prova*, in *Dir. Pen. Cont.*, 5 aprile 2011.

Stato membro allo scopo di acquisire oggetti, documenti e dati da un altro Stato membro ai fini del loro uso»[366] nei procedimenti penali o di altro tipo, compresi quelli amministrativi, la cui decisione potesse proseguire dinanzi a organi giurisdizionali competenti in materia penale, relativi a persone fisiche o giuridiche[367].

Lo strumento scontava un limite: l'ambito di applicazione era riservato alle prove precostituite, con esclusione di quelle dichiarative, scientifiche, delle intercettazioni, dell'acquisizione dei tabulati telefonici e telematici, a meno che non fossero siano già in possesso dell'autorità di esecuzione prima dell'emissione del mandato[368].

Era, tuttavia, consentito raccogliere dichiarazioni dalle persone presenti al momento di esecuzione dell'atto, in conformità alla *lex loci*[369]. La limitazione nell'uso dello strumento alle sole prove precostituite finiva per appesantire la procedura, con il rischio di dovere ricorrere a istituti diversi in relazione alla tipologia di prova da assumere: se precostituita o meno. Questa circostanza, unita alla volontà di non limitare la sovranità nazionale, ha portato solo un numero ristretto di Stati ad implementare il MER.

Tuttavia, tra gli aspetti rilevanti di questa misura va sottolineata l'eliminazione del filtro ministeriale, l'individuazione delle autorità competenti, identificate nel giudice, un organo giurisdizionale, un magistrato inquirente, un pubblico ministero o qualsiasi altra autorità giudiziaria definita dallo Stato di emissione che, nel caso specifico, agisca nella sua qualità di autorità inquirente nei procedimenti penali e sia competente a ordinare l'acquisizione dei mezzi di prova nei casi transfrontalieri in base alla legislazione nazionale.

La scelta dell'autorità di esecuzione veniva, invece, rimessa alla discrezionalità degli Stati, che avrebbero dovuto definirla nella legislazione di recepimento.

---

366 Art. 1, Decisione quadro 2008/978/GAI.

367 Art. 5, Decisione quadro 2008/978/GAI.

368 Art. 4, co. 2, Decisione quadro 2008/978/GAI: «Il MER non è emesso allo scopo di richiedere all'autorità di esecuzione di:

a) condurre interrogatori, raccogliere dichiarazioni o avviare altri tipi di audizioni di indiziati, testimoni, periti o di qualsiasi altra parte;
b) procedere ad accertamenti corporali o prelevare materiale biologico o dati biometrici direttamente dal corpo di una persona, ivi compresi campioni di DNA o impronte digitali;
c) c)acquisire informazioni in tempo reale, ad esempio attraverso l'intercettazione di comunicazioni, la sorveglianza discreta dell'indiziato o il controllo dei movimenti su conti bancari;
d) condurre analisi di oggetti, documenti o dati esistenti;
e) ottenere dati sulle comunicazioni conservati dai fornitori di servizi di comunicazioni elettroniche accessibili al pubblico o di una rete pubblica di comunicazione».

Ed anche, Art. 4, co. 4: «4. Il MER può essere emesso per acquisire gli oggetti, i documenti o i dati di cui al paragrafo 2, laddove tali oggetti, documenti o dati sono già in possesso dell'autorità di esecuzione prima dell'emissione del MER».

369 *Ibidem*, «Fatto salvo il paragrafo 2, il MER, se richiesto dall'autorità di emissione, può riguardare anche la raccolta di dichiarazioni di persone presenti all'atto dell'esecuzione del MER e direttamente collegate all'oggetto dello stesso. Per la raccolta di tali dichiarazioni sono altresì di applicazione le norme pertinenti dello Stato di esecuzione applicabili ai casi nazionali».

Il MER, diversamente dalla decisione sul provvedimento di blocco e sequestro dei beni, prevedeva anche il trasferimento delle prove, così evitando la necessità di dovere ricorrere alla rogatoria per entrare in possesso dei dati.

Il riconoscimento e l'esecuzione del mandato erano subordinati alla doppia incriminazione solo nel caso in cui fosse necessario compiere atti di perquisizione e sequestri, ad eccezione di una lista di reati (indicati all'articolo 14)[370], qualora fossero punibili nello Stato di emissione con una pena o misura di sicurezza privativa della libertà della durata massima di almeno tre anni.

Con il Programma di Stoccolma, adottato il 10-11 dicembre 2009, il Consiglio ha annunciato i criteri ispiratori e le priorità politiche dell'azione dell'Unione nel quinquennio 2010-2014 e invitato la Commissione a «proporre un sistema globale […] in sostituzione di tutti gli strumenti esistenti nel settore» per l'acquisizione probatoria nelle cause aventi dimensione transfrontaliera, basato anch'esso sul riconoscimento reciproco[371].

---

[370] Art.14: «1. Il riconoscimento o l'esecuzione del MER non è subordinato alla verifica della doppia incriminazione se non è necessario effettuare una perquisizione o un sequestro.
2. Se è necessario effettuare una perquisizione o un sequestro per eseguire il MER, i seguenti reati, qualora siano punibili nello Stato di emissione con una pena o una misura di sicurezza privative della libertà della durata massima di almeno tre anni e quali definiti dalla legislazione di detto Stato membro, non sono sottoposti alla verifica della doppia incriminazione in alcuna circostanza: partecipazione a un'organizzazione criminale, terrorismo, tratta di esseri umani, sfruttamento sessuale dei bambini e pornografia infantile, traffico illecito di stupefacenti e sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, corruzione, frode, compresa la frode che lede gli interessi finanziari delle Comunità europee ai sensi della convenzione del 26 luglio 1995 relativa alla tutela degli interessi finanziari delle Comunità europee, riciclaggio di proventi di reato, falsificazione e contraffazione di monete, tra cui l'euro, criminalità informatica, criminalità ambientale, compreso il traffico illecito di specie animali protette e il traffico illecito di specie e di essenze vegetali protette, favoreggiamento dell'ingresso e del soggiorno illegali, omicidio volontario, lesioni personali gravi, traffico illecito di organi e tessuti umani, sequestro di persona, sequestro e presa di ostaggi, razzismo e xenofobia, rapina organizzata o a mano armata, traffico illecito di beni culturali, compresi gli oggetti d'antiquariato e le opere d'arte, truffa, racket ed estorsione, contraffazione e pirateria in materia di prodotti, falsificazione di atti amministrativi e traffico di documenti falsi, falsificazione di mezzi di pagamento, traffico illecito di sostanze ormonali e altri fattori di crescita, traffico illecito di materie nucleari e radioattive, traffico di veicoli rubati, violenza sessuale, incendio doloso, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, dirottamento di aeromobile/nave, sabotaggio.
3. Qualora il MER non si riferisca ad alcuno dei reati di cui al paragrafo 2 e l'esecuzione dello stesso comporti il ricorso alla perquisizione o al sequestro, il riconoscimento o l'esecuzione del MER può essere subordinato alla condizione della doppia incriminazione.
In relazione a reati in materia di tasse o imposte, di dogana e di cambio, il riconoscimento o l'esecuzione del mandato non può essere rifiutato a motivo del fatto che la legislazione dello Stato di esecuzione non impone lo stesso tipo di tasse o imposte o non prevede lo stesso tipo di regolamenti in materia di tasse o imposte, di dogana e di cambio della legislazione dello Stato di emissione».
[371]Consiglio europeo, Programma di Stoccolma – Un'Europa aperta e sicura al servizio e alla tutela dei cittadini, 2010/C 115/01, § 3.1.1.: «Il Consiglio europeo ritiene che debba proseguire ulteriormente l'istituzione di un sistema generale di acquisizione nelle cause aventi dimensione transfrontaliera, basato sul principio di riconoscimento reciproco. Gli strumenti esistenti nel settore costituiscono una disciplina frammentaria. È necessario un nuovo approccio che, pur ispirandosi al principio di riconoscimento reciproco, tenga conto altresì della flessibilità del sistema tradizionale di assistenza giudiziaria reciproca. Tale nuovo modello potrebbe essere di più ampia portata e dovrebbe contemplare quanti più tipi di prove possibile, nel rispetto delle misure interessate». Vedasi BACHMAIER WINTER L., *Prueba transnacional penal en Europa: la Directiva 2014/41 relativa a la orden europea de investigacion*, in *Revista general de derecho europeo*, 2015; DANIELE M., *L'impatto dell'ordine europeo di indagine penale sulle regole probatorie nazionali*, in *Dir. Pen. Cont. Rivista*

Successivamente, il 29 aprile 2010 un gruppo composto da 7 Stati membri[372] ha avanzato una proposta di direttiva del Parlamento e del Consiglio relativa all'ordine europeo di indagine penale, strumento omnicomprensivo valido per ogni tipo di prova e in grado di sostituire quelli fino ad allora utilizzati.

La proposta ha ottenuto il consenso il 14 dicembre 2011 e, a seguito di ulteriori emendamenti, approvati il 27 febbraio 2014, è stata emanata in data 3 aprile 2014.

4.2.4. L'ordine europeo di indagine penale

Con la Direttiva 2014/41/UE (D/OEI) è stato introdotto un meccanismo di cooperazione di natura "ibrida": nell'ordine europeo di indagine penale, infatti, convivono tratti degli strumenti di mutuo riconoscimento con la flessibilità tipica dei meccanismi di assistenza giudiziaria[373].

---

trimestrale, 2016, 3; ESPINA RAMOS J.A., *The European investigation order and its relationship with other judicial cooperation instruments*, in www.eucrim.eu, 2019.

[372] Belgio, Bulgaria, Estonia, Austria, Slovenia, Svezia, Spagna. In argomento v. MANGIARACINA A., *A new and controversial scenario in the gathering of evidence at the european level: the proposal for a directive on the european investigation order*. in *Utrecht Law Review*, 2014, 10; PISANI M.M., *Problemi di prova in materia penale. La proposta di direttiva sull'Ordine Europeo di Indagine,* in *Arch. Pen.,* 2011.

[373] La direttiva è stata recepita in Italia con il d. lgs. 21 giugno 2017, n. 108, entrato in vigore il 28 luglio 2019, G.U. n. 162 del 13 luglio 2017. Per approfondimenti v. BENE T., LUPARIA L., MARAFIOTI L., *L'ordine europeo di indagine*, G. Giappichelli Editore, 2016; GERACI R.M., *Primi disorientamenti interpretativi in tema di OEI: la Cassazione interviene sulle corrette modalità del giudizio di riconoscimento*, in *Proc. Pen. Giust.*, 2019, 5, p. 1157; MANGIARACINA A., *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale*, in *Dir. Pen. proc.,* 2018, 2, p. 158; RUGGIERI F., *Le nuove frontiere dell'assistenza penale internazionale: l'ordine europeo di indagine penale*, in *Proc. Pen. Giust.*, 2018, 1, p. 131; RUGGERI E., *L'ordine europeo di indagine – EIO: come funziona?*, in *Cass. Pen.*, 1, 2017; SELVAGGI E., *La circolare del Ministero della Giustizia sul c.d. ordine europeo di indagine*, in *Dir. Pen. Cont.*, 7 novembre 2017; SIRACUSANO F., *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, in *Arch. Pen.*, 2017, 2.
In Spagna è stata, invece, recepita con la *Ley 3/2018 de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, para regular la Orden Europea de Investigación,* in BOE n. 142 del 12 giugno 2018. Per approfondimenti: AGUILERA MORALES M., *Las diligencias de investigación fiscal*, Aranzadi, 2015, p. 165; BACHMAIER WINTER L., *Transnational Evidence: Towards the Transposition of the Directive 2014/41 Regarding the European Investigation Order in Criminal Matters*, in www.eucrim.eu, 2015, p. 47; BURGOS LADRÓN DE GUEVARA J., *La orden europea de investigación penal en España: aplicación y contenido. Posible relación con la orden europea de protección,* in *Diario La Ley,* 2015, 8660; CAIANIELLO M., *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Proc. Pen. Giust.,* 2015, 3, p. 2; GARCIMARTIN MONTERO R., *The european investigation order ad the respect for fundamental rights in criminal investigations,* in *www.eucrim.eu,* 2017, n 1; JÍMENEZ LÓPEZ M. de las Nieves, *Las medidas de investigación tecnológicas en la orden europea de investigación*, in FONTESTAD PORTALÈS L., JIMÈNEZ LÓPEZ M., *La transformación digital de la cooperación jurídica penal internacional*, Aranzadi, 2021; JIMENO BULNES M., *Aproximación legislativa versus reconocimiento mutuo en el desarrollo del espacio judicial europeo: una perspectiva multidisciplinar,* Bosch Editor, 2016; MARTINEZ GARCÍA E., *La orden de investigación europea. Las futuras complejidades previsibles en la implementación de la Directiva en España*, in *La Ley Penal*, 2014, 106; MARTINEZ GARCÍA E., *La orden europea de investigación*, Tirant Lo Blanch, 2016; RODRIGUEZ MEDEL NIETO C., *Obtención y admisibilidad en España de la prueba penal transfronteriza*, Aranzadi, 2016; SÁNCHEZ ARJONA M. L., *La Orden Europea de Investigación y su incorporación al derecho español*, Tirant lo Blanch, 2020; TINOCO

Volendo sintetizzare, la Direttiva risponde ai seguenti principi[374]:

a) semplificazione e rapidità: un formulario *standard* e la previsione di termini stringenti per l'esecuzione hanno la funzione di ridurre i tempi, rendendo più agevole la cooperazione;

b) orizzontalità: l'OEI è in grado di «attirare nel proprio ambito di applicazione ogni tipo di mezzo di prova e di ricerca della prova»[375];

c) onnicomprensività: l'OEI, infatti, ha sostituito le disposizioni corrispondenti dei precedenti strumenti di cooperazione previsti in materia probatoria[376].

Sul piano definitorio, l'OEI è una decisione giudiziaria emessa o convalidata da un'autorità competente di uno Stato membro (*Stato di emissione*) per compiere uno o più atti di indagine specifici in un altro Stato membro (*Stato di esecuzione*) ai fini dell'acquisizione probatoria[377]. A differenza del MER, l'istituto può essere utilizzato per il compimento di qualsiasi atto di natura probatoria – con specifiche disposizioni relative ad alcuni atti[378] – e comprende anche le prove già in possesso dello Stato di esecuzione.

PASTRANA A., *El embargo preventivo y el aseguramiento de pruebas en los procesos penales en la Unión Europea. Novedades tra la Ley 23/2014, de reconocimiento mutuo de resoluciones penales en la Unión Europea y la Directiva 2014/41/CE relativa a la orden europea de investigación en materia penal,* in *Cuadernos Europeos de Deusto,* 2015, 52; VALLS PRIETO J., *Un ejemplo de análisis empírico en el derecho penal basado en una metodología mixta : la Orden Europea de Investigación*, Editorial Comares, 2022; Per un'analisi sull'applicazione dell'OEI vedasi EUROJUST, *Report on Eurojust's casework in the field of the European Investigation Order*, 25 novembre 2020, https://www.eurojust.europa.eu/publication/report-eurojust-casework-european-investigation-order e ESPOSITO G., *Analisi del "Report on Eurojust's casework in the field of the European Investigation Order*", in *Proc. Pen. Giust.*, 2021, 3, p. 677.

[374] In proposito AGUILERA MORALES M., *El Exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas*, in *Boletín del Ministerio de Justicia* n. 2145, p. 5. L'autrice indica come pilastri della Proposta della Direttiva*: reunificación normativa, horizontalidad o centralidad; simplificación y celeridad procedimental; reforzamiento del principio de reconocimiento mutuo*.

[375] BELFIORE R., *La prova penale "raccolta" all'estero,* cit., p. 206.

[376] La Convenzione di Strasburgo del 1959, i relativi Protocolli aggiuntivi del 17 marzo 1978 e dell'8 novembre 2001 e accordi bilaterali conclusi in virtù di tale convenzione; la Convenzione di applicazione dell'Accordo di Schengen; la Convenzione di Bruxelles del 2000 e il relativo Protocollo del 16 ottobre 2001; la Decisione quadro 2003/577/GAI relativa ai provvedimenti di blocco e sequestro dei beni, per quanto concerne il sequestro probatorio, e la Decisione quadro 2008/978/GAI sul mandato europeo di ricerca delle prove. Cfr. DE AMICIS G., *Dalle rogatorie all'ordine europeo di indagine: verso un nuovo diritto della cooperazione giudiziaria penale*, in *Cass. Pen.*, 2018, 1, p. 26. Si precisa, tuttavia, che l'OEI non è applicabile per le richieste di assistenza riguardanti ambiti non disciplinati dall'OEI, per i rapporti con Stati dell'Unione non aderenti alla direttiva (Irlanda e Danimarca) e con Stati terzi.

[377] Art. 1, Direttiva 2014/41/UE.

[378] Trasferimento temporaneo di persone detenute per realizzare atti di indagine, audizione mediante videoconferenza, informazioni su conti ed operazioni bancarie e finanziarie, operazioni di infiltrazione, intercettazioni di telecomunicazioni. Per approfondimenti BACHMAIER, L., *Mutual recognition and cross-border interception of communications: the way ahead for the European Investigation Order*, Hart Publising, 2017.

È espressamente esclusa la creazione di squadre investigative comuni – governate dalla Decisione quadro 2002/465/GAI[379] – e l'acquisizione di prove nell'ambito di tali squadre[380].

L'emissione di un OEI può collocarsi nell'ambito di procedimenti penali avviati da un'autorità giudiziaria o promossi davanti questa, per fatti qualificati come illeciti dalla legge dello Stato di emissione e, ancora, di procedimenti avviati da autorità amministrative o autorità giudiziarie, quando la decisione possa sfociare in un procedimento davanti ad un organo giurisdizionale competente in materia penale.

Se, dal punto di vista dell'autorità emittente, il testo si colloca sul solco della tradizione – potendo l'ordine essere emesso da un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero competente nel caso interessato o da qualsiasi altra autorità competente, che agisca come autorità inquirente nel procedimento penale secondo la legge dello Stato di emissione[381] – la vera novità si registra sul fronte della difesa: questa è, infatti, legittimata a richiedere l'emissione dell'ordine, conformemente al diritto e alla procedura penale nazionale[382]. Tuttavia, va evidenziato come non sia stata raggiunta una parità di posizioni tra accusa e difesa e, invece, il rinvio alle disposizioni nazionali possa aumentare la frammentazione o anche, come nel caso italiano – in cui la richiesta viene "canalizzata" attraverso l'autorità competente designata – porre la difesa in una posizione di svantaggio[383].

---

[379] Disciplinate dalla Decisione quadro 2002/465/GAI del Consiglio, del 13 giugno 2002, relativa alle squadre investigative comuni, in G.U.U.E. L/162 del 20 giugno 2002, p. 1-3. Recepita in Italia dal d. Lgs. 15 febbraio 2016, n. 34. Le squadre investigative comuni potranno, tuttavia, avvalersi di tale strumento per acquisire prove da Stati che non abbiano partecipato alla costituzione della squadra o da Stati terzi.

[380] Ed infatti tale restrizione risulta adeguata per la differenza tra i differenti principi e meccanismi che stanno alla base dell'OEI e di tali squadre: nonostante i fini siano parzialmente coincidenti, mentre l'OEI si fonda sul tentativo di rafforzare il principio di mutuo riconoscimento, le squadre investigative comuni nascono dalla volontà degli Stati di attuare una cooperazione mirata e possono estendersi anche a Stati che non facciano parte dell'Unione. Vedasi BACHMAIER WINTER L., *Prueba transnacional penal en Europa: la Directiva 2014/41 relativa a la orden europea de investigacion*, in *Revista general de derecho europeo.* 2015,36, p. 5.

[381] Ar. 2 lett. c) D/OEI. La scelta del legislatore europeo di inserire "qualsiasi altra autorità competente" secondo la legislazione dello Stato di emissione è dettata dalle notevoli differenze in materia processuale tra gli Stati membri. Tale scelta è frutto dell'importanza che, a livello processuale, rivestono le autorità amministrative in numerosi Stati. V. RUGGERI E., "*L'ordine europeo di indagine – EIO:come funziona?,* in *Cass. Pen.*, 2017, p. 46: «Si è inteso farsi carico di quei provvedimenti, tipici del diritto austriaco e tedesco, che sono gli *Ordnungswidrigkeiten*, che fanno riferimento a infrazioni sanzionate sul piano amministrativo ma avverso le quali è possibile proporre appello sul quale si pronuncia l'autorità giudiziaria».

[382] In proposito UBERTIS G., *Considerazioni generali su investigazioni e prove transnazionali.* in *Cass. Pen.,* 2017, p. 51. Sulle indagini difensive e l'OEI vedasi GRIFANTINI F.M., *Ordine europeo di indagine penale e investigazioni difensive*, in *Proc. Pen. Giust.*, 2016, 6, p. 1.

[383] La disposizione è coerente con i modelli di processo inquisitorio, in cui la procura è "imparziale difensore della legalità" e ricerca prove a carico sia a discarico.
In tal modo la disparità di armi tra l'accusa e la difesa sarebbe equilibrata dall'imparzialità che deve mantenere l'accusa. Tale modello però non si concilia con modelli più vicini al sistema accusatorio (Italia, Regno Unito, Cipro, Irlanda, Malta).
La previsione che la difesa possa richiedere un OEI causa, tuttavia, un notevole svantaggio e, obbligando la difesa a "scoprire le carte", implica l'esposizione della strategia difensiva prima di quanto necessario.

Trattandosi di uno strumento con una portata orizzontale, l'OEI può essere emesso per qualunque tipo di atto di indagine ed è, pertanto, idoneo, anche alla raccolta di dati di traffico.

In merito, risulta di particolare interesse una pronuncia della CGUE[384] relativa all'emissione di un OEI da parte del pubblico ministero per l'acquisizione di dati di traffico.

Nello specifico, il Tribunale speciale per i procedimenti penali della Bulgaria interrogava la Corte sulla possibilità di attribuire al pubblico ministero il potere di emettere un OEI per ottenere dati di traffico relativi alle telecomunicazioni, allorquando in una procedura interna analoga tale competenza spetti al giudice. Domandava, inoltre, se l'eventuale riconoscimento da parte dello Stato di esecuzione possa "sanare" l'assenza dell'atto previsto dalla legge dello Stato di emissione.

Ebbene, secondo la Corte, in virtù di quanto previsto dall'art. 6, co. 1, lett. b), della D/OEI, l'autorità di emissione può emettere un ordine solo qualora l'atto richiesto possa essere adottato alle stesse condizioni in un caso interno analogo. «Ne consegue che il pubblico ministero, quando ai sensi del diritto nazionale è privo della competenza a disporre un atto di indagine per acquisire dati relativi al traffico e all'ubicazione connessi alle telecomunicazioni, non può essere considerato autorità di emissione, ai sensi dell'articolo 2, lettera c), punto i), della direttiva 2014/41»[385].

La Corte richiama, peraltro, l'orientamento già espresso nella causa *Prokuratuur,* secondo cui la normativa comunitaria osta a una disciplina nazionale che renda il pubblico ministero competente a disporre l'acquisizione di dati di traffico e ubicazione ai fini di un'istruttoria penale. Rispetto al secondo quesito, l'organo di giustizia ha ribadito che i

---

[384] CGUE, 16 dicembre 2021, C-724/19, *HP* con nota di DANIELE M., *Il controllo giurisdizionale sull'emissione dell'ordine europeo di indagine: la necessaria simmetria con la disciplina nazionale nei casi interni analoghi*, in *www.sistemapenale.it*, 31 marzo 2022. Nel caso di specie, nel corso di un procedimento penale per reati di terrorismo, il pubblico ministero bulgaro emetteva 4 OEI per acquisire dati di traffico connessi alle telecomunicazioni, inviandoli alle autorità di Belgio, Germania, Austria e Svezia. I dati acquisiti a mezzo OEI venivano, successivamente, posti alla base dell'atto di rinvio a giudizio. Tuttavia, il Tribunale bulgaro ha interrogato la Corte, dal momento che in una procedura interna analoga, il pubblico ministero non può disporre l'acquisizione di tali dati, che spetta invece ad un giudice, cui il pubblico ministero può rivolgere la richiesta. Inoltre, veniva chiesto alla Corte se il riconoscimento effettuato dallo Stato di esecuzione possa sostituire validamente l'atto che avrebbe dovuto essere adottato da parte della legge dello Stato di emissione, al fine di garantire i principi di legalità e inviolabilità della vita privata.

[385] CGUE, 16 dicembre 2021, C-724/19, *HP*, § 39. Al § 40 ss. si legge: «Nel caso di specie, dalla domanda di pronuncia pregiudiziale risulta che il pubblico ministero, benché costituisca, ai sensi del diritto bulgaro, l'autorità competente a emettere un ordine europeo di indagine nel procedimento penale, è privo della competenza a disporre l'acquisizione dei dati relativi al traffico e all'ubicazione connessi alle telecomunicazioni in un procedimento nazionale analogo. Infatti, l'organo giurisdizionale di rinvio rileva che, ai sensi del diritto bulgaro, l'autorità competente a disporre l'acquisizione di siffatti dati è costituita dal giudice dell'organo giurisdizionale di primo grado competente per la trattazione del procedimento in questione, e che il pubblico ministero può soltanto rivolgere a quest'ultimo giudice una richiesta motivata. Pertanto, in una situazione siffatta, non può sussistere la competenza del pubblico ministero all'emissione di un ordine europeo di indagine per l'acquisizione di simili dati».

motivi di non riconoscimento o non esecuzione hanno carattere tassativo e, pertanto, lo Stato di esecuzione non può prendere in considerazione condizioni ulteriori. Quest'ultimo, infatti, non può sostituirsi allo Stato di emissione e controllare il rispetto dei requisiti sostanziali sottesi all'emissione dell'ordine: una scelta di segno diverso segnerebbe il venir meno della fiducia reciproca. Al momento dell'emissione dell'ordine, l'autorità competente dovrà valutare l'esistenza dei requisiti di necessità, proporzionalità[386] e legalità[387] ed emettere o tradurre l'OEI nella lingua dello Stato di esecuzione o in una tra quelle da questo indicate[388]. Una volta ricevuto l'OEI, l'autorità di esecuzione lo riconosce e ne dispone l'esecuzione senza ulteriori formalità, alla stregua di un atto pronunciato da un'autorità interna[389], a meno che non si configuri taluno dei motivi di rifiuto indicati nella direttiva[390].

---

[386] GUERRERO PALOMARES S., *El principio de proporcionalidad en los principales instrumentos de cooperación judicial europeos: la OEDE y la OEI* in FONTESTAD PORTALÈS L., JIMÈNEZ LÓPEZ M. de las Nieves (a cura di), *A vueltas con la transformación digital de la cooperación jurídica penal internacional,* Aranzadi, 2022.

[387] È infatti necessario che la misura richiesta:

a) sia indispensabile per ottenere la prova di un fatto, che non potrebbe essere dimostrato con altre misure;
b) apporti un beneficio maggiore rispetto al sacrificio dei diritti fondamentali;
c) possa emettersi alle stesse condizioni in un caso interno analogo, onde evitare il fenomeno del c.d. forum shopping.

Qualora l'autorità di esecuzione ritenga che tali requisiti non sussistano, può avviare una consultazione con l'autorità di emissione, che potrebbe anche ritirare l'OEI qualora ritenga che sia la soluzione più adatta. V. GATTO C.E., *Il principio di proporzionalità nell'ordine europeo di indagine penale*, in *Dir. Pen. Cont.*, 12 febbraio 2019; SCOMPARIN L., CABIALE A., *The proportionality test in Directive 2014/3ì41/EU: present and future of a fundamental principle*, in *www.eurojus.it*, 2022,2.

[388] Ogni Stato membro deve, infatti, comunicare in quali altre lingue sarà consentita la trasmissione dell'OEI, ad esclusione di quella ufficiale. Art.5.2.

[389] Art. 9.1.

[390] Art.11.1.

Lo Stato di esecuzione può, dunque, rifiutare l'esecuzione di un OEI quando:

a) la legislazione nazionale preveda immunità o privilegi anche relativi alla libertà di stampa e di espressione che ostacolino l'esecuzione dell'OEI.
b) L'esecuzione dell'OEI possa pregiudicare interessi essenziali di sicurezza nazionale, causare un pericolo alla fonte delle informazioni o richiedere l'utilizzo di informazioni riguardanti attività di *intelligence.*
c) L'OEI sia stato emesso nel quadro di un procedimento avviato dalle autorità amministrative o giudiziarie, la cui decisione possa sfociare in un procedimento dinanzi ad un'autorità competente in materia penale, allorquando tale atto non sia ammesso secondo la legge dello Stato di esecuzione in un caso interno analogo.
d) L'esecuzione dell'OEI sia contraria al principio del *ne bis in idem.*
e) L'OEI si riferisca ad un reato commesso al di fuori del territorio dello Stato di emissione, in cui la condotta non costituisca reato, e interamente o parzialmente nel territorio dello Stato di esecuzione (*principio di territorialità*).
f) Vi siano seri motivi per credere che l'esecuzione dell'atto richiesto sia incompatibile con gli obblighi dello Stato di esecuzione relativi all'art. 6 TUE e alla Carta di Nizza.
g) La condotta oggetto dell'OEI non costituisca reato nello Stato di esecuzione (requisito della *doppia incriminazione*); a meno che la condotta sia configurabile tra i reati indicati nell'elenco di cui all'allegato D e sia punibile nello Stato di emissione con una pena o misura di sicurezza detentiva della durata massima di almeno tre anni.
h) Qualora l'atto richiesto sia limitato, secondo la legge dello Stato di esecuzione, ad un elenco di reati tra cui non è presente quello indicato nella richiesta.

Vedasi BACHMAIER WINTER L., *The proposal for a directive on the european investigacion order and the grounds for refusal: a critical assessment*, in RUGGERI S., (a cura di) *Transnational evidence and multicultural inquiries in Europe*, Springer, 2014, p.79.

Come per i precedenti strumenti, è previsto un elenco di reati per cui l'OEI andrà sempre riconosciuto ed eseguito[391], anche senza la verifica della doppia incriminazione, purché questi reati siano punibili nello Stato di emissione con una pena o misura di sicurezza detentiva della durata massima di almeno tre anni.
Inoltre, il requisito della doppia incriminazione non potrà essere opposto qualora l'atto richiesto riguardi:

- l'acquisizione di informazioni o prove già in possesso dell'autorità di esecuzione se, per il diritto dello Stato di esecuzione, queste avrebbero potuto essere acquisite nell'ambito di un procedimento penale o ai fini dell'OEI;
- l'acquisizione di informazioni contenute nelle banche dati della polizia o delle autorità giudiziarie;
- l'audizione di un testimone, un esperto, una vittima, una persona sottoposta ad indagini o di un imputato o di terzi nel territorio dello Stato di esecuzione;
- l'individuazione di persone titolari di un abbonamento a uno specifico numero telefonico o indirizzo IP.

Per favorire l'innesto dell'atto nell'ordinamento di destinazione, la direttiva prevede che l'autorità emittente possa indicare alcune formalità da rispettare nel compimento dell'atto; l'autorità di esecuzione dovrà rispettarle, salvo che siano in contrasto con i principi fondamentali del suo ordinamento (art. 9.2). Con la medesima finalità, l'autorità di emissione può anche richiedere che all'esecuzione dell'OEI partecipino dei suoi funzionari, nella stessa misura in cui potrebbero partecipare in un caso interno analogo[392].

[391] Tale elenco di reati coincide con quello riportato nella decisione quadro.
[392] Art. 9.4. Inoltre, *ex* art. 9.5 i funzionari presenti nello Stato di esecuzione dovranno attenersi alla *lex loci:* potranno svolgere attività di contrasto solo nel rispetto di questa e nel rispetto di eventuali accordi tra gli Stati

393

Sul versante dei tempi, la direttiva, nonostante preveda l'utilizzo della «stessa celerità e priorità usate in un caso interno analogo[394]», contempla dei termini *ad hoc* per il riconoscimento e l'esecuzione, anche se non perentori.

Nello specifico: 30 giorni per emettere la decisione sul riconoscimento o sull'esecuzione, a partire dalla ricezione[395]; 90 giorni per svolgere l'atto di esecuzione, a partire dalla decisione di cui sopra.

Laddove si riscontrino problemi che possano ostacolare l'esecuzione, è prescritto che si avvii un'interlocuzione tra le parti, rappresentando le ragioni di un possibile ritardo (art. 9.6). Per facilitare ulteriormente la collaborazione, l'autorità di emissione potrà indicare nell'OEI, in situazioni di urgenza, l'esigenza di un termine più breve o la necessità che l'atto sia eseguito in una data specifica (art. 9.2).

393 EUROJUST, *European Investigation Order- Infographic*, https://www.eurojust.europa.eu/sites/default/files/assets/2020-02-european-investigation-order.pdf.

394 Art. 12.1.

395 Il termine per la decisione sul riconoscimento o l'esecuzione sarà prorogabile per un massimo di 30 giorni; per ciò che concerne l'atto di esecuzione dell'indagine, invece, vi sarà la possibilità, secondo quanto concertato dalle autorità, di scegliere il momento più adatto.

L'autorità di esecuzione può rinviare l'esecuzione qualora questa possa causare un pregiudizio ad un'indagine o un procedimento penale in corso o quando gli oggetti, documenti o dati richiesti siano utilizzati in altro procedimento (art. 15.1).

Cessati tali ostacoli, procederà all'esecuzione dell'atto richiesto e lo trasmetterà, senza ritardo, all'autorità di emissione.

Gli Stati membri, al fine di rendere effettivo il diritto di difesa sancito all'art. 47[396] della CEDU, devono inoltre garantire all'imputato il ricorso a mezzi di impugnazione, conformemente a quanto disposto per un caso interno analogo.

Le ragioni di fondo della decisione possono essere impugnate solo nello Stato di emissione, mentre nello Stato di esecuzione possono essere censurati gli atti di acquisizione della prova in caso di lesioni dei diritti fondamentali. Affinché tale diritto al ricorso sia effettivo è necessario che l'imputato possa disporre, anche nello Stato di esecuzione, di un avvocato che difenda i suoi diritti, che sia messo al corrente dell'emissione dell'ordine in tempo utile, che sappia di quali elementi di prova dispone l'accusa, possa partecipare all'atto di indagine e verificare il rispetto delle formalità necessarie[397].

Il tema dei rimedi è stato oggetto di alcune interessanti pronunce della Corte di Giustizia: in particolare, nelle sentenze *Gavanozov* "I"[398] e "II" [399] si è riaffermata la necessità che gli

---

[396] «Ogni individuo i cui diritti e le cui libertà, garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo».

[397] BACHMAIER WINTER L., *Prueba transnacional en Europa: la Directiva 2014/41/UE*, cit.

[398] CGUE, 24 ottobre 2019, C-324/17, *Gavanozov*, con commento di WAHL T., *First CJEU judgement on European Investigation Order*, in *www.eucrim.eu*, 2020. Nel caso in esame, il Tribunale speciale per i procedimenti penali bulgaro (*Spetsializiran nakazatelen sad*) emetteva un OEI affinché le autorità ceche effettuassero perquisizioni e sequestri presso l'abitazione del rappresentante legale di una società utilizzata per commettere reati fiscali e ne organizzassero l'audizione mediante videoconferenza. Tuttavia, al momento dell'emissione dell'ordine, le autorità riscontravano talune difficoltà nella compilazione del modulo, nello specifico per la parte relativa ai mezzi di impugnazione previsti dall'ordinamento nazionale. Per tale ragione veniva chiesto alla CGUE di interpretare alcune disposizioni della direttiva valutando la compatibilità con il diritto nazionale bulgaro, che non predispone alcun mezzo di impugnazione per contestare le ragioni di merito poste alla base dell'emissione di un OEI che prevede perquisizioni, sequestri e audizioni tramite videoconferenza. Inoltre, veniva chiesto se l'art. 14 della direttiva configurasse per le persone interessate il diritto di impugnare la decisione relativa all'OEI, anche in assenza di un apposito rimedio processuale nell'ordinamento interno. La Corte, nel caso di specie, si è limitata ad analizzare la parte del modulo su cui le autorità bulgare hanno sollevato i dubbi, non valutando la questione nella sua interezza ed ha, pertanto, ritenuto che l'autorità di emissione, nel punto 1 della sezione J del modulo, dovesse semplicemente indicare se fossero già stati esperiti dei mezzi di impugnazione, ed eventualmente descriverli. In tal senso, specifica che non è richiesta all'autorità di emissione una disamina dei mezzi di ricorso esistenti. § 38: « Alla luce dell'insieme delle considerazioni che precedono, occorre rispondere alle questioni poste dichiarando che l'articolo 5, paragrafo 1, della direttiva 2014/41, in combinato disposto con la sezione J del modulo di cui all'allegato A a tale direttiva, deve essere interpretato nel senso che l'autorità giudiziaria di uno Stato membro non deve, al momento dell'emissione di un ordine europeo di indagine, far figurare in tale sezione una descrizione dei mezzi di impugnazione che sono previsti, se del caso, nel suo Stato membro avverso l'emissione di un siffatto ordine».

[399] CGUE, 11 novembre 2021, C-852/19, *Gavanozov* con nota di DE LUCA C., *La Corte di giustizia si pronuncia nuovamente sull'ordine europeo di indagine penale: la tutela dei diritti fondamentali prevale sull'efficienza investigativa*, in *www.sistemapenale.it,* 9 marzo 2022. A seguito del primo rinvio pregiudiziale effettuato dall'autorità bulgara, la Corte veniva nuovamente interrogata sull'interpretazione della D/OEI e sulla sua conformità con la Carta dei diritti fondamentali dell'Unione europea, per chiarire se una normativa nazionale che non prevede alcun mezzo di impugnazione contro l'emissione di un OEI finalizzato alla

Stati membri, nell'attuazione del diritto dell'Unione, assicurino il diritto a un ricorso effettivo, *ex* art. 47 della Carta di Nizza.

Nello specifico, con riguardo ad atti quali perquisizioni, sequestri e audizione di testimoni, incombe sugli Stati il dovere di prevedere appositi strumenti per contestarne la regolarità davanti allo Stato di emissione, legittimato a conoscere il provvedimento nel merito[400].

Sulla scorta di quanto detto, uno Stato che non garantisca il diritto ad un ricorso effettivo mette in atto una violazione dei diritti sanciti dalla Carta dei diritti dell'Unione europea, « con la conseguenza che il riconoscimento reciproco non può trovare applicazione e andare a beneficio di tale Stato membro»[401], generando una lesione al principio di fiducia reciproca e leale collaborazione, legittimando lo Stato di esecuzione a rifiutare lo svolgimento dell'atto qualora questo sia incompatibile con i diritti fondamentali.

4.2.4.1. Il caso Encrochat e la decriptazione: la valutazione delle prove acquisite all'estero

L'OEI è stato al centro di un'attività d'indagine che ha permesso di ottenere a più Stati le comunicazioni criptate dell'azienda *Encrochat*, acquisite e decriptate nell'ambito della *Task Force Emma 95.*

Il tema è di particolare rilievo, tanto da essere stato portato all'attenzione della Corte di giustizi. Gli sviluppi di tale vicenda sono, infatti, rilevanti anche in relazione a operazioni investigative legate ad altre aziende che forniscono servizi di comunicazione criptati quali SKY-ECC o Anom.

Encrochat è un *provider* di servizi di telecomunicazione con sede in Francia, i cui cellulari (*cryptophones*) sono provvisti di particolari caratteristiche, tra le quali l'assenza di una telecamera, di GPS e di ingressi USB.

Si avvale di un sistema modificato che, attraverso una specifica combinazione di *hardware* e *software,* permette agli utenti di scambiare messaggi e chiamate criptate. L'acquisto dei

perquisizione di un'abitazione e di locali commerciali, del sequestro e dell'audizione di un testimone, sia compatibile con il disposto della direttiva e con gli art. 7 e 47 della Carta di Nizza e se, a tali condizioni, possa essere emesso un OEI.

[400] *Ibidem*, § 50 « Alla luce delle suesposte considerazioni, si deve rispondere alla prima questione dichiarando che l'articolo 14 della direttiva 2014/41, letto in combinato disposto con l'articolo 24, paragrafo 7, della medesima direttiva e l'articolo 47 della Carta, deve essere interpretato nel senso che esso osta alla normativa di uno Stato membro di emissione di un ordine europeo di indagine la quale non preveda alcun mezzo d'impugnazione contro l'emissione di un ordine europeo di indagine avente ad oggetto lo svolgimento di perquisizioni e di sequestri nonché l'organizzazione di un'audizione di testimoni mediante videoconferenza.».

[401] *Ibidem*, § 56.

dispositivi è legato ad una specifica piattaforma *online* e include la sottoscrizione dell'abbonamento, per un costo di circa 1.000 – 1.600 euro[402].

Nel 2017 la *Gerdarmerie* francese e le autorità giudiziarie hanno svolto un'indagine relativa a questi dispositivi, riscontrando una frequente connessione con gruppi riconducibili alla criminalità organizzata[403].

Nel dicembre 2018 e ottobre 2019, su autorizzazione di un giudice nazionale, veniva effettuata la copia dei dati connessi al dominio da un *server* localizzato nella città francese di *Roubaix*.

Una parziale decriptazione delle informazioni ottenute ha palesato una stretta connessione con attività illegali, specialmente relative al traffico di droga.

Nel 2020, veniva così ottenuta l'autorizzazione giudiziaria per installare da remoto un *tool* finalizzato ad intercettare i dispositivi connessi al *server*.

L'installazione di tale strumento è stata classificata come segreto di difesa nazionale ed è stata seguita dalla creazione di una squadra investigativa comune con le autorità olandesi, supportata da Eurojust[404] ed Europol (*Task force Emma 95*).

---

[402] EUROPEAN PARLAMENTARY RESEARCH SERVICE, *EncroChat's path to Europe's highest courts*, dicembre 2022, https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739268/EPRS_ATA(2022)739268_EN.pdf .

[403] Per i dettagli sull'operazione vedasi EUROJUST, *The Encrochat investigation in France*, 2 luglio 2020, https://www.eurojust.europa.eu/fr/document/encrochat-investigation-france.

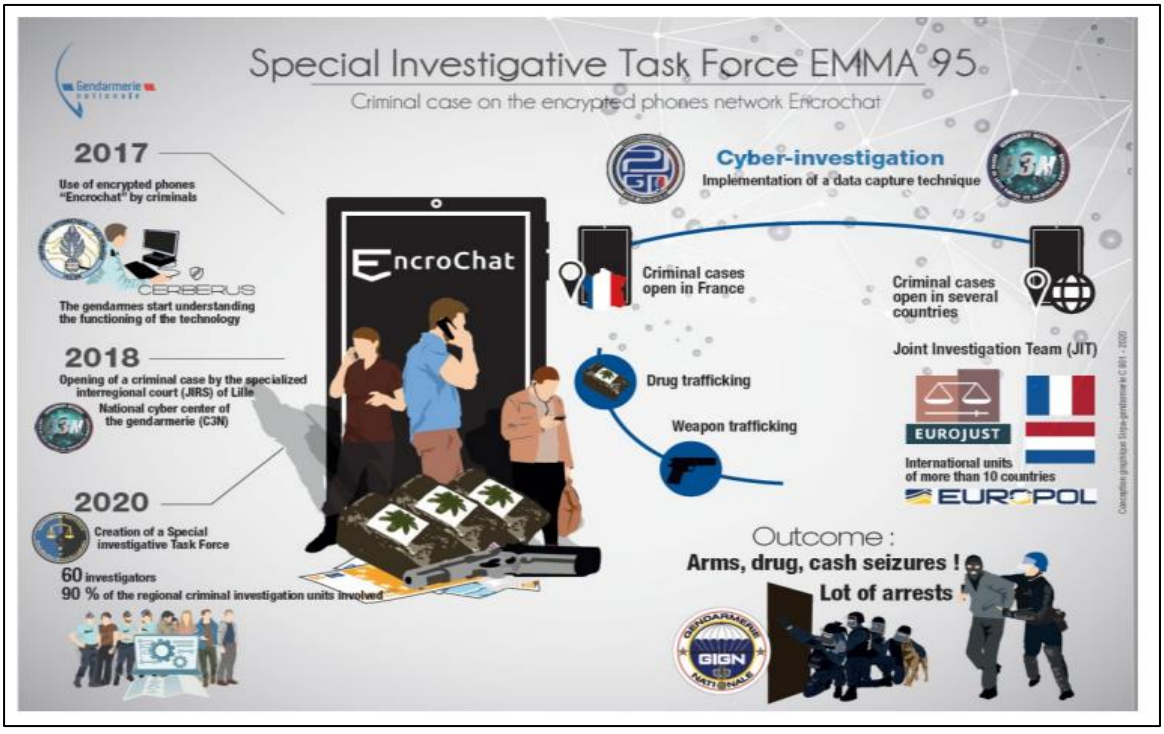
[404] EUROJUST svolge un lavoro di coordinamento e di *soft law* attraverso la pubblicazione di pareri, linee guida e manuali in cui si danno suggerimenti concreti per superare situazioni basate su squadra investigative comuni e cooperazione transnazionale. È stato istituito con decisione 2002/187/GAI del febbraio 2002, in G.U. L 63 del 6 marzo 2002. Si tratta di un organismo sovranazionale dotato di personalità giuridica e finanziato dal bilancio dell'Unione, che ha preso il posto dell'unità provvisoria di cooperazione giudiziaria, denominata *pro Eurojust*. Tra gli obiettivi di Eurojust:

- stimolare e migliorare il coordinamento delle indagini e delle azioni penali tra le competenti autorità nazionali degli Stati membri, sulla base di qualsiasi richiesta da essere formulata o qualsiasi elemento informativo proveniente da un organo comunitario;
- migliorare gli aspetti della cooperazione giudiziaria con particolare riferimento all'agevolazione delle domande di assistenza giudiziaria e delle richieste tradizionali;

prestare in altro modo assistenza alle autorità competenti degli Stati membri per migliorare l'efficacia delle loro indagini e azioni penali.

L'ultima formulazione, volutamente ampia e generica, è idonea a ricomprendere non solo forme di supporto logistico e di consulenza con riguardo al diritto comparato processuale e sostanziale degli Stati membri, ma anche e soprattutto forme di coinvolgimento in attività di tipo operativo come la raccolta delle prove, la partecipazione ad atti concordati nell'ambito di una squadra investigativa comune, la trasmissione di rogatorie o ordinanze a carattere preliminare, quali mandati di arresto europeo o decisioni di blocco dei conti bancari. Il coordinamento delle competenti autorità nazionali non implica poteri autoritativi nei confronti delle medesime, ma ha costituito la vera novità di Eurojust, poiché ha consentito di realizzare un progressivo avvicinamento alle finalità di tendenziale verticalizzazione delle attività investigative ed un sensibile allontanamento dal modello orizzontale di cooperazione giudiziaria fondato su intese e accordi.
Per approfondimenti KOSTORIS E.R., *Manuale di procedura penale europea*, cit., p.249 ss.

405



406

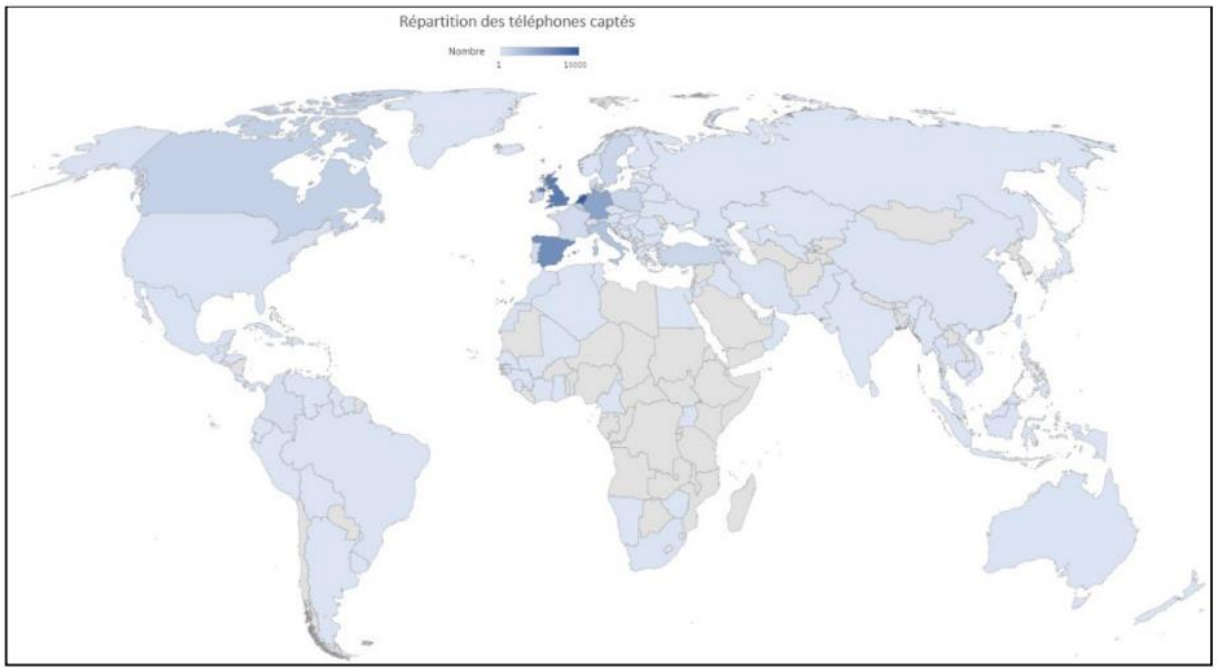
L'installazione dello *spyware* ha permesso di acquisire:

- codici IMEI,
- nomi degli utenti,

405 EUROJUST, *The dismantling of an encrypted phone solution used by organized crime groups, 2* luglio 2020, https://www.eurojust.europa.eu/sites/default/files/assets/2020-07-02-encrochat-case-final.pdf .
406 EUROJUST, *The Encrochat investigation in France,* cit., p. 6.

- *password*,
- *chat* salvate,
- dati di geolocalizzazione,
- note dei dispositivi.

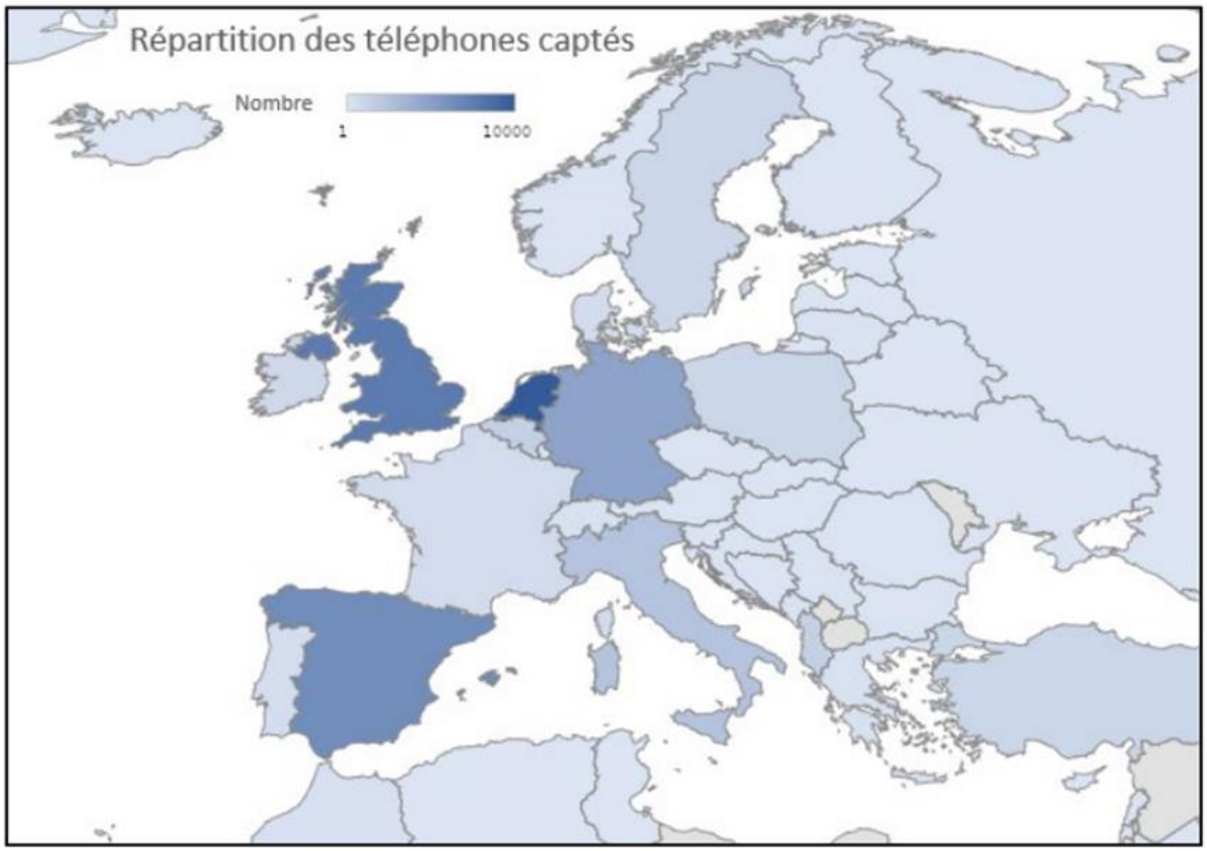
Le indagini hanno portato all'acquisizione di circa 120 milioni di messaggi, inviati da 60.000 dispositivi e gli esiti sono stati, successivamente, condivisi con le autorità di altri Stati membri interessati ai dati. Proprio questi ultimi, mediante OEI indirizzati alle autorità francesi, hanno infatti acquisito la messaggistica per utilizzarla nei procedimenti interni[407].



[408] *Ripartizione dei dispositivi captati su scala mondiale*

[407] Ciò ha portato all'arresto di 7700 soggetti e all'avvio di 3800 procedimenti giudiziari. J.J., VAN TOOR D.A.G., *Legal Aspects of the EncroChat Operation: A Human Rights Perspective, in European Journal of crime, criminal law and criminal justice*, 27 dicembre 2022: «*As a result of the operation, new investigations were initiated, thousands of people were arrested and large amounts of drugs were confiscated. For example, in the Netherlands, more than 100 persons were arrested as a result of the EncroChat operations and analysis of the data. In April 2021, there were 200 ongoing criminal investigations arising from EncroChat. In Sweden, more than 200 suspects were identified in 2021. In the United Kingdom, the National Crime Agency reported that 2.631 people had been arrested in the United Kingdom following the analysis of EncroChat messages and 1.384 had been charged*».

[408] EUROJUST, *The Encrochat investigation in France*, cit., p. 7.



[409] *Ripartizione dei dispositivi captati su scala europea*

Questa operazione ha posto all'attenzione delle autorità giudiziarie di diversi Paesi alcune rilevanti questioni sull'utilizzabilità del materiale probatorio così acquisito. In particolare, tra le obiezioni mosse dalle difese vi era quella fondata sull'assenza di un limite temporale alle misure intercettive, nonché sulla captazione generale e indiscriminata e sul rifiuto della gendarmeria francese di specificare i dettagli tecnici dell'operazione.

In Spagna, la *Audiencia Nacional* in relazione a un caso di estradizione, in cui le prove dell'accusa erano collegate alle indagini di *EncroChat*, ha escluso profili di violazione dei diritti fondamentali[410].

In altro procedimento[411], la difesa chiedeva di emettere una rogatoria al tribunale di *Lille* per ottenere la documentazione sulle operazioni effettuate dalla polizia e dal pubblico

[409] *Ibidem*.
[410] *Audiencia Nacional, sala de lo penal, auto del pleno*, 20 settembre 2022, n. 77: «*Debemos coincidir con la decisión adoptada por la sala a quo, en que lo trascendente no es la modificación observada por el recurrente, sino que no se aprecia "riesgo real" que determine cualquier comprobación sobre la protección de los derechos fundamentales del reclamado, ni precise de cualquier decisión distinta de la adoptada en la instancia. No existe ni el más mínimo indicio de que las pruebas de la acusación que existan contra él se hubieren obtenido mediante una infiltración indiscriminada de conversaciones mantenidas a través de la red EncroChat pero, aunque así hubiera sido, ello es irrelevante a los fines del procedimiento de extradición en el que nos encontramos*». V. anche CHABANEIX L., *EncroChat: aproximación al estado de la cuestión en perspectiva comparada*, in *www.elderecho.com*, 21 dicembre 2022.
[411] *Audiencia Nacional, Sala de lo Penal*, Sez. IV, *auto*, 19 luglio 2022, n. 439.

ministero relativamente alle conversazioni di *EncroChat*. A fronte del rifiuto, la parte proponeva appello ritenendo che l'acquisizione fosse utile per valutare le condizioni in cui erano stati ottenuti i dati e la compatibilità con il diritto dell'Unione e i diritti fondamentali.

La *Audiencia Nacional,* tuttavia, confermava la decisione del *Magistrado Instructor*, ritenendo che la misura di acquisizione documentale fosse carente sul profilo della pertinenza, dell'inutilità e della necessità[412].

In altro caso, peraltro, lo stesso Organo escludeva la *facultad de supervisiòn*, ritenendo che il coinvolgimento di Eurojust nelle operazioni effettuate dalle autorità francesi fosse indice, *a fortiori*, della legittimità delle operazioni e della conformità al diritto europeo e ai diritti fondamentali[413].

Diverso l'approccio in Francia, dove la Corte di Cassazione francese[414] chiedeva al *Conseil constitutionell* di valutare la legittimità delle norme del codice di procedura penale

---

[412] Per approfondimenti MONTES P., *La Audiencia Nacional admite diligencias que podrían comprometer decenas de causas relacionadas con Encrochat en España*, in *Economist & Jourist*, 23 ottore 2023, https://www.economistjurist.es/tal-dia-como-hoy/nace-ricardo-salvador-huesca-boadilla-abogado-del-estado-que-ejerce-ante-el-tribunal-supremo/; OERLEMANS J.J., VAN TOOR D.A.G., *Legal aspects of the EncroChat operation: a human rights perspective*, in *European Journal of crime, criminal law and criminal justice*, 27 dicembre 2022.

[413] *Audiencia Nacional. Juzgados Centrales de Instrucción*, auto, 1 dicembre 2021, n. 38: « *A su vez, debemos reiterar que la intervención de Encrochat fue acordada por un órgano judicial, en el marco de una investigación judicial abierta, por una serie de delitos, varios de ellos atribuidos a dicho sistema de comunicación. Por si ello fuera insuficiente, hemos de tomar en consideración que la investigación francesa estuvo participada por Eurojust, puesto que en su página web figuraba la información referente a este caso. De ahí que, al contar con la cobertura de Eurojust, ello constituya un indicio de la licitud de las diligencias practicadas. Así y todo, no podemos obviar que lo que ha de tenerse presente es la ley francesa, puesto que la medida limitativa de derechos ha de tamizarse a la luz del ordenamiento galo, y no ha lugar a efectuar una lectura desde los parámetros internos del Derecho español. Tomamos como punto inicial que existía una habilitación legal para adoptar la medida de injerencia en el derecho fundamental a la intimidad de los afectados, y que esta diligencia se acordó por un juez de garantías, lo que suministra la máxima cobertura posible, en orden a la ponderación de todos los intereses en presencia y, en esencia, a la salvaguarda de los derechos fundamentales, salvo en aquellos casos en los que se repute que existe un interés superior, como es el presente supuesto*».

[414] *Cour de Cassation, Chambre criminelle*, 1 febbraio 2022, 173, rinvio al *Conseil Constitutionell,* :«*En édictant les dispositions des articles 706-102-1 et 230-1 et suivants du code de procédure pénale - lesquelles permettent au procureur de la République ou au juge d'instruction de procéder à la mise en place d'un dispositif technique ayant pour objet la captation de données informatiques, par le recours aux moyens de l'Etat soumis au secret de la défense nationale - le législateur a-t-il, d'une part, méconnu sa propre compétence en affectant des droits et libertés que la Constitution garantit, en l'occurrence, les droits de la défense, les principes de l'égalité des armes et du contradictoire ainsi que le droit à un recours effectif, en ce qu'il s'est totalement abstenu de prévoir des garanties légales suffisantes et adéquates concernant le recours à ces moyens, ne fixant aucun critère pour y recourir, et ne prévoyant aucun contrôle a priori ou a posteriori pour encadrer cette décision, laquelle apparaît ainsi purement discrétionnaire, au surplus, sans contrôle préalable par une juridiction indépendante lorsque la mesure est édictée par le seul procureur et, d'autre part, porté une atteinte injustifiée et disproportionnée à l'ensemble de ces mêmes droits et libertés que la Constitution garantit ? […] La question posée présente un caractère sérieux. En effet, le choix fait par le procureur de la République ou le juge d'instruction, qui n'est pas encadré par des critères spécifiques, de prescrire le recours aux moyens de la défense nationale, lesquels peuvent être utilisés pour l'ensemble de l'opération et pas seulement pour le décryptage des données captées, peut avoir pour conséquence que, par l'effet des règles concernant le secret-défense, de nombreuses informations utiles au contrôle de la régularité de l'opération ne puissent être soumises au débat contradictoire, ce qui est susceptible de constituer une atteinte excessive aux droits et libertés invoqués*».

che permettono al Procuratore della Repubblica o al Giudice di istruzione di installare un dispositivo tecnico finalizzato alla captazione di dati informatici e di secretare le informazioni sull'operazione opponendo il segreto di Stato.

La Corte costituzionale francese[415], nella sua decisione, ha specificato che, per la validità delle procedure, devono rispettarsi precise formalità, pena la nullità del procedimento stesso. Ha, d'altro canto, considerato legittimo il ricorso al segreto di Stato da parte delle autorità per occultare tecniche investigative, necessarie a garantire l'efficace repressione del crimine.

Sulla scorta del bilanciamento della persecuzione dei reati con la tutela dei diritti fondamentali, ha ritenuto che, pur essendo legittimo mantenere il segreto sulle tecniche utilizzate, tuttavia, la difesa doveva essere messa in condizione di esaminare l'ordinanza scritta e motivata del giudice che aveva autorizzato l'installazione del dispositivo di captazione, con l'indicazione, a pena di nullità, del reato per cui si procede e che giustifica la misura, della localizzazione esatta o della descrizione dettagliata dei metodi di trattamento automatizzato dei dati e la durata dell'operazione.

Occorreva, inoltre, esibire i verbali di installazione del dispositivo, con la data e l'ora di inizio dell'operazione e l'indicazione del soggetto che descriveva o trascriveva i dati utili.

A seguito di tale pronuncia, la stessa Corte di Cassazione francese[416], in data 11 ottobre 2022, riteneva che il mancato rispetto delle menzionate formalità avesse viziato la validità e legalità del procedimento, impedendo la verifica sull'affidabilità dei dati registrati.

---

[415] *Conseil Constitutionell*, decisione 8 aprile 2022, n. 987, p. 19: «*Le Conseil a ensuite examiné l'étendue des informations qui pouvaient être soustraites au débat contradictoire. Sur ce point, il a relevé que « si les dispositions contestées sont susceptibles de soustraire au contradictoire certaines informations techniques soumises au secret de la défense nationale, demeure obligatoirement versée au dossier de la procédure l'ordonnance écrite et motivée du juge qui autorise la mise en œuvre d'un dispositif de captation et mentionne, à peine de nullité, l'infraction qui motive le recours à ce dispositif, la localisation exacte ou la description détaillée des systèmes de traitement automatisé de données concernés, ainsi que la durée pendant laquelle cette opération est autorisée ». Il a ajouté que « Sont également versés au dossier le procès-verbal de mise en place du dispositif, qui mentionne notamment la date et l'heure auxquelles l'opération a commencé et s'est terminée, et celui décrivant ou transcrivant les données enregistrées jugées utiles à la manifestation de la vérité » et que « l'ensemble des éléments obtenus à l'issue des opérations de mise au clair font l'objet d'un procès-verbal de réception versé au dossier de la procédure et sont accompagnés d'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis* ».

[416] *Cour de Cassation, criminelle, Chambre criminelle*, 11 ottobre 2022 n.1226; *Cour de Cassation, criminelle, Chambre criminelle*, 25 ottobre 2022 n. 1216.

Il Tribunale Regionale di Berlino[417], accogliendo il ricorso della Procura, annullava la decisione, ritenendo preminente il principio del reciproco riconoscimento. Nello stesso senso, il Tribunale Federale di Giustizia (*Bundesgerichtshof*)[418].

Il principio è stato valorizzato anche dalla giurisprudenza portoghese, che ha considerato ammissibili le prove acquisite dalla SIC[419].

Come anticipato, in questo quadro di incertezza, si inserisce il Tribunale di Berlino che, in data 24 ottobre 2022, ha proposto una questione pregiudiziale alla Corte di Giustizia, avente ad oggetto l'utilizzo dei dati ottenuti nell'operazione *Encrochat* [420]e la sua compatibilità con la D/OEI e il diritto ad un equo processo[421].

Il Tribunale ha sottoposto ben 14 questioni. In questa sede, tuttavia, rilevano le seguenti:

- se un OEI volto ad acquisire prove già in possesso dello Stato di esecuzione debba essere emesso da un giudice e se, in un caso interno analogo, la raccolta delle prove di tale tipo sia di competenza del giudice.
- Se un OEI vada sempre emesso da un giudice (o organismo indipendente non coinvolto nelle indagini), senza tener conto delle norme nazionali in tema di competenza dello Stato di emissione, qualora riguardi gravi ingerenze nei diritti fondamentali.
- Se la direttiva osti ad un OEI volto al trasferimento di dati già disponibili nello Stato di esecuzione, concernenti dati di traffico e ubicazione, registrazione dei contenuti delle comunicazioni, quando l'intercettazione «riguardi

---

[417] *BUNDESGERICHTSHOF*, 2 marzo 2022, 5 StR 457/21, con commento di WAHL T., *Germany: Federal Court of Justice confirms use of evidence in Encrochat cases,* in *www.eucrim.eu*, 19 maggio 2022: « *Legal experts voiced concerns over the legality of the operation from a German point of view. They mainly criticised that the secret interception under French law which affected a mass of people without concrete criminal suspicion at that date would not have been possible under German law and severely infringed German fundamental rights of privacy. They also doubted the legality of the way the data were transferred to Germany. This included, among others, the fact that mass data were first exchanged via police channels and the subsequent European Investigation Order served only to rather rubber-stamp these operations without judicial oversight in Germany*».

[418] V. WAHL T., *Dismantled encryption networks: German Courts confirmed use of evidence from Encrochat surveillance*, in *www.eucrim.eu,* 20 marzo 2022.

[419] *TRIBUNAL DA RELAÇÃO DE LISBOA*, 29 settembre 2021, 158/19.5JELSB.A. L1-3, § 18: «*Acresce que, nos termos do artº 125.º do C.P. Penal, são admissíveis as provas que não forem proibidas por lei. Não existindo, no que se refere à transmissibilidade de elementos probatórios já adquiridos, ao abrigo da Lei do Cibercrime, em país estrangeiro, qualquer norma que a proíba, teremos de concluir, como alega o recorrente que sendo a prova originalmente válida, a admissibilidade da transmissão verificar-se-á, sem qualquer limitação, sempre que não exista qualquer restrição de âmbito objectivo (catálogo de crimes) ou subjectivo quanto ao concreto meio de obtenção de prova, por razões de economia processual e em obediência a um primado de justiça e procura da verdade material*».

[420] Domanda di pronuncia pregiudiziale proposta dal *Landgericht Berlin* (Germania) il 24 ottobre 2022, C-670/22.

[421] Vedasi WAHL T., *Encrochat turns into a case for the CJEU*, in *www.eucrim.eu*, 18 novembre 2022.

tutti gli utenti di un determinato indirizzo di comunicazione, in secondo luogo, venga richiesto, tramite l'OEI, il trasferimento dei dati relativi a tutti gli indirizzi utilizzati sul territorio dello Stato di emissione e, in terzo luogo, non vi fossero indizi concreti della commissione di gravi reati da parte di detti singoli utenti al momento in cui è stata disposta e eseguita la misura di intercettazione né al momento dell'emissione dell'OEI»[422].

- se la direttiva «osti a tale OEI qualora l'integrità dei dati ottenuti grazie alla misura di intercettazione non possa essere verificata dalle autorità dello Stato di esecuzione a causa dell'assoluta riservatezza dei dati»[423].

Il 26 ottobre, l'Avvocato Generale Tamara Capeta ha presentato le sue conclusioni[424], nelle quali ha sostenuto che «la direttiva OEI non obbliga, bensì addirittura impedisce all'autorità di emissione di valutare la legittimità degli atti sulla base dei quali sono state raccolte le prove nello Stato membro di esecuzione».

Nel mese di aprile 2024 si è, invece, pronunciata la Grand Chamber[425], che ha sancito che:

- un OEI volto ad ottenere prove già in possesso della autorità competenti dello Stato di esecuzione non deve essere emesso necessariamente da un giudice, quando, in un caso interno analogo, sia competente il pubblico ministero;
- il giudice deve espungere dal processo elementi probatori, qualora l'imputato non possa contestare la correttezza di tali informazioni e queste influiscano in maniera preponderante sulla valutazione dei fatti,

Sullo stesso tema è da segnalare, per completezza, che a oggi si trova investita anche la Corte EDU, alla quale sono stati presentati due ricorsi[426] da parte di detenuti britannici,

---

[422] Domanda di pronuncia pregiudiziale proposta dal *Landgericht Berlin, cit.*
[423] *Ibidem.*
[424] Conclusioni dell'Avvocato Generale Tamara Carpeta, 26 ottobre 2023, Causa C-670/2022, *Staatsanwaltschaft Berlin* contro M.N. §48.L'Avvocato Generale ritiene, inoltre, che – specie nel caso di prove costituite – non possa essere rimessa in discussione la legittimità delle misure con cui sono state raccolte le prove e che, pertanto, nella presente causa, non può essere oggetto di discussione la proporzionalità delle operazioni svolte dalle autorità francesi.
Rispetto alle menzionate questioni pregiudiziali, l'Avvocato ritiene che anche laddove il diritto interno dello Stato di emissione preveda l'autorizzazione del giudice per la raccolta di tali prove, non è comunque necessario che sia questi ad emettere l'OEI, essendo sufficiente la semplice autorizzazione dell'atto iniziale.
Inoltre, sostiene che la valutazione sulla necessità e proporzionalità di un OEI sia di competenza dell'autorità di emissione, con la possibilità di un controllo da parte del giudice nazionale competente. L'ingerenza della misura va, peraltro, controbilanciata da un importante interesse pubblico connesso all'indagine.
[425] CGUE, 30 aprile 2024, C-670/2022.
[426] Ricorsi n. 44715/20, A.L. c. Francia e 47930/21, E.J. c. Francia, https://hudoc.echr.coe.int/eng?i=001-214862.

sottoposti a processo nel Regno Unito sulla scorta dei dati inviati dalle autorità francesi; nella specie, i ricorrenti contestano la legalità, necessità e proporzionalità, ritenendo sussistenti le violazioni degli artt. 6 e 13 CEDU.

Nell'attesa di ulteriori pronunce, non è da escludere che possano essere sollevate nuove questioni in considerazione dell'incremento delle piattaforme di cui si avvalgono i criminali. Tra queste, rileva ANOM[427] , la quale differisce per il fatto che la polizia non ha dovuto introdursi nel sistema, ma ha direttamente operato per la sua creazione, e EXCLU[428].

Pertanto, spetterà alle Corti di Strasburgo e Lussemburgo tracciare il punto di equilibrio tra il reciproco riconoscimento e la primazia del diritto comunitario e, d'altro lato, i diritti fondamentali e la sovranità nazionale.

4.2.5. Il pacchetto sulla prova digitale: alla ricerca di un compromesso

Pur riconoscendo la portata innovativa dell'ordine europeo di indagine, tale strumento, come evidenziato, non riesce a soddisfare compiutamente le esigenze connesse alla lotta contro il *cybercrime,* specie nel caso di dati conservati nel *cloud* o allocati in *server* stranieri[429].

I principali nodi riguardano l'identificazione dello Stato al quale trasmettere l'ordine e le tempistiche della procedura.

Sul primo versante, l'identificazione dello Stato di esecuzione non è agevole allorquando i dati non siano conservati in un dispositivo fisico ben preciso, ma si trovino archiviati con la tecnologia del *cloud computing*.

Sul versante dei tempi, invece, il termine per dare esecuzione all'OEI è fissato in 90 giorni: un lasso eccessivo qualora gli elementi da acquisire siano digitali e, dunque, facilmente soggetti ad alterazione e cancellazione.

---

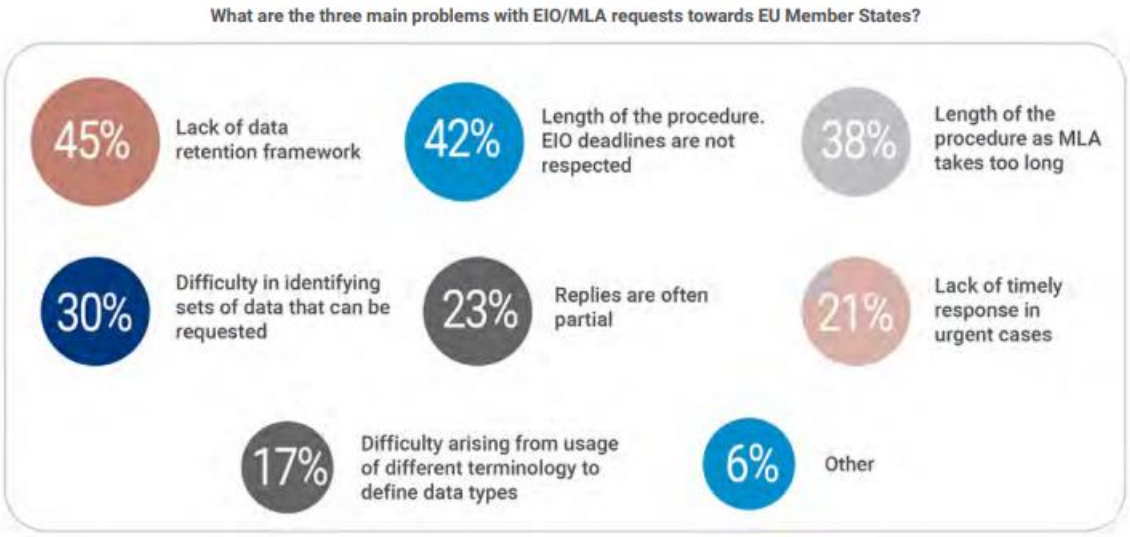
[427] Sull'operazione *OTF Greenlight /Trojan Shield* condotta da FBI, Polizia olandese e svedese, DEA ed autorità di circa 15 Paesi , con il supporto di Europol: https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication; https://www.ilriformista.it/che-cose-anom-lapp-utilizzata-dallfbi-nelloperazione-ironside-per-infiltrare-la-criminalita-organizzata-225036/?refresh_ce . WAHL T., RIEHLE C., *Trojan – Encrypted device reveals criminal activities*, in *www.eucrim.eu*, 10 luglio 2021.

[428] https://www.eurojust.europa.eu/news/new-strike-against-encrypted-criminal-communications-dismantling-exclu-tool .

[429] 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*, in *New Journal of European Criminal Law,* 2020, 11.

Una conferma si può ricavare dal Report SIRIUS 2022[430], secondo il quale i principali problemi connessi all'utilizzo dell'OEI e alle procedure di MLA sono i seguenti:

- mancanza di un quadro comune sulla *data retention*, anche in relazione ai termini di conservazione;
- lentezza delle procedure di MLA e dell'OEI e mancato rispetto dei termini prescritti;
- difficoltà di identificare le categorie di dati che possono essere richieste;
- risposte incomplete alle richieste;
- mancanza di risposte tempestive in casi di urgenza;
- difficoltà causate da differenti definizioni per le categorie di dati.

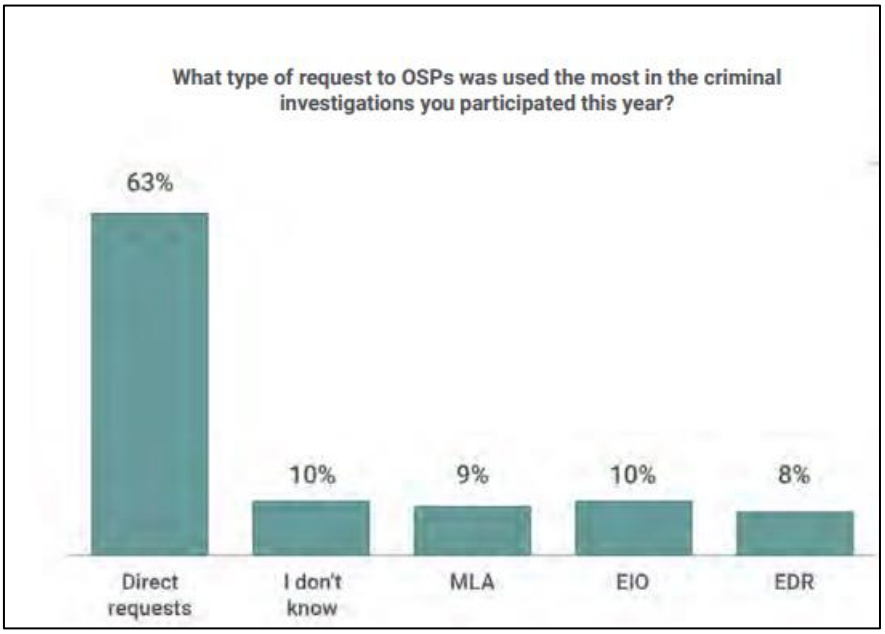


[431]

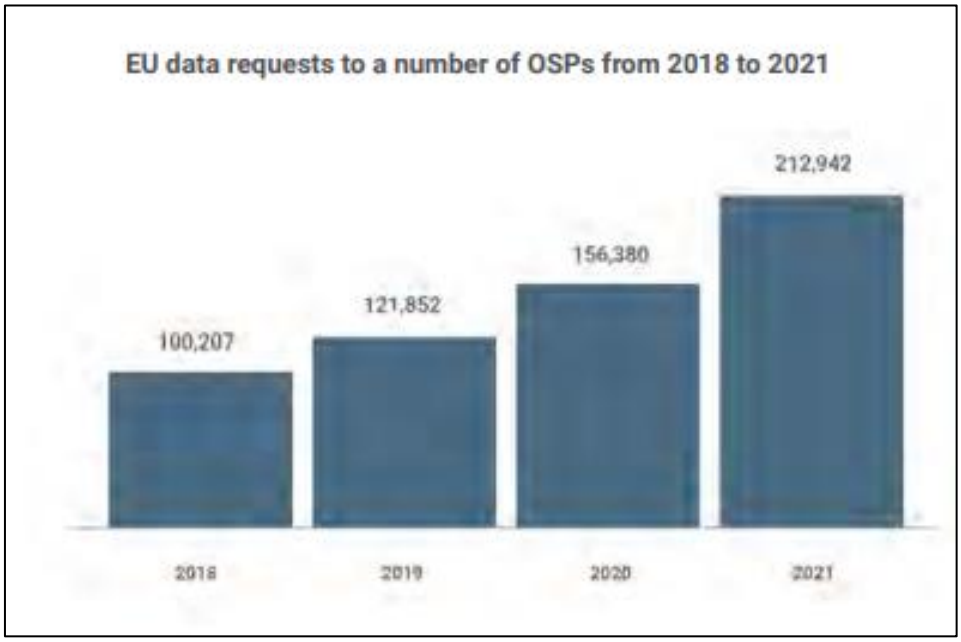
Per ovviare a questi ostacoli alcuni Stati ricorrono a degli *escamotage*, inviando le richieste di collaborazione volontaria direttamente ai *provider*. Così, nell'anno 2022, si registrano richieste di collaborazione diretta nella misura del 63%, seguite dal 10% di OEI e dal 9% di richieste di assistenza giudiziaria con procedure di MLA.

[430] SIRIUS EU *Digital Evidence Situation Report 2022 – 4th Annual Report*, https://www.eurojust.europa.eu/publication/sirius-eu-digital-evidence-situation-report-2022.
[431] *SIRIUS EU Digital Evidence Situation Report 2022 – 4th Annual Report,* https://www.eurojust.europa.eu/publication/sirius-eu-digital-evidence-situation-report-2022, p. 50

Allo stesso modo, va, inoltre, sottolineato l'ampio numero di richieste effettuate agli *online service provide*r da parte delle autorità, con un *trend* in costante aumento.

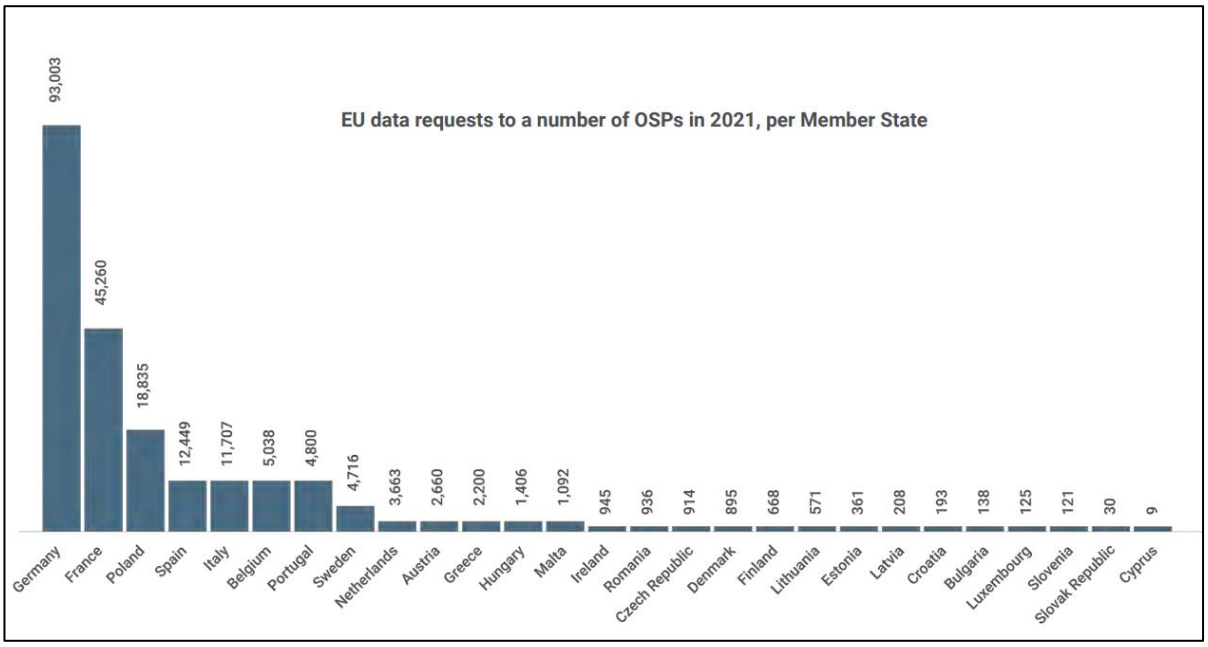


[432] *Percentuale dei tipi di richieste utilizzate dalle autorità di polizia in UE*



[433] *Richieste di dati agli online service provider da parte dei Paesi UE dal 2018 al 2021*

[432] *Ibidem*, p. 16.
[433] *Ibidem*, p. 60.



[434] *Percentuale dei tipi di richieste utilizzate dalle autorità di polizia in UE*

A fronte di questo quadro, soprattutto dopo gli attentati terroristici di Bruxelles del 2016[435], l'UE ha avvertito la necessità di predisporre un nuovo strumento di cooperazione, specificatamente dedicato alle prove digitali. La Commissione ha così presentato il c.d. "pacchetto *E-evidence*"[436] costituito dalla proposta di regolamento sull'ordine di produzione e conservazione delle prove elettroniche in materia penale[437] e dalla proposta di direttiva

[434] *Ibidem*, p. 16.

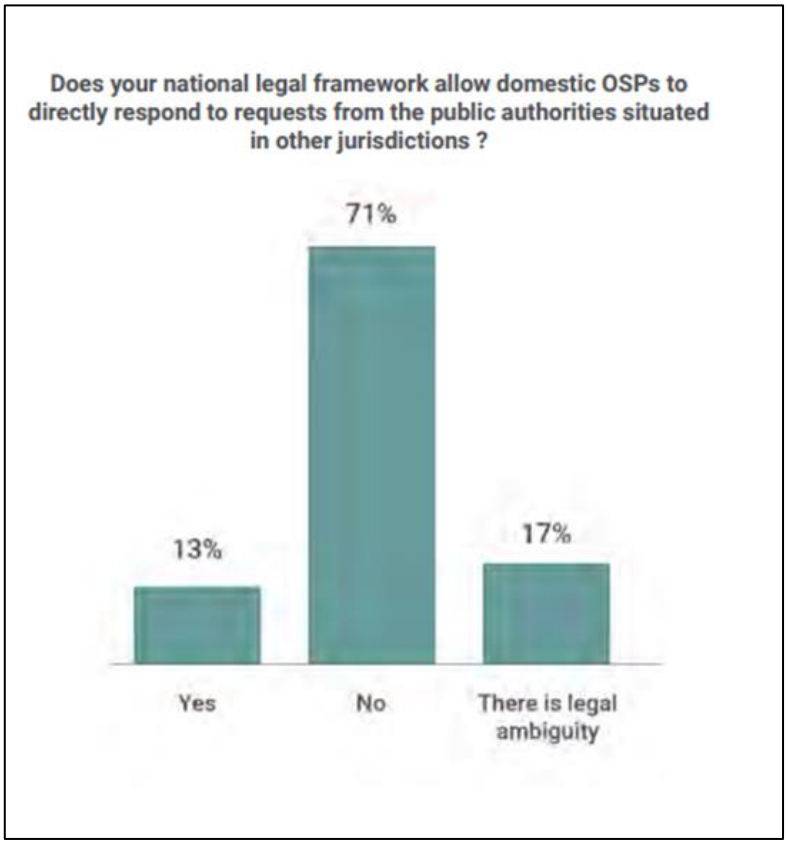
[435] Consiglio dell'Unione europea, *Council conclusions on improving criminal justice in cyberspace*, Lussemburgo, 9 giugno 2016, https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf : « *The Commission is requested, to develop a common framework for cooperation with service providers for the purpose of obtaining specific categories of data, in particular subscriber data, when allowed by third countries legislation, or any other comparable solution that allows for a quick lawful disclosure of such data8 . The Commission is requested to do so in association with Member States and relevant third countries and in cooperation with the private sector*».

[436] Vedasi GIALUZ M., DELLA TORRE J., *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. Pen. Cont.*, 31 maggio 2018; MAGNO T., *Il progetto* Evidence *e le principali criticità nell'accesso alle prove elettroniche transnazionali in materia penale: quale futuro?,* in *Informatica e diritto*, 2016, XXV, 2. Ed anche GONZÁLEZ CANO, I., *Nuevos paradigmas de la cooperación judicial penal en la Union Europea*, in BARONA VILAR S. (a cura di), *Justicia civil y penal en la era global,* Tirant Lo Blanch, 2017.

[437] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, 17 aprile 2018, COM (2018) 225 finale. Vedasi Parere del Comitato economico e sociale europeo sulla "Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale" e sulla "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", 10 ottobre 2018, 2018/C 367/17, in G.U. 367 del 10 ottobre 2018. Vedasi BUONO L., *The genesis of the European Union's new proposed legal instrument(s) on e-evidence. Towards the EU Production and Preservation Orders*, in *ERA Forum*, 2019, 19; COMBO E., *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, in *Cass. Pen.*, 2018; COLOMBO E., *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, *in Cass. Pen.*, 2019, 7; FUENTES SORIANO O., *The (future) European Electronic Evidence Delivery Order, in Journal of Applied Business &*

recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali[438].

Sul piano normativo, la scelta di adottare il regolamento in luogo della direttiva risponde alla necessità di evitare una ulteriore frammentazione e garantire un'applicazione omogenea.



[439] *Percentuali relative alla possibilità per i provider di rispondere legittimamente alle richieste di autorità di altri Paes*i

Economics, 2020, vol. 22, 8; GERACI R. M., *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento E-evidence*, in *Cass. Pen.*, 2019.

[438] 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, 17 aprile 2018, COM (2018) 226 finale. Vedasi TOSZA S., *The European Commission's Proposal on Cross-Border Access to E-Evidence*, in *www.eucrim.eu,* 2018,4.

[439] *Ibidem*, p. 36.

All'esito di un lungo e complesso negoziato[440], in data 12 luglio 2023, sono stati approvati la Direttiva 2023/1544/UE[441] e il Regolamento 1543/2023/UE[442].

[440] https://www.europarl.europa.eu/RegData/commissions/libe/lcag/2023/0125/LIBE_LA(2023)000664_EN.pdf; https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7246. Per approfondimento sui negoziati e sulla procedura vedasi anche Presidenza del Consiglio dell'Unione europea, Relazione sullo stato di avanzamento dei lavori, 23 maggio 2022, 9296/22, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CONSIL:ST_9296_2022_INIT. V. FORLANI G., The E-evidence Package - The Happy Ending of a Long Negotiation Saga, in *www.eucrim.eu*, 2023,2, p. 174.

[441] 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, in G.U.U.E. L 191181 del 28 luglio 2023, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32023L1544 .

[442] Regolamento (UE) 1543/2023, cit.

17/04/2018	Legislative proposal published	COM(2018)0225
31/05/2018	Committee referral announced in Parliament, 1st reading	
12/10/2018	Debate in Council	3641
21/10/2019	Committee referral announced in Parliament, 1st reading	
07/12/2020	Vote in committee, 1st reading	
07/12/2020	Committee decision to open interinstitutional negotiations with report adopted in committee	
11/12/2020	Committee report tabled for plenary, 1st reading	A9-0256/2020
14/12/2020	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 71)	
16/12/2020	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)	
30/01/2023	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	PE740.885 GEDA/A/(2023)000664
12/06/2023	Debate in Parliament	
13/06/2023	Results of vote in Parliament	
13/06/2023	Decision by Parliament, 1st reading	T9-0225/2023
27/06/2023	Act adopted by Council after Parliament's 1st reading	
12/07/2023	Final act signed	
28/07/2023	Final act published in Official Journal	

443 *Procedura interna sulla proposta*

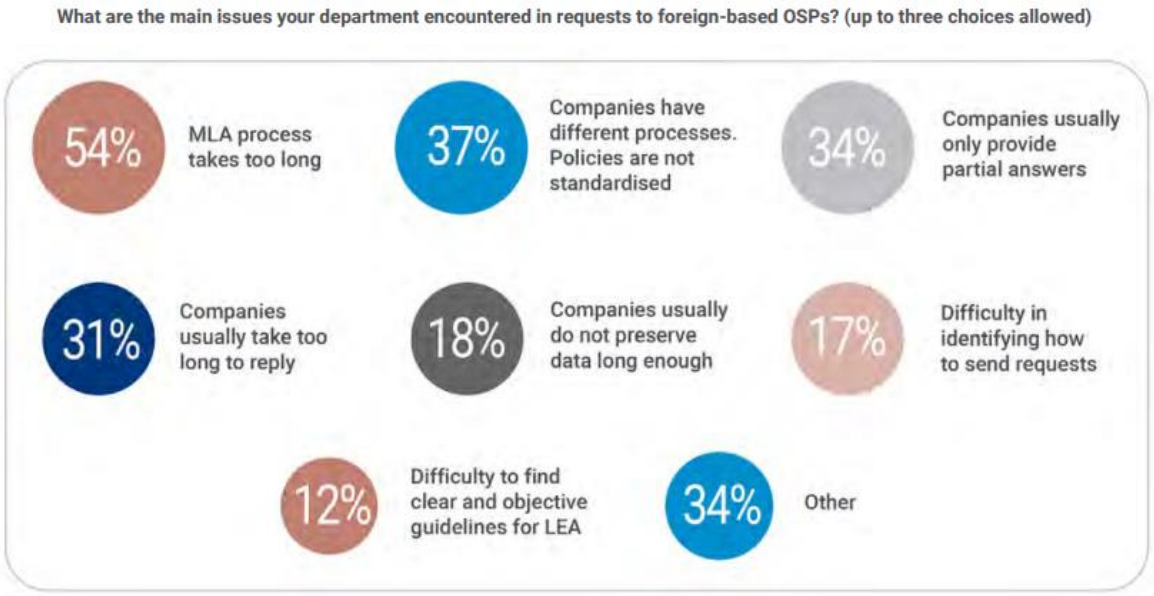
443 Osservatorio legislativo del Parlamento europeo, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2018/0108(OLP) .

Nell'elaborare il Regolamento, la Commissione ha agito nella piena consapevolezza che *internet* non conosce frontiere e che i servizi possono essere prestati in qualunque parte del mondo, senza necessità di un'infrastruttura fisica nello Stato in cui i servizi stessi vengono offerti.

Infatti, in un numero sempre maggiore di procedimenti penali le autorità richiedono accesso a dati conservati al di fuori del proprio Paese, a *provider* localizzati in altri Stati membri o in Paesi terzi.

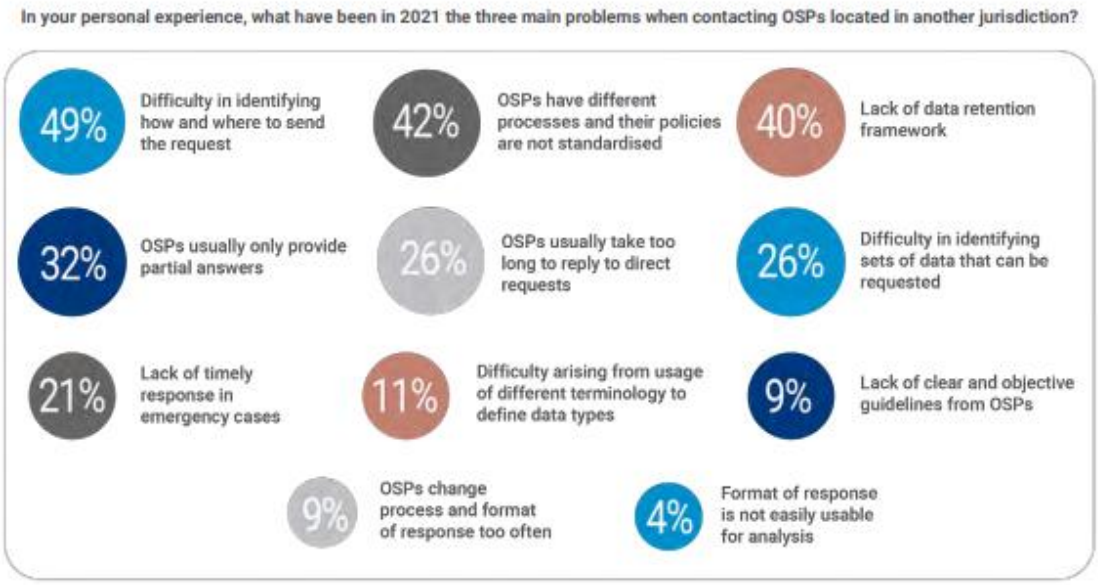
I principali profili problematici legati all'inoltro di richieste ai *provider* stranieri sono:

- lunghezza delle procedure di MLA o dei tempi impiegati dai *provider*,
- mancanza di procedure standardizzate,
- ottenimento di risposte parziali,
- mancata conservazione dei dati per un periodo sufficiente,
- difficoltà a identificare le modalità di invio della richiesta,
- mancanza di *guidelines* per le forze di polizia, sufficientemente chiare e oggettive.



[444] *Percentuali dei principali problemi affrontati dalle autorità di polizia in merito alle richieste a online service provider con sede all'estero*

[444] *SIRIUS EU Digital Evidence Situation Report 2022*, cit., p. 20



[445] *Principali problemi relativi alla comunicazione con online service provider con sede all'estero*

Va subito precisato come l'ordine europeo di produzione (da qui in avanti EPO) dei dati elettronici non intenda sostituirsi all'OEI – che continuerà ad applicarsi per l'assunzione delle prove non digitali – ma piuttosto affiancarsi ad esso per i dati precostituiti e ciò, a partire dal 18 agosto 2026, data in cui entrerà in vigore. Come per l'OEI, anche nel nuovo testo, rivestono fondamentale importanza il principio di proporzionalità e di specialità, dal momento che lo strumento non potrà essere utilizzato con finalità preventiva ma solo per procedimenti già avviati.

Per maggior chiarezza, si riporta di seguito un confronto grafico tra la procedura dell'OEI e quella dell'EPO:

[446]

[445] *Ibidem*, p. 45.
[446] *Frequently Asked Questions: New EU rules to obtain electronic evidence*, https://ec.europa.eu/commission/presscorner/detail/el/MEMO_18_3345 .

4.2.5.1. Profili definitori

L'EPO, nella versione originaria[447], era indicato come la decisione vincolante di un'autorità di emissione di uno Stato membro attraverso la quale si richiede la produzione di prove elettroniche a un prestatore di servizi che offra servizi nell'Unione e che è stabilito o rappresentato in un altro Stato membro (art. 2 co. 1).

> (1) 'European Production Order' means a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence;

Nel corso dei negoziati, tuttavia, l'articolo è stato emendato e la versione sulla quale Consiglio e Parlamento hanno raggiunto un accordo, privilegiando una maggiore specificità sull'autorità di emissione competente, è la seguente: «la decisione che dispone la produzione di prove elettroniche, emessa o convalidata da un'autorità giudiziaria di uno Stato membro […], e rivolta a uno stabilimento designato o a un rappresentante legale di un prestatore di servizi che offre servizi nell'Unione, qualora tale stabilimento designato o rappresentante legale sia ubicato in un altro Stato membro vincolato dal presente regolamento»[448].

> (1) 'European Production Order' means a decision ordering the production of electronic evidence, issued or validated by a judicial authority of a Member State in accordance with Article 4(1), (2), (4) and (5), and addressed to a designated establishment or to a legal representative of a service provider offering services in the Union, where that designated establishment or legal representative is located in another Member State bound by this Regulation;

[447] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, 17 aprile 2018, COM (2018) 225 finale, cit., Art. 2 (1)
[448] Art. 3 (1).

449

L'ordine europeo di conservazione (EPO-PR) è la decisione, emessa o convalidata a un'autorità giudiziaria di uno Stato membro, che ingiunge a un prestatore di servizi di conservare prove elettroniche in vista di una successiva richiesta di produzione[450].

> 'European Preservation Order' means a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to preserve electronic evidence in view of a subsequent request for production;

Versione originaria

> (2) 'European Preservation Order' means a decision which orders the preservation of electronic evidence for the purposes of a subsequent request for production, and which is issued or validated by a judicial authority of a Member State in accordance with Article 4(3), (4) and (5), and addressed to a designated establishment or to a legal representative of a service provider offering services in the Union, where that designated establishment or legal representative is located in another Member State bound by this Regulation;

Versione definitiva

449 *Frequently Asked Questions: New EU rules to obtain electronic evidence*, cit.

450 Art. 3 (2): «la decisione che dispone la conservazione di prove elettroniche ai fini di una richiesta di produzione successiva, e che è emessa o convalidata da un'autorità giudiziaria di uno Stato membro a norma dell'articolo 4, paragrafi 3, 4 e 5, e rivolta a uno stabilimento designato o a un rappresentante legale di un prestatore di servizi che offre servizi nell'Unione, qualora tale stabilimento designato o rappresentante legale sia ubicato in un altro Stato membro vincolato dal presente regolamento».

4.2.5.2. *L'autorità di emissione*

Quanto all'autorità emittente, il testo della proposta prevedeva un doppio binario nel caso in cui venissero richiesti *subscriber data* o dati utili per la sola identificazione degli utenti e, per altro verso, nel caso in cui si volessero ottenere *traffic data.*

Qualora l'EPO sia finalizzato ad ottenere dati di traffico, a meno che questi siano finalizzati alla sola identificazione dell'utente, potrà essere emesso da:

a) un giudice, un organo giurisdizionale o un magistrato inquirente competente nel caso interessato, o

b) qualsiasi altra autorità competente, definita dallo Stato di emissione che, nel caso di specie, agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale. In tal caso l'EPO è convalidato, previo esame della sua conformità alle condizioni di emissione, dalle autorità di cui alla lettera a.

Le maggiori tutele apprestate – che si sostanziano nell'escludere il pubblico ministero dai soggetti legittimati in via autonoma – si giustificano per la particolare intrusività che caratterizza il controllo dei dati di traffico, in virtù dei quali è possibile tracciare un profilo specifico della personalità e delle abitudini di un soggetto.

Una scelta, peraltro, compatibile con gli orientamenti della CGUE[451] in tema di *data retention* e accesso ai dati.

Diversamente, in tutti i casi di emissione di un EPO-PR o di un EPO adottato per *subscriber data* o dati utili ai fini dell'identificazione di un utente, le autorità competenti saranno:

a) un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero competente nel caso in esame, o

b) qualsiasi altra autorità competente, secondo la legge dello Stato di missione, che nel procedimento agisca in qualità di autorità inquirente e sia legittimata ad acquisire prove. In tal caso l'ordine dovrà essere convalidato da uno dei soggetti di cui alla lettera a, che valuterà la conformità alle condizioni di emissione.

Se l'ordine dovesse necessitare della convalida, l'autorità di emissione sarà sempre quella incaricata della convalida.

[451] CGUE C-746/18, *H. K. v Prokuratuur;* CGUE, C-724/19, *HP.*

In caso di emergenza[452], l'ordine potrà eccezionalmente essere emesso senza convalida preventiva, qualora questa non possa essere ottenuta in tempo utile e, laddove in un caso interno analogo, le autorità possano emettere l'atto.

La convalida dovrà tuttavia essere fatta al più tardi entro 48 ore; in mancanza, l'autorità di emanazione dovrà ritirare l'ordine e cancellare i dati ricevuti o limitarne l'uso (art. 4 co. 5).

Il Regolamento, all'art.1 co. 2, prevede la possibilità per la difesa dell'indagato o imputato di richiedere l'emanazione degli ordini, in conformità alla legislazione nazionale.

Tuttavia, come già accade nell'ambito dell'OEI, la disposizione non garantisce pienamente l'indagato o l'imputato, obbligato a disvelare la propria strategia difensiva già al momento stesso della richiesta, con il rischio peraltro che l'iniziativa sia bloccata dall'autorità giudiziaria.

Un ulteriore limite – anche questo comune all'OEI – è la mancanza di qualunque riferimento al difensore della vittima del reato, il quale, al più, potrebbe sottoporre la richiesta alle autorità competenti ai sensi della propria legislazione nazionale, con il rischio di trattamenti differenziati tra i vari Stati membri.

4.2.5.3. I destinatari della richiesta

Gli ordini vanno inoltrati direttamente a uno stabilimento designato dal rappresentante legale del *provider*.

Qualora questo soggetto non risponda all'ordine, in caso di emergenza o di grave rischio di perdita dei dati, si potrà inoltrare a qualsiasi stabilimento o rappresentante legale del *provider* all'interno dell'Unione.

Il regolamento chiarisce, inoltre, cosa debba intendersi per *provider*, qualificandolo come la persona fisica o giuridica che fornisca uno più delle seguenti categorie di servizi (art. 3 co. 3):

a. servizi di comunicazione elettronica[453];
b. servizi di nomi di dominio *internet* e di numerazione IP, quali i prestatori di indirizzi IP, i registri di nomi di dominio, i *registrars* di nomi di dominio e i connessi servizi per la *privacy* o *proxy*;

[452] Ai sensi dell'art. 2 (15), le situazioni di emergenza sono caratterizzate da un imminente pericolo per la vita o l'integrità fisica o la sicurezza di una persona o di un'infrastruttura strategica.
[453]«Come definiti all'art. 2, punto 4, della direttiva che istituisce il codice europeo delle comunicazioni elettroniche».

c. servizi della società dell'informazione[454] attraverso i quali gli utenti scambiano comunicazioni e che processano o conservano dati per contro degli utenti, quando la conservazione è componente determinante del servizio offerto.

Condizione per l'invio della richiesta è che il *provider* offra servizi nell'Unione europea e ivi abbia uno stabilimento o, in assenza di tale elemento, che abbia un legale rappresentante in uno degli Stati membri.

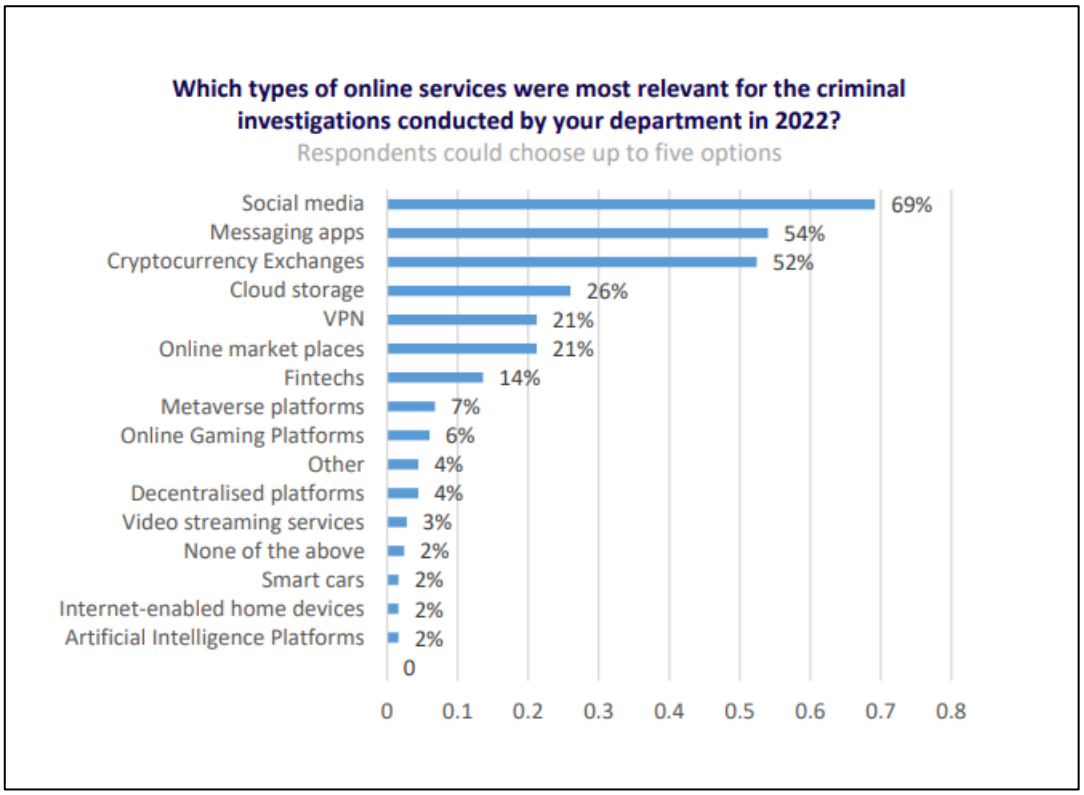
Il requisito dell'offerta dei servizi nell'Unione è soddisfatto se questi siano messi a disposizione di persone fisiche o giuridiche in uno Stato membro con cui vi sia una connessione sostanziale basata su specifici criteri oggettivi, quali la presenza di uno stabilimento o, in assenza, la presenza di un numero significativo di utenti in uno o più Stati membri o di attività mirate ad uno o più Stati membri[455].

Per stabilimento, inoltre, si intende un'entità che esercita effettivamente un'attività economica a tempo indeterminato, con un'infrastruttura stabile a partire dalla quale è svolta l'attività di prestazione di servizi o è gestita l'attività (art. 3 co. 5).

---

[454] «Come definiti all'art. 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio 44 ».

[455] Art. 2 (4). E inoltre, Considerando 27: «I prestatori di servizi più pertinenti per l'acquisizione di prove nei procedimenti penali sono i prestatori di servizi di comunicazione elettronica e specifici prestatori di servizi della società dell'informazione che facilitano l'interazione tra utenti. Pertanto, entrambi i gruppi dovrebbero rientrare nell'ambito di applicazione del presente regolamento […] Il trattamento dei dati dovrebbe essere inteso nel senso tecnico di creazione o manipolazione di dati, vale a dire di operazioni tecniche volte a produrre o modificare dati attraverso la potenza di elaborazione informatica. Le categorie di prestatori di servizi che rientrano nel presente regolamento dovrebbero includere, ad esempio, i mercati online che offrono ai consumatori e alle imprese la possibilità di comunicare tra loro e altri servizi di *hosting*, anche quando il servizio è fornito attraverso *cloud computing*, nonché le piattaforme di gioco online e le piattaforme di gioco d'azzardo online. Se un prestatore di servizi della società dell'informazione non offre ai propri utenti la possibilità di comunicare tra loro, ma solo con il prestatore di servizi, o non offre la possibilità di memorizzare o altrimenti trattare dati, ovvero se la conservazione di dati non costituisce una componente propria, ovvero una parte essenziale del servizio fornito agli utenti, quali i servizi giuridici, di ingegneria architettonica e contabili forniti online a distanza, esso non dovrebbe rientrare nella definizione di "prestatore di servizi" di cui al presente regolamento, anche se i servizi forniti da tale prestatore sono servizi della società dell'informazione ai sensi della direttiva (UE) 2015/1535». Ed inoltre, al Considerando 29: «Per determinare se un prestatore di servizi offre servizi nell'Unione occorre verificare se il prestatore di servizi consente alle persone fisiche o giuridiche di uno o più Stati membri di usufruire dei suoi servizi. Tuttavia, la semplice accessibilità di un'interfaccia online nell'Unione, ad esempio l'accessibilità di un sito web o di un indirizzo di posta elettronica o di altri dati di contatto di un prestatore di servizi o di un intermediario, presi singolarmente, dovrebbero essere considerati insufficienti per determinare che un prestatore di servizi offre servizi nell'Unione ai sensi del presente regolamento». Considerando 30: «L'orientamento delle attività verso uno Stato membro potrebbe anche desumersi dalla disponibilità di un'applicazione ("app") nell'apposito negozio online ("app store") nazionale, dalla fornitura di pubblicità a livello locale o nella lingua generalmente usata nello Stato membro in questione o dalla gestione dei rapporti con la clientela, ad esempio la fornitura dell'assistenza alla clientela nella lingua generalmente usata in tale Stato membro».



[456] *Servizi online più rilevanti per le indagini svolte nel 2022*

4.2.5.4. Tipologie di prove e dati acquisibili

Secondo l'originaria proposta, per prove elettroniche dovevano intendersi quelle «conservate in formato elettronico dal prestatore di servizi o per suo conto al momento della ricezione del certificato di ordine europeo di produzione o di conservazione, consistenti nei dati conservati relativi agli abbonati, agli accessi, alle operazioni o al contenuto» [457].

La definizione è stata poi modificata, riferendosi il testo alle prove conservate in formato elettronico da o per conto di un *service provider*, consistenti in dati relativi agli abbonati (*subscriber data)*, *traffic data*, e dati di contenuto (*content data).*

E infatti, la suddivisione dei dati in queste tre categorie, alle quali va aggiunta quella relativa ai "dati richiesti al solo scopo di identificare l'utente", è intervenuta in un momento

[456] *SIRIUS EU Electronic Evidence Situation Report 2023, 5th Annual Report*, 18 dicembre 2023, https://www.eurojust.europa.eu/publication/sirius-eu-electronic-evidence-situation-report-2023, p. 23.
[457] Art. 2 (6).

successivo, posto che la proposta originaria distingueva tra *subscriber data, access data* [458], *transactional data* [459] e *content data* [460].

Nel testo è effettuata un'opportuna distinzione dei dati in:

a) *subscriber data* che riguardano:
   - l'identità di un abbonato o un cliente (nome, data di nascita, indirizzo postale o geografico, dati di fatturazione e pagamento, numero di telefono indirizzo *email*);
   - il tipo di servizio e la durata, tra cui i dati tecnici e quelli che identificano le misure tecniche correlate o le interfacce usate dal cliente o dall'abbonato o a questi fornite e i dati connessi all'uso del servizio, ad esclusione di *password* o altri mezzi di autentificazione forniti dall'utente o creati a sua richiesta.

b) "Dati richiesti ai fini della sola identificazione dell'utente, ovvero indirizzi IP[461], e se necessario, porte di origine e indicatori temporali o equivalenti tecnici di tali indicatori e informazioni correlate, laddove richieste per il solo scopo di identificare l'utente in specifici procedimenti penali.

c) *Traffic data*, relativi alla fornitura di un servizio e che permettono di fornire un contesto o informazioni addizionali a riguardo (fonte e destinatario del messaggio o di altro tipo di interazione, dati di localizzazione, data, orario, durata, dimensione, formato, protocollo utilizzato e tipo di compressione, includendo metadati sulle

[458] «"dati relativi agli accessi": i dati riguardanti l'inizio e la fine di una sessione di accesso utente a un servizio strettamente necessari al solo fine di identificare l'utente del servizio, come la data e l'ora d'uso, o la connessione al servizio (*log-in*) e la disconnessione (*log-off*) dal medesimo, unitamente all'indirizzo IP assegnato all'utente dal prestatore di servizi di accesso a internet, ai dati che identificano le interfacce usate e all'identificativo utente. Rientrano in questa categoria i metadati delle comunicazioni elettroniche come definiti all'articolo 4, paragrafo 3, lettera c), del [regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche».

[459] «"dati relativi alle operazioni": i dati riguardanti la fornitura di un servizio offerto da un prestatore di servizi che servono per fornire informazioni di contesto o supplementari sul servizio e che sono generati o trattati da un sistema di informazione del prestatore di servizi, come la fonte e il destinatario di un messaggio o altro tipo di interazione, i dati sull'ubicazione del dispositivo, la data, l'ora, la durata, le dimensioni, il percorso, il formato, il protocollo usato e il tipo di compressione, a meno che tali dati costituiscano dati relativi agli accessi. Rientrano in questa categoria i metadati delle comunicazioni elettroniche come definiti all'articolo 4, paragrafo 3, lettera c), del [regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche]».

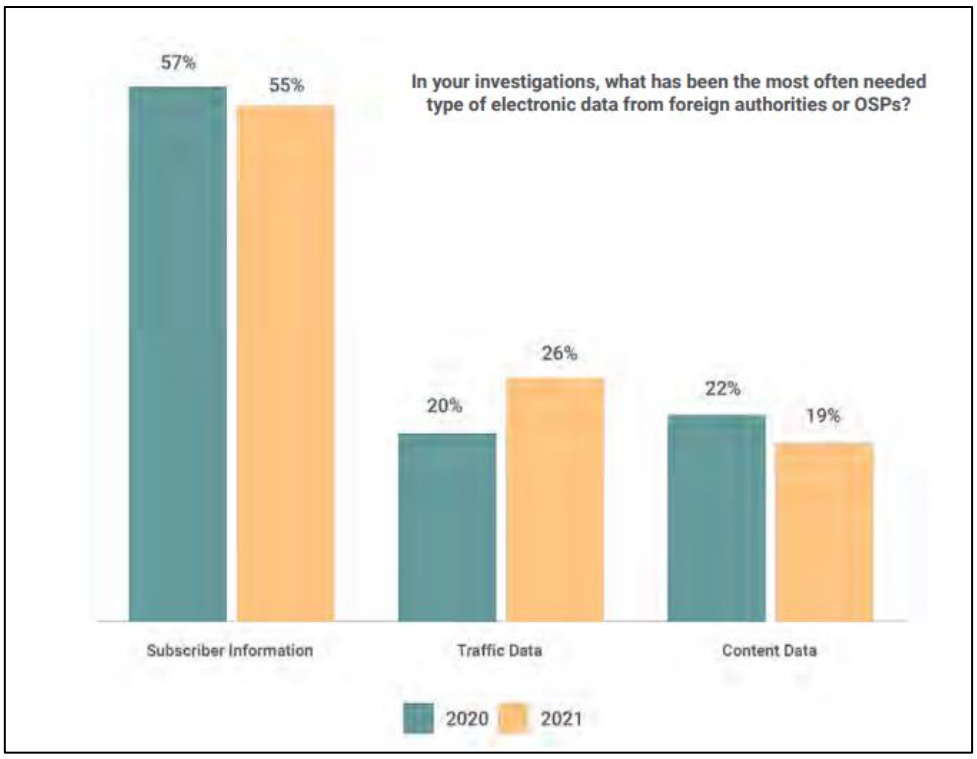
[460] «"dati relativi al contenuto": qualsiasi dato conservato in formato digitale, come testo, voce, video, immagine o suono, diverso dai dati relativi agli abbonati, agli accessi e alle operazioni».

[461] Il considerando 22 ritiene che, conformemente all'interpretazione della Corte europea di giustizia, gli indirizzi IP sono considerati dati personali e devono beneficiare della protezione completa in relazione all' "*EU data protection acquis*". In specifiche circostanze, questi, possono essere considerati dati di traffico. Tuttavia, per specifici procedimenti penali le autorità di polizia vi ricorrono per identificare l'utente. In questi casi, il legislatore comunitario ha ritenuto di poter applicare lo stesso regime dei *subscriber data*. Quando invece l'indirizzo IP, i numeri di accesso o le informazioni connesse non siano richiesti per identificare il soggetto, ma per fini ulteriori legati alle indagini, si potrebbe incorrere in un'eccessiva ingerenza all'interno della sfera privata del soggetto, potenzialmente idonea a tracciare il profilo di un individuo.
E inoltre, tali dati, sono più facilmente accessibili rispetto ai dati di contenuto, per cui è essenziale che siano trattati come dati di traffico e richiesti secondo il regime previsto per i dati di contenuto.

comunicazioni elettroniche e relativi all'inizio e alla fine di un accesso), che non rientrino tra i *subscriber data*.

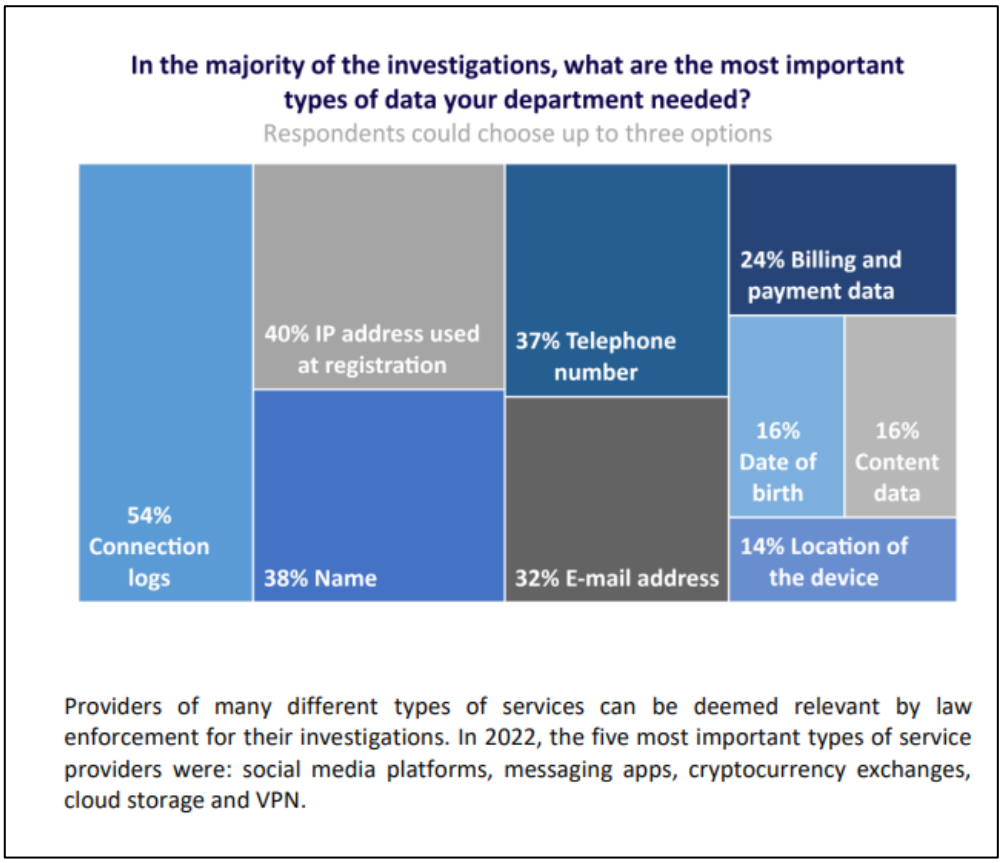
d) *content data*: qualsiasi dato conservato in formato digitale quale testo, registrazione vocale, immagine o suono diverso dalle altre categorie di data.

Le modifiche apportate alla definizione di prova elettronica e alla classificazione dei dati a questa riconducibili sono certamente appropriate, dal momento che evitano di creare distinzioni ulteriori a quelle già previste dalle fonti internazionali e si avvicinano, invece, alle categorie già utilizzate nella Convenzione di Budapest.

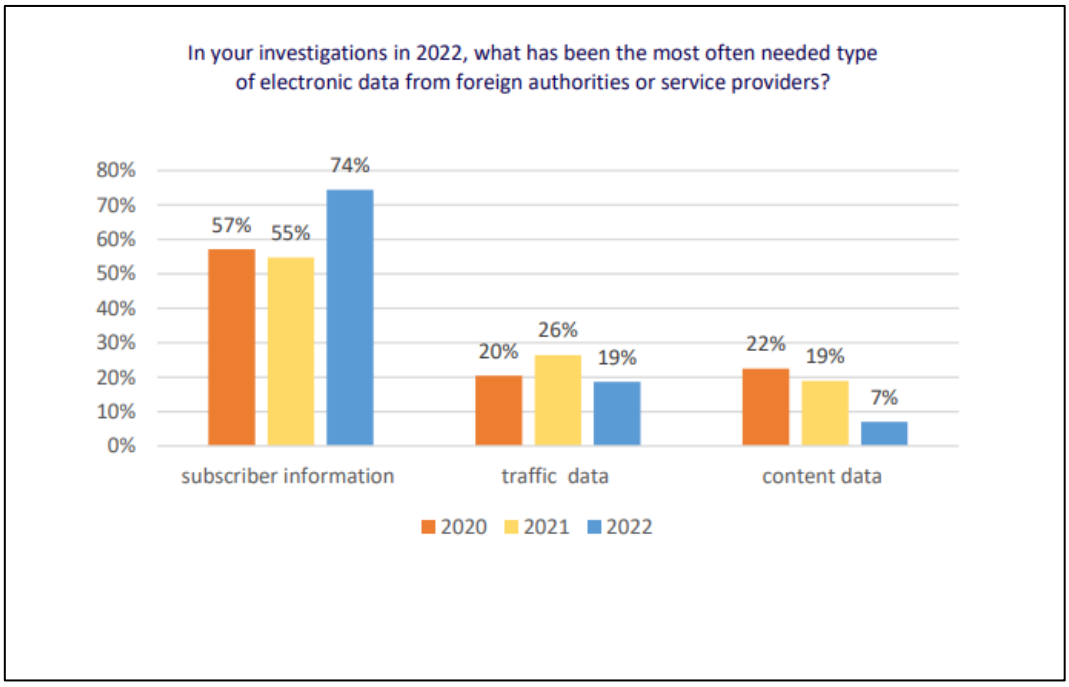


[462] *Categorie di dati più utili per le indagini, in possesso di provider stranieri (Report SIRIUS 2022)*

[462] *SIRIUS EU Digital Evidence Situation Report* 2022, cit., p. 27.



463 Categorie di dati più importanti per le indagini (Report SIRIUS 2023)



464 Confronto sulle tipologie di dati più richieste per le indagini dal 2020 al 2022

[463] *SIRIUS EU Electronic Evidence Situation Report 2023, 5th Annual Report*, cit., p. 22
[464] *Ibidem*, p. 33.

4.2.5.5. La procedura di emissione

Gli ordini possono essere emessi in relazione a procedimenti penali contro persone fisiche o giuridiche, qualora queste ultime possano essere considerate responsabili o punibili nello Stato di emissione.

Gli emendamenti alla proposta hanno, inoltre, esteso l'applicazione all'esecuzione di pene detentive o di misure di sicurezza privative della libertà non inferiore a 4 mesi, irrogate a seguito di un procedimento penale e non applicate *in absentia*, qualora il condannato si sottragga alla giustizia. Inoltre, gli ordini possono essere emessi in relazione a procedimenti per i quali una persona giuridica potrebbe essere considerata responsabile o punibile nello Stato di emissione.

L'emissione è subordinata ai criteri di necessità e proporzionalità e può avvenire solo se un ordine dello stesso tipo avrebbe potuto essere emesso alle stesse condizioni in un caso interno analogo.

Per i dati di traffico e di contenuto è, tuttavia, prevista una disciplina più restrittiva, in quanto l'EPO, vista l'intrusività determinata dall'accesso a tali categorie di dati, può essere emesso solo per particolari categorie di reati:

- reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni,
- reati di terrorismo[465] e, inoltre, se commessi in tutto o in parte attraverso sistemi informatici,
- utilizzo fraudolenti di mezzi di pagamento diversi dai contanti[466],
- abusi sessuali, sfruttamento sessuale di minori e pedopornografia[467],
- attacchi contro sistemi informatici[468],

[465] Artt. 3-12 e 14 della Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio, G.U.U.E. L 88 del 31 marzo 2017: reati di terrorismo, reati riconducibili a un gruppo terroristico, pubblica provocazione per commettere reati di terrorismo, reclutamento a fini terroristici, fornitura di addestramento a fini terroristici, ricezione di addestramento a fini terroristici, viaggi a fini terroristici, organizzazione o agevolazione di viaggi a fini terroristici, finanziamento del terrorismo, altri reati connessi ad attività terroristiche; concorso, istigazione e tentativo.

[466] Nello specifico artt. 3-8 della Direttiva 2019/713/UE del Parlamento europeo e del Consiglio del 17 aprile 2019 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio, G.U.U.E. L 123/18.

[467] Artt. 3-7 Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio, in G.U. L 335 del 17 dicembre 2011: abuso sessuale, sfruttamento sessuale, pornografia minorile, adescamento di minori per scopi sessuali; istigazione, favoreggiamento, concorso e tentativo.

[468] Artt. 3-8 della Direttiva (UE) 2013/40/UE del Parlamento europeo e del Consiglio del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, G.U.U.E. L 218 del 14 agosto 2013.

- per l'esecuzione di una pena detentiva o una misura di sicurezza non inferiore ai 4 mesi, inflitta per i reati di cui sopra.

Gli ordini dovranno contenere le seguenti informazioni:

- i dati relativi all'autorità di emissione e, laddove applicabile, all'autorità di convalida;
- il destinatario,
- le persone i cui dati sono richiesti, tranne quando questo sia da identificare attraverso i dati richiesti,
- la tipologia di dati richiesti, secondo la categorizzazione fatta dal regolamento,
- l'eventuale limite di tempo in cui è richiesta la consegna,
- l'indicazione delle disposizioni di diritto penale applicabili dello Stato di emissione,
- le ragioni a conferma della necessità e della proporzionalità della misura.

Inoltre, solo per l'EPO, saranno anche necessari:

- i motivi posti alla base di una richiesta di emergenza o di consegna anticipata, e
- nel caso in cui l'ordine sia direttamente indirizzato al *provider*, che tratta i dati per contro del titolare del trattamento[469], la dichiarazione che l'ordine è emesso conformemente al co. 6[470],
- una descrizione sommaria del caso.

L'ordine dovrà essere inoltrato a *provider* che operino come *controller* dei dati, ai sensi del Regolamento 2016/679/UE[471]. In via eccezionale, può essere inoltrato al *provider* che tratta i dati per contro del titolare, qualora quest'ultimo non possa essere identificato con uno sforzo ragionevole da parte dell'autorità di emissione o quando indirizzare l'atto al *controller* potrebbe causare un pregiudizio alle indagini (art. 5.6).

---

[469] La proposta fa riferimento alla figura del *controller*, identificato ai sensi dell'art. 4 punto 7 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) in G.U. L 119 del 4 maggio 2016 (GDPR): « la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».

[470] Il co. 6 prevede che l'ordine europeo di produzione debba essere indirizzato ai *service providers*, che operano come *controllers*, conformemente al Regolamento UE 2016/679. Ad eccezione dei casi in cui possa essere direttamente inviato al *service provider*, che processa i dati per conto del *controller*, quando:

- il *controller* non può essere identificato con uno sforzo ragionevole dall'autorità di emissione o,
- indirizzarlo al *controller* può pregiudicare le indagini.

[471] *Ibidem.*

Nello specifico, gli ordini andranno inoltrati allo stabilimento o al rappresentante legale designato in conformità alla Direttiva sui rappresentanti legali di cui sopra.

Qualora questi, in caso di emergenza, non forniscano una rapida risposta all'EPO nei tempi richiesti, si potrà interpellare qualunque altro rappresentante legale o stabilimento del *provider* localizzato all'interno dell'Unione.

Il responsabile del trattamento (*processor*)[472] – che conserva o tratta i dati per conto del titolare – dovrà informare quest'ultimo in merito alla consegna dei dati, a meno che l'autorità di emanazione abbia richiesto al *provider* di astenersi, per lo stretto necessario, al fine di non pregiudicare le indagini, e ne abbia illustrato le ragioni (art. 5 co. 6 (a).

Se l'autorità di emissione ha motivo di ritenere che i dati di traffico, ad eccezione di quelli finalizzati alla sola identificazione, e di contenuto richiesti siano protetti da immunità e privilegi riconosciuti dal diritto dello Stato membro nel quale il destinatario risiede, o siano relativi alla libertà di stampa o di espressione[473] , richiederà dei chiarimenti alle autorità competenti dello Stato in cui si trova il destinatario, direttamente o tramite Eurojust o la Rete giudiziaria europea. Se le consultazioni avranno esito positivo, non emetterà l'EPO (art. 5 co. 10).

Quando un EPO è emesso per ottenere *traffic data*, a meno che siano utili ai soli fini dell'identificazione, e *content data*, l'autorità di emissione dovrà inoltrarlo al *provider* e, contestualmente, notificare[474] l'autorità competente dello Stato di esecuzione, a meno che vi siano ragionevoli motivi di temere che:

---

[472] Ai sensi dell'art. 4 punto 8 del Regolamento 2016/679 (GDPR): «persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento». Vedasi Considerando n. 34 della proposta emendata (*Interinstitutional File:* 2018/0108(COD): « *As a matter of principle, European Production Orders should be addressed to the service provider, acting as controller. However, in some circumstances, the delimitation between the roles of controller and processor can prove particularly challenging, in particular where several service providers are involved in the processing of data or where service providers process the data on behalf of a natural person. The delimitation between the roles of controller and processor with regard to a particular set of data requires not only specialised knowledge of the legal context, but it could also require interpretation of often very complex contractual frameworks providing in a specific case for allocation of different tasks and roles with regard to a particular set of data to various service providers. Where service providers process data on behalf of a natural person, it may be difficult in some cases to determine who the controller is, even where there is only one service provider involved. It follows that where the data is stored or processed by a service provider and there is no clarity as to who the controller is, despite reasonable efforts on the part of the issuing authority, it should be possible to address a European Production Order directly to that service provider*».

[473] Aggiunto successivamente.

[474] Sul punto parte della dottrina ritiene che tale meccanismo di notifica depotenzi l'efficacia investigativa dell'ordine. V. PEZZUTO R., *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione,* in *Dir. Pen. Cont. Rivista trimestrale*, 2019, 1, p. 69 « Come vedremo, la valenza da attribuire a questo meccanismo di notifica ed i conseguenti poteri di rifiuto dell'ordine di produzione da riconoscersi o meno all'autorità "notificata" dello Stato di esecuzione costituisce un aspetto ancora molto controverso tra gli Stati membri, che continuerà ad essere discusso nel negoziato di trilogo con il Parlamento UE e che rischia di depotenziare in maniera rilevante l'efficacia investigativa del nuovo strumento, rendendolo una sorta di "duplicato" dell'ordine europeo di indagine penale, ove alla fine prevalesse l'orientamento di un coinvolgimento sostanziale (e non meramente informativo) dell'autorità dello Stato di esecuzione già nella fase di trasmissione dell'ordine di produzione».

- il reato è stato commesso, sia in atto o sia suscettibile di essere commesso nello Stato di emissione,
- la persona i cui dati sono richiesti è residente nello Stato di emissione (art. 8 co. 1 e 2).

Questa previsione, assente nel testo originario della Commissione, costituisce uno dei punti che più hanno animato il dibattito durante i negoziati[475].

La prima formulazione della proposta prevedeva il contatto diretto con il *provider:* questi, nel caso di conflitto di legge con uno Stato terzo, avrebbe dovuto informare l'autorità dello Stato di esecuzione per avviare una procedura di revisione.

In tal modo, eventuali valutazioni relative all'esecuzione dell'ordine venivano interamente lasciate nella discrezionalità di un'azienda privata, non del tutto competente ad effettuare considerazioni legate ai diritti coinvolti. Infatti, le aziende potrebbero ritenere economicamente più opportuno consegnare immediatamente i dati, piuttosto che effettuare una valutazione sul rispetto dei diritti umani, impiegando le proprie risorse, e avviando lunghe interlocuzioni con le autorità[476].

La soluzione opposta prevedeva la consegna dell'ordine alle autorità competenti dello Stato di emissione, circostanza che avrebbe totalmente depotenziato l'efficacia dell'ordine, operando così allo stesso modo dell'OEI.

La formulazione finale della proposta sembra raggiungere un giusto compromesso tra le diverse istanze in gioco, per consentire una rapida consegna e, d'altro canto, non lasciare valutazioni rilevanti, quali quelle relative al rispetto dei diritti e delle libertà, a soggetti privi delle idonee competenze.

D'altro canto, tale notifica non è prevista per i *subscriber da*ta e i dati previsti ai soli fini dell'identificazione di un utente, ritenuti meno lesivi dei diritti fondamentali.

Per agevolare il procedimento e renderlo più rapido, la trasmissione degli ordini sarà effettuata attraverso dei moduli *standard*: l'*European Production Order Certificate* (EPOC) e l'*European Preservation Order Certificate* (EPOC-PR). Questi saranno emessi, convalidati e firmati dall'autorità di emissione e trasmessi con ogni mezzo che permetta di conservare una traccia scritta e di garantirne l'autenticità.

È possibile utilizzare apposite piattaforme utilizzate dai *provider* o altri canali sicuri.

---

[475] V. Presidenza del Consiglio UE, *Draft Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-evidence) - Certain issues: state of play and discussion*, 26 agosto 2021, 11314/21.

[476] V. JUSZCZAK A., SASON E., *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice*, in *www.eucrim.eu*, 2023, 2, p.182.

Nel contesto dell'Unione europea si prevede di autorizzare il sistema E-Codex[477] – un sistema informatizzato per lo scambio elettronico transfrontaliero di dati nel settore della cooperazione giudiziaria – o altre piattaforme all'uopo dedicate.

4.2.5.6. La fase di esecuzione

Una volta ricevuto l'ordine di produzione, il destinatario dovrà preservare i dati fino alla consegna.

Nel caso in cui sia stata inviata una notifica alle autorità dello Stato di esecuzione e queste non abbiano individuato alcun motivo di rifiuto entro 10 giorni, il *provider* provvederà a trasmettere i dati direttamente all'autorità di emissione al termine del periodo.

Qualora, invece, l'autorità di esecuzione, prima dei 10 giorni, dichiari di non avere evidenziato alcun motivo di rifiuto, il destinatario dell'EPO dovrà consegnare i dati quanto prima, entro 10 giorni dalla ricezione dell'ordine.

Nei casi di emergenza, i dati dovranno essere consegnati senza indebito ritardo, al massimo entro 8 ore dalla ricezione dell'EPOC.

Quando sia necessaria la notifica, l'autorità di esecuzione potrà, senza ritardo e al massimo entro 96 ore dalla ricezione, notificare il destinatario e l'autorità di emissione, opporsi alla consegna o richiedere che sia effettuata a specifiche condizioni.

Inoltre, nel caso in cui identifichi un motivo di rifiuto e i dati siano già stati consegnati, l'autorità di emissione dovrà cancellarli o limitarne l'utilizzo o, nel caso in cui siano state opposte delle specifiche condizioni, adempiere a queste ultime.

I motivi di rifiuto opponibili dall'autorità di esecuzione che abbia ricevuto la notifica sono i seguenti:

- i dati sono protetti da immunità o privilegi secondo la legge nazionale, o sono coperti dalle regole che limitano la responsabilità penale in relazione alla libertà di stampa o di espressione;
- in situazioni eccezioni, vi sono ragionevoli motivi di ritenere che, sulla base di prove specifiche e oggettive, l'esecuzione dell'ordine causi una manifesta violazione dei diritti fondamentali come disposto dall'art. 6 TUE e della Carta di Nizza;

[477] Definito dal Regolameto 2022/850/UE del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo a un sistema informatizzato per lo scambio elettronico transfrontaliero di dati nel settore della cooperazione giudiziaria in materia civile e penale (sistema e-CODEX) e che modifica il Regolamento (UE) 2018/1726, in G.U.U.E. L 150/1 del 1° giugno 2022. Vedasi BIASOTTI M.A, *Present and future of the exchange of electronic evidence in Europe*, in BIASIOTTI M.A. MIFSUF BONNICI J.P., CANNATACI J., TURCHI F., (a cura di), *Handling and exchanging electronic evidence across Europe*, Springer, 2019, p. 19 ss.

- l'esecuzione dell'ordine è contraria al principio del *ne bis in idem*;
- il reato per cui l'EPO è stato emesso non costituisce reato per la legge dello Stato di esecuzione, a meno che sia incluso nella lista di delitti dell'Annesso IIIA e sia punibile nello Stato di emissione con una pena detentiva o misura privativa della libertà per un periodo massimo di almeno 3 anni (art. 12 co. 1).

Quando l'autorità di esecuzione individui uno dei precedenti motivi, contatterà il *provider* e l'autorità di emissione per trovare un accordo, che potrà sfociare nella modifica o nel ritiro dell'ordine. Qualora non si trovi una soluzione, occorrerà opporre il motivo di rifiuto.

Se il destinatario, basandosi sulle informazioni contenute nel certificato, ritenga che l'esecuzione dell'ordine possa interferire con immunità o privilegi o con regole sulla determinazione o limitazione della responsabilità penale relativamente alla libertà di stampa o di pensiero prevista dallo Stato di esecuzione, informerà le autorità competenti di quest'ultimo e dello Stato di emissione.

Queste ultime terranno in considerazione le informazioni e decideranno se mantenere, adattare o ritirare l'ordine.

In merito a entrambe le tipologie di ordini, qualora il *provider* non possa adempiere ai suoi obblighi per incompletezza, errori o insufficienza delle informazioni del certificato, avvierà una comunicazione con le autorità di emissione chiedendo chiarimenti in vista di una soluzione quanto più rapida possibile.

Allo stesso modo, qualora non possa fornirle per altri motivi, provvederà ad informare le autorità affinché l'ordine sia modificato o, se necessario, sia fissato un nuovo termine.

Quando, invece, non sia possibile adempiere per cause di forza maggiore o impossibilità materiale non imputabile al destinatario (ad es. perché l'utente non è un cliente o i dati sono già stati cancellati) informerà l'autorità di emissione che, sulla scorta dei motivi addotti, può eventualmente ritirare l'ordine.

L'art. 11, sulla confidenzialità, è una delle disposizioni modificate nel corso dei negoziati. La formulazione ultima prevede che l'autorità di emissione informi la persona i cui dati sono richiesti, indicandole i rimedi esperibili. Tuttavia, se previsto dalla legge nazionale, può ritardare o omettere tale passaggio, indicando le ragioni nel certificato EPOC.

Ciò, tuttavia, secondo parte della dottrina, potrebbe causare un'applicazione dello strumento non omogenea tra gli Stati[478].

Il destinatario dell'ordine dovrà prendere tutte le misure idonee ad assicurare la confidenzialità, segretezza e integrità degli ordini e dei dati (art. 11 co. 3).

Gli Stati dovranno prevedere delle sanzioni da applicare ai *provider* in caso di violazione degli obblighi previsti, che dovranno essere effettive, proporzionate e dissuasive, nella misura di circa il 2% del fatturato totale annuale del *provider*[479].

La normativa prevede, inoltre, una forma di tutela per tali soggetti, disponendo che, senza pregiudizio per le obbligazioni relative alla protezione dei dati, non incorrano in forme di responsabilità per ragioni legate alla buona fede nell'esecuzione degli ordini (art. 13 co. 2).

È poi disciplinata, all'art. 14, una procedura di esecuzione allorquando il *provider* non adempia entro il termine prestabilito, ovvero non fornisca motivi che siano accettati dall'autorità di emissione e non siano configurabili motivi di rifiuto.

In tale circostanza, l'autorità di emissione può richiedere l'intervento dell'autorità di esecuzione che riconoscerà l'ordine, senza ulteriori formalità e non oltre 5 giorni, e prenderà le misure idonee per eseguire un EPO o un EPO-PR, a meno che individui dei motivi di rifiuto.

L'autorità di esecuzione, pertanto, richiederà al *provider* di adempiere all'ordine, informandolo della possibilità di opporre dei motivi di rifiuto e dell'eventuale applicazione di sanzioni in caso di non collaborazione.

L'esecuzione di un EPO o di un EPO-PR potrà essere negata se:

- l'ordine non è stato emesso o validato da un'autorità di emissione competente secondo il regolamento;
- sussiste un'impossibilità oggettiva di adempiere, non imputabile al destinatario, o vi sono errori manifesti nel certificato;
- l'ordine non riguarda dati conservati da o per conto del *provider* al momento dell'emissione;
- la fattispecie non è regolata dal regolamento;

---

[478] JUSZCZAK A., SASON E., *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice*, cit. p.193

[479] Art. 13, co. 1. Va segnalato che «*the threat against service providers of pecuniary sanctions for infringements of the Regulation undoubtedly undermines the "will" to scrutinize the legitimacy of the Orders, as it is rather apparent that the service provider would prefer an "easy" compliance with the Orders over being subjected to the looming threat of pecuniary sanctions*» , cit., TOPALNAKOS P., *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, in www.eucrim.eu , 2023, 2, p.200.

- i dati richiesti sono protetti da immunità o privilegi dello Stato di esecuzione, o da regola relative alla limitazione di responsabilità penale in relazione alla libertà di stampa o espressione;
- sulla scorta delle informazioni del certificato, vi sono ragioni specifiche e oggettive per ritenere che l'esecuzione dell'ordine possa violare i diritti fondamentali.

E, inoltre, solo per l'EPO quando non sia stato emanato per uno dei reati previsti dal regolamento.

Una volta ottenuti dal *provider* i dati, questi vengono trasmessi all'autorità di emissione senza indebito ritardo.

4.2.5.7. I mezzi di ricorso

L'art. 15, rubricato "Procedura di riesame in caso di obblighi contrastanti basati su diritti fondamentali o interessi fondamentali di un paese terzo", è stato abrogato nella versione definitiva della proposta.

Questo prevedeva che il destinatario informasse l'autorità di emissione dei motivi per non eseguire l'ordine, qualora la divulgazione dei dati fosse in contrasto con il diritto applicabile in un Paese terzo, nello specifico con un divieto alla divulgazione dei richiesti, a tutela dei diritti delle persone interessate o degli interessi fondamentali connessi alla sicurezza o alla difesa nazionali. Sulla base di tale segnalazione, l'autorità di emissione avrebbe potuto riesaminare l'EPO e valutare l'opportunità di una richiesta di riesame all'organo giurisdizionale competente nel territorio nazionale, per vagliare il ritiro dell'ordine o l'avvio di comunicazioni con l'autorità centrale del Paese terzo.

Tuttavia, la scelta di lasciare questa valutazione sui conflitti di legge al *provider* è stata ritenuta inadatta e, pertanto, l'articolo in questione è stato abrogato[480].

---

[480] DE BUSSER E., *The digital unfitness of mutual legal assistance,* in *Security and human rights,* 2017, vol. 28, 1: « *Three consequences of giving companies such responsibility in the context of interstate cooperation in criminal matters are particularly concerning. First, the proposed regulation effectively gives companies the role of a public authority. Where even direct contact between police authorities of two states was unthinkable in MLA until the 1990 Schengen Implementation Convention, we now see direct cross-border transfers of evidence from companies to law enforcement authorities being institutionalized. The reason why a central authority - mostly the Ministry of Justice of a country - is the intermediary for incoming requests for MLA in the 1959 CoE Convention is the protection of sovereignty and indirectly the protection of their international relations. Answering the question of whether or not to deliver assistance to a foreign criminal investigation also means judging the quality of the requesting state's criminal justice system, especially when human rights compliance is concerned. This is not the kind of responsibility that should be placed in the hands of a company. Besides the fact that companies have economic interests, the companies in question are quite often us based companies, even when acting through a legal representative in the Eu. As the first line responder to a production order for data, if the legal representative does not alert the competent enforcement authority of the member State where he or she is based, no other public authority but the issuing authority will ever get to see*

L'art. 16 disciplina, invece, la procedura di riesame basata su obblighi di legge contrastanti, in relazione alla disciplina dello Stato di emissione e di uno Stato terzo a cui sia sottoposto il *provider*.

Qualora quest'ultimo ritenga che l'assolvimento dell'EPO possa confliggere con la normativa di un Paese terzo, informerà le autorità di emissione e di esecuzione esplicandone le ragioni. L' opposizione dovrà includere tutti i dettagli rilevanti sulla legge del Paese terzo, l'applicabilità al caso specifico e la natura delle obbligazioni confliggenti e non può essere basata sul fatto che la legge del Paese terzo non preveda l'ordine di produzione o che i dati siano ivi conservati.

L'autorità di missione riesaminerà l'EPO sulla base di tale obiezione e degli input provenienti dallo Stato di esecuzione. Qualora intenda confermare l'ordine, richiederà un riesame al giudice competente all'interno del territorio nazionale e l'esecuzione sarà sospesa fino al termine della procedura. Il giudice che tratta il riesame dovrà, anzitutto, verificare se esista un conflitto, valutando se la legge dello Stato terzo si applichi al caso specifico e se dall'applicazione derivi il divieto divulgare i dati richiesti.

Se non è rilevato un conflitto, lo Stato confermerà l'ordine.

Diversamente, la Corte stabilirà se confermare o ritirare l'ordine, valutando:

- l'interesse protetto dallo Stato terzo, tra cui i diritti fondamentali o altri interessi essenziali relativi a specifici interessi di sicurezza nazionale;
- la connessione del procedimento con le due giurisdizioni, in base alla localizzazione, nazionalità e residenza del titolare dei dati e/o della vittima e al *locus commissi delicti*;
- la connessione tra il *provider* e lo Stato terzo[481];

the production order. Effectively, this means that an Eu based company or an Eu based legal representative of a third State's company has the responsibility to decide whether or not the order by a member State is in line with human rights or not. Second, companies are not equipped to be placed in such position. In addition to the argument made concerning their economic interests, companies - especially Small and Medium Sized Enterprises (SMES) - would have to spend a considerable amount of their resources to scrutinize potential grounds for refusal for every incoming request for data. Also related to the first concern, and not to be underestimated, is the risk that companies may not be able to make a proper assessment of the grounds for refusal. Third, an imaginable liability issue could arise for any company that does not object or refuse a request for data where it should have. A consumer whose data was transferred by a service provider in reaction to an order for digital evidence that was manifestly breaching the right to data protection could first of all submit a legal claim against that company. Furthermore, the evidence resulting from it would be inadmissible in the subsequent criminal proceedings and potentially - depending on the evidence laws of the member state and whether or not the fruit of the poisonous tree doctrine is supported - endanger all further evidence derived from it. Such action could therefore result in possible legal claims from victims as well ».

[481] La previsione specifica che il luogo di archiviazione dei dati non è sufficiente da solo a stabilire una sostanziale connessione.

- l'interesse ad ottenere tali prove, basato sulla serietà dell'offesa e sulla necessità di una rapida acquisizione;
- le conseguenze per il destinatario nell'adempimento dell'ordine, incluse le sanzioni in cui potrebbe incorrere.

Il giudice, nel compiere questa valutazione, potrà richiedere informazioni alle autorità dello Stato terzo; successivamente, comunicherà all'autorità di emissione e al destinatario la scelta sulla revoca o sulla conferma dell'EPO.

Ex art. 18, senza pregiudizio per gli ulteriori rimedi legali esperibili secondo il diritto interno, ogni persona i cui dati siano stati richiesti attraverso un EPO deve avere il diritto ad un rimedio effettivo. Se, peraltro, si tratta di indagato o imputato, questo diritto dev'essere garantito durante il procedimento penale in cui i dati sono utilizzati.

Infatti, lo Stato di emissione o ogni altro Stato al quale sono state inviate le prove elettroniche deve assicurare il diritto alla difesa e a un equo processo.

È da evidenziare che questi rimedi non ostano all'esperimento di quelli previsti dalla Direttiva (EU) 2016/680/UE[482] e dal Regolamento 2016/679/UE. Dovranno, inoltre, poter essere attivati davanti all'autorità giurisdizionale dello Stato di emissione, in conformità alle leggi nazionali, con la possibilità di contestare la legalità, la necessità e proporzionalità della misura, senza pregiudizio per la tutela dei diritti fondamentali nello Stato di esecuzione[483].

Non è, tuttavia, chiaro se tali rimedi possano essere utilizzati anche contro un ordine di conservazione dei dati, in ragione del riferimento espresso solo all'EPO[484].

4.2.5.8. Il sistema decentrato di comunicazione

Il nuovo art. 19 stabilisce che le comunicazioni scritte tra *provider* e autorità competenti debbano svolgersi attraverso un sistema decentrato di comunicazione (*decentralised IT system*) affidabile e sicuro.

Compito degli Stati è quello di assicurare che i *provider* abbiano accesso a questo sistema − canale privilegiato per inviare e ricevere EPOC e EPOC-PR − per inoltrare i dati richiesti e ogni altra comunicazione relativa.

---

[482] Direttiva 2016/680/UE del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in G.U.U.E. L 119/89 del 4 maggio 2016.

[483] V. DANIELE M., *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazion*ale, cit.

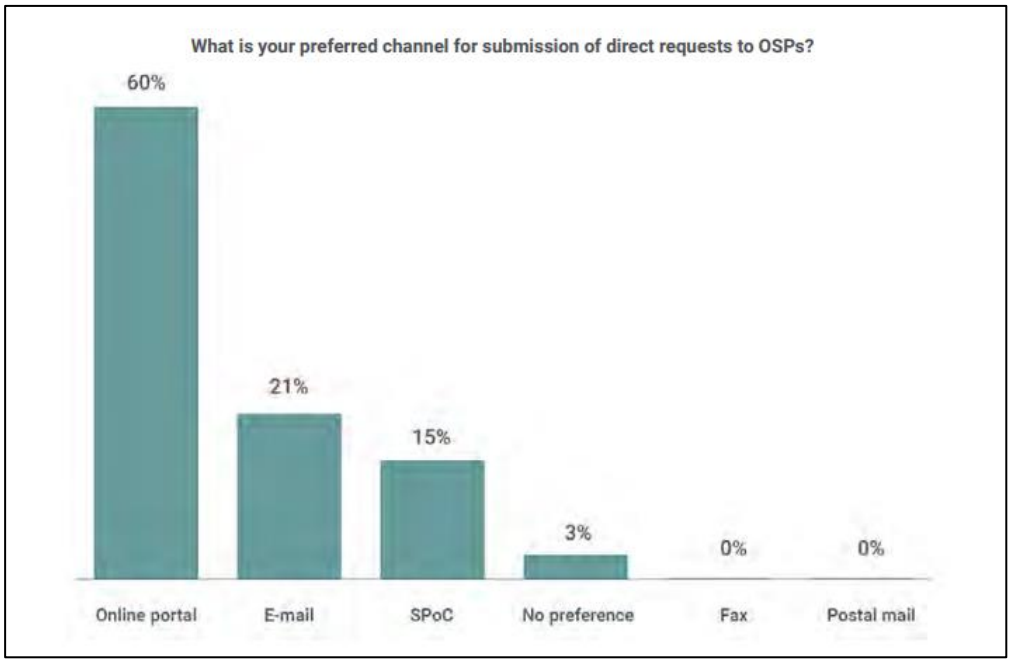
[484] JUSZCZAK A., SASON E., *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice*, cit., p.189.

Qualora non sia possibile utilizzare il sistema, in circostanza eccezionali, si potrà ricorrere ad un metodo alternativo, purché sia sicuro e affidabile. In tal caso, bisognerà poi registrare nel sistema decentrato comunicazioni, data, ora, mittente e destinatario, nome del file e dimensione.

Il Regolamento prevede inoltre che i documenti trasmessi in formato elettronico non debbano essere considerati inammissibili nel contesto della cooperazione transfrontaliera per il solo fatto che siano trasmessi in tale formato, riconoscendo il loro valore legale.

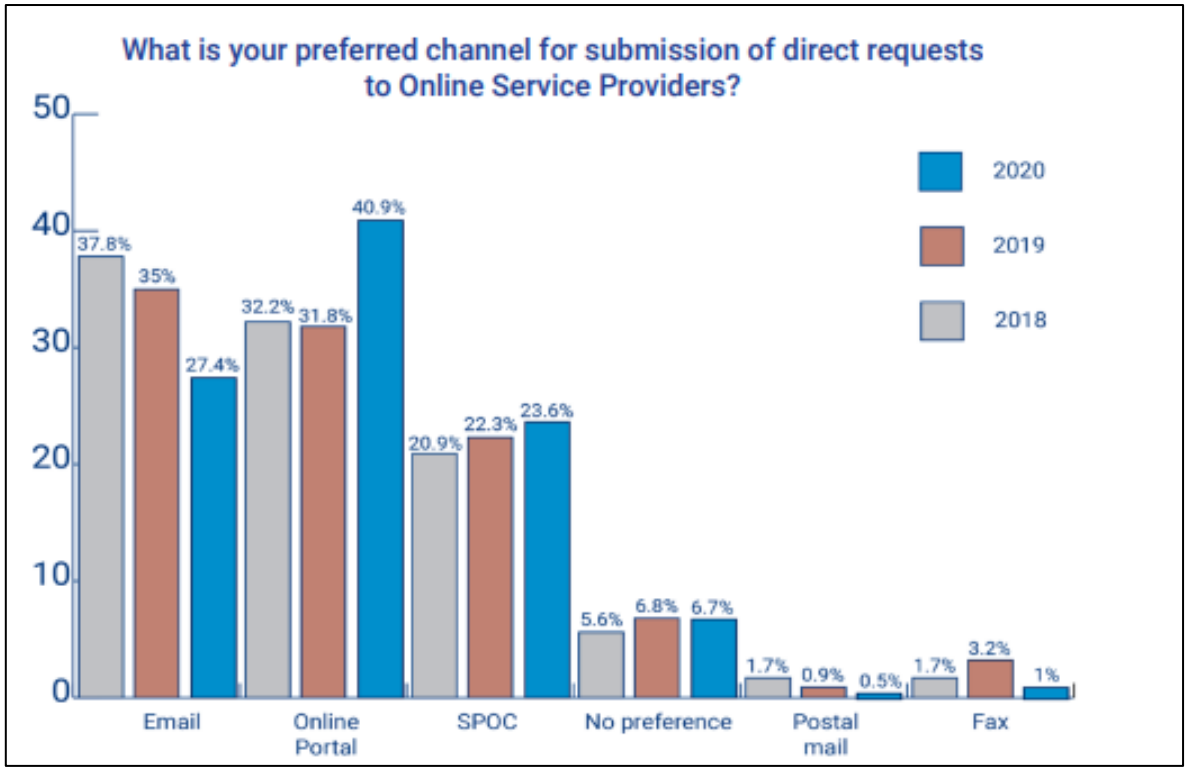
Viene lasciato alla Commissione il compito di implementare, entro due anni dall'adozione del Regolamento, l'adozione di tale sistema, stabilendo le specifiche tecniche delle comunicazioni e del funzionamento, gli obiettivi di sicurezza e gli *standard* necessari. Pertanto, questa sarà responsabile della creazione, sviluppo e mantenimento di un *software* idoneo a fungere da sistema decentrato per lo scambio di informazioni. Fino alla creazione di tale infrastruttura, gli Stati potranno adottare metodi alternativi che garantiscano adeguati livelli di sicurezza e affidabilità. In tal caso, si potranno prendere in considerazione le piattaforme E-Codex e SIRIUS, in grado di offrire una connessione sicura e affidabile.

E d'altronde, proprio in riferimento all'utilizzo di piattaforme per lo scambio sicuro di comunicazioni, le autorità di polizia hanno manifestato il loro favore rispetto a metodi alternativi, come evidenziato dal Report SIRIUS.

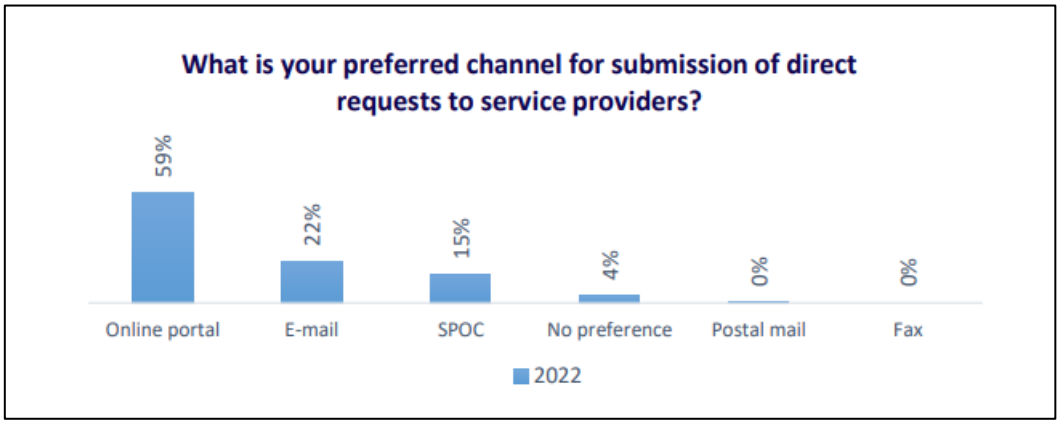


[485] *Canali più utilizzati per l'invio di richieste dirette ai provider*

[485] SIRIUS EU *Digital Evidence Situation Report 2022*, cit., p. 17.



[486] *Preferenze delle autorità di polizia in relazione ai metodi utilizzati per richiedere dati agli OSP, tendenze dal 2018 al 2020*



[487] *Preferenze delle autorità di polizia in relazione ai metodi utilizzati per richiedere dati agli OSP (2022)*

E-Codex – piattaforma che permette l'interoperabilità dei sistemi digitali nazionali – consentirà la connessione di questi per lo scambio sicuro di dati in materia civile e penale (documenti, modelli, prove e informazioni). Elemento chiave potrebbe essere il sistema eEDES – e-*Evidence Digital Exchange System*[488] – che consente lo scambio digitale di richieste di collaborazione, di documenti e prove. Questo, attraverso la sincronizzazione con

[486] *SIRIUS EU Digital Evidence Situation Report 3rd Annual Report 2021*, https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_DESR_12_2021.pdf, p 19.
[487] *SIRIUS EU Digital Evidence Situation Report 3rd Annual Report, 2023*, cit., p. 25.
[488] https://e-justice.europa.eu/37138/EN/eevidence_digital_exchange_system.

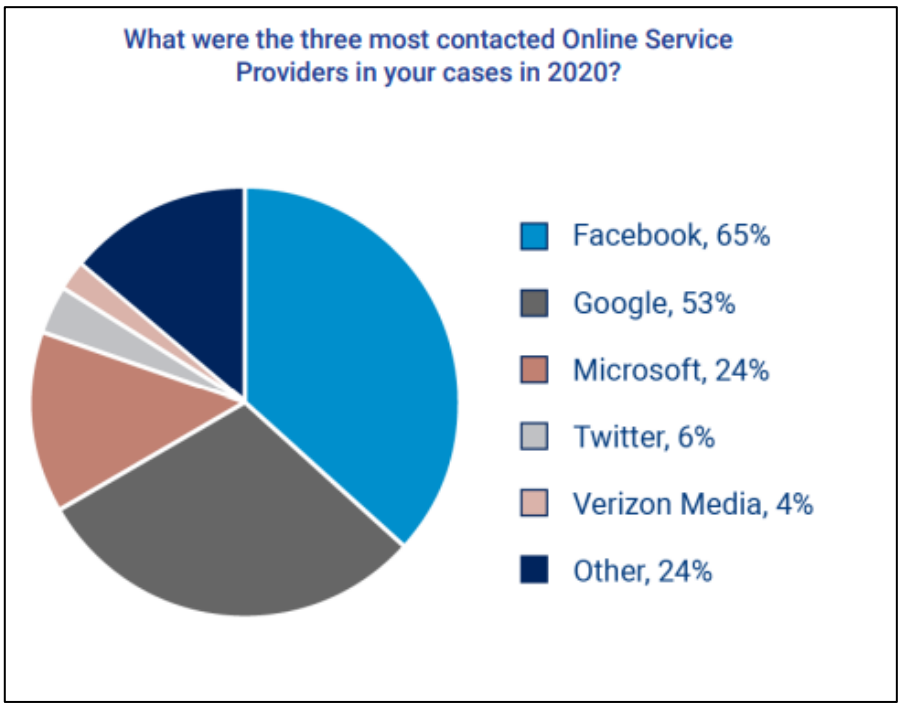
E-Codex, da utilizzare come canale di comunicazione, permetterà di velocizzare e rendere più efficaci le procedure di cooperazione transfrontaliera[489].

4.2.6. Le criticità nell'acquisizione della prova digitale nei rapporti tra UE e USA

Nel futuro, la competenza ultra-territoriale dell'EPO e dell'EPO-PR se, da un lato, faciliterà l'acquisizione di dati non fisicamente localizzati all'interno dell'Unione europea o di ubicazione ignota, dall'altro, potrebbe generare dei problemi nei rapporti con Stati terzi.

Questa eventualità assume la connotazione di una certezza, se si considera che i maggiori *service provider* hanno sede legale al di fuori dell'Unione europea e, in particolare, negli Stati Uniti[490].

Il *report* SIRIUS conferma che i fornitori più contattati dalle forze di polizia sono, già dal 2020, Facebook, Google, Microsoft e Twitter, tutte aziende con sede legale negli Stati Uniti [491].



[489] Approfondimenti in SPIEZIA F., *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: il ruolo di Eurojust,* cit.

[490] Per un *excursus* su *privacy*, *provider* e ordine pubblico v. VACIAGO G., Privacy *e tutela dell'ordine pubblico in Europa e negli Stati Uniti: un differente approccio per raggiungere un compromesso*, in *Informatica e diritto*, 2009, XVIII, 1.

[491] BIASIOTTI M.A., *Present and future of the exchange of electronic evidence in Europe*, in BIASIOTTI M.A. MIFSUF BONNICI J.P., CANNATACI J., TURCHI F., (a cura di), *Handling and exchanging electronic evidence across Europe*, Springer, 2019, p.3.

492

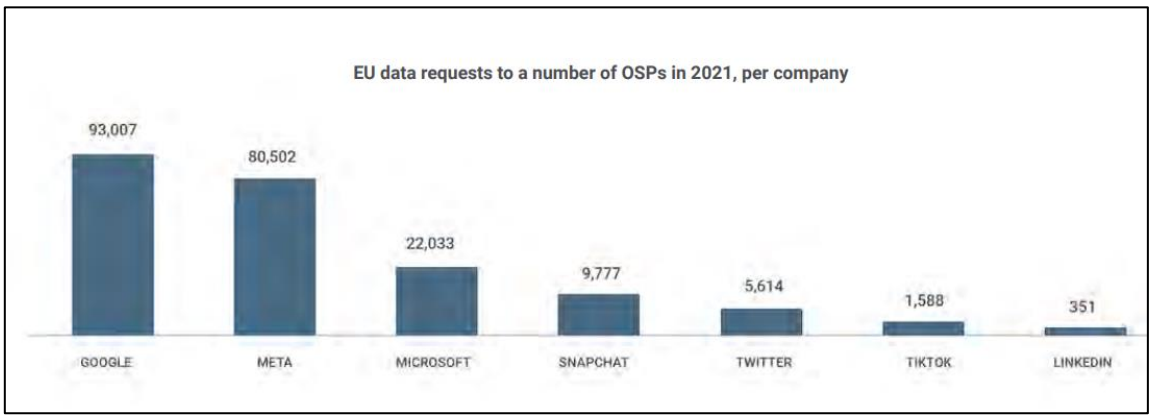
Table 9 shows the aggregated number of requests sent to four OTTs (Apple, Facebook, Google and Microsoft) over the whole of 2018 and in the period between 1 January 2019 to 30 June 2019[116].

Table 9: Total number of requests sent to OTTs, 2018 and January-June 2019

MS	January-December 2018	January-June 2019
All Member States	129,098	74,059
Germany	64,593	36,194
France	32,063	17,583
Spain	10,833	6,559
Italy	9,252	5,129
Poland	5,890	4,996
Portugal	3,909	2,242
Austria	1,656	831
Ireland	564	263
Estonia	193	176
Slovenia	145	86

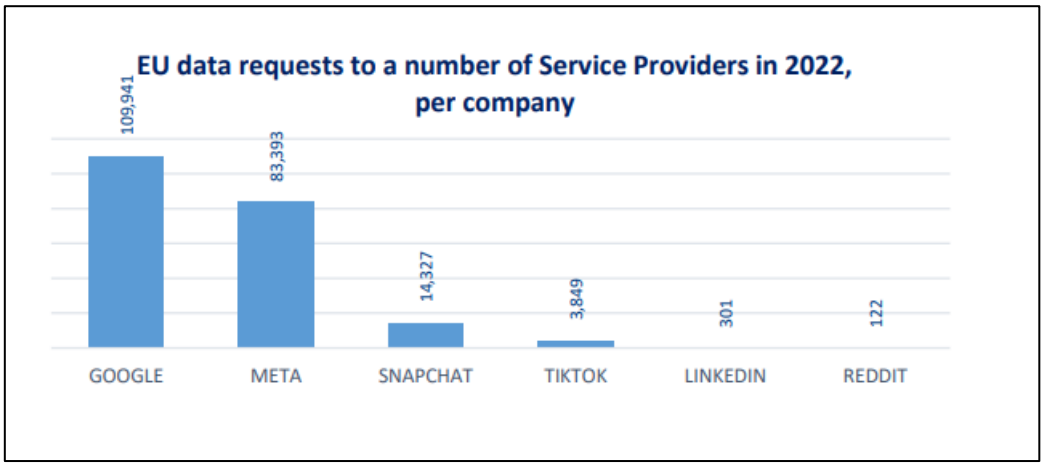
Source: Milieu elaboration from transparency reports of OTTs

493 *Numero di richieste inviate a Apple, Facebook, Google e Microsoft nell'anno 2018 e nel primo semestre 2019.*

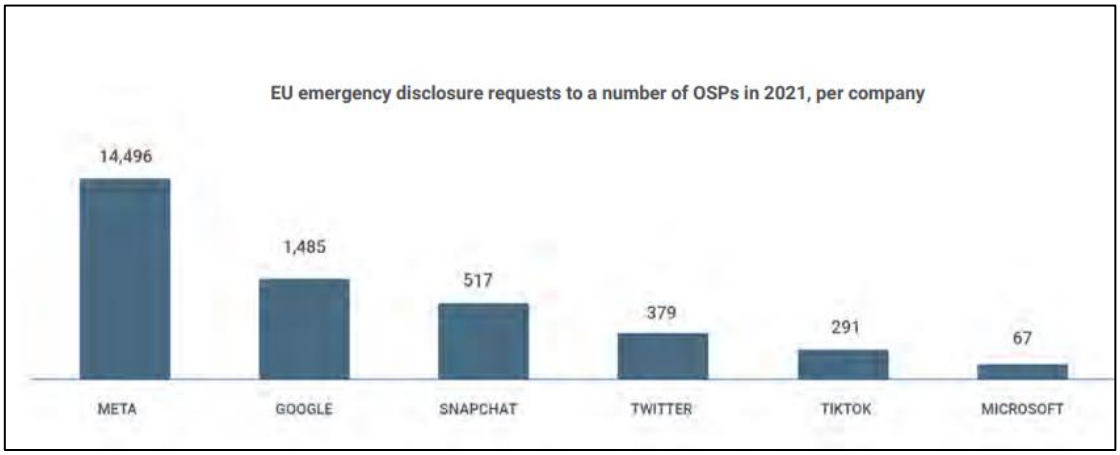


494 *Richieste inviate ai provider da Stati UE nel 2021, distinte per compagnia*

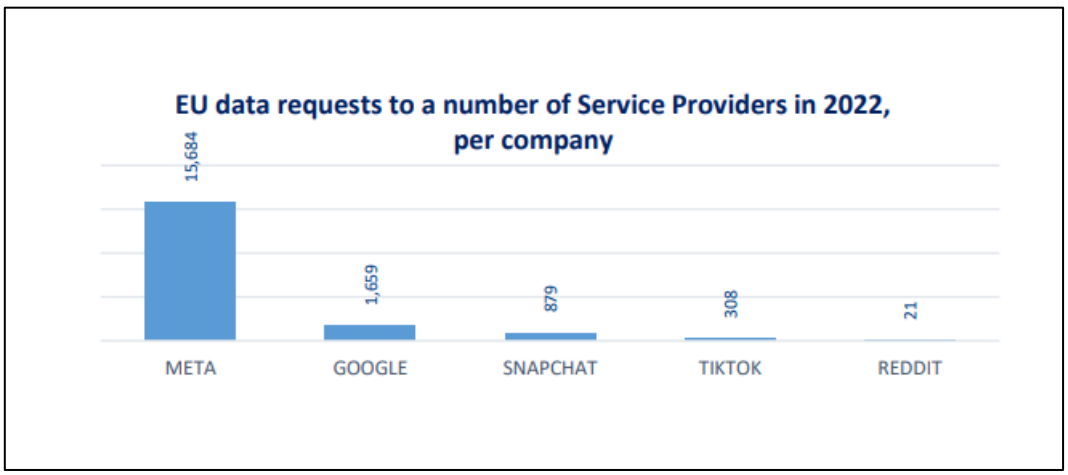
492 *SIRIUS EU Digital Evidence Situation Report 3rd Annual Report 2021,* cit., p. 28.
493 Commissione europea, *Study on the retention of electronic communications non-content data for law enforcement purposes – Final report*, https://www.statewatch.org/media/1453/eu-com-study-data-retention-10-20.pdf, p. 105.
494 *SIRIUS EU Digital Evidence Situation Report 2022*, cit., p. 61



[495] *Richieste inviate ai provider da Stati UE nel 2021, distinte per compagnia*



[496] *Richieste inviate in casi di emergenza ai provider da Stati UE nel 2021, distinte per compagnia*

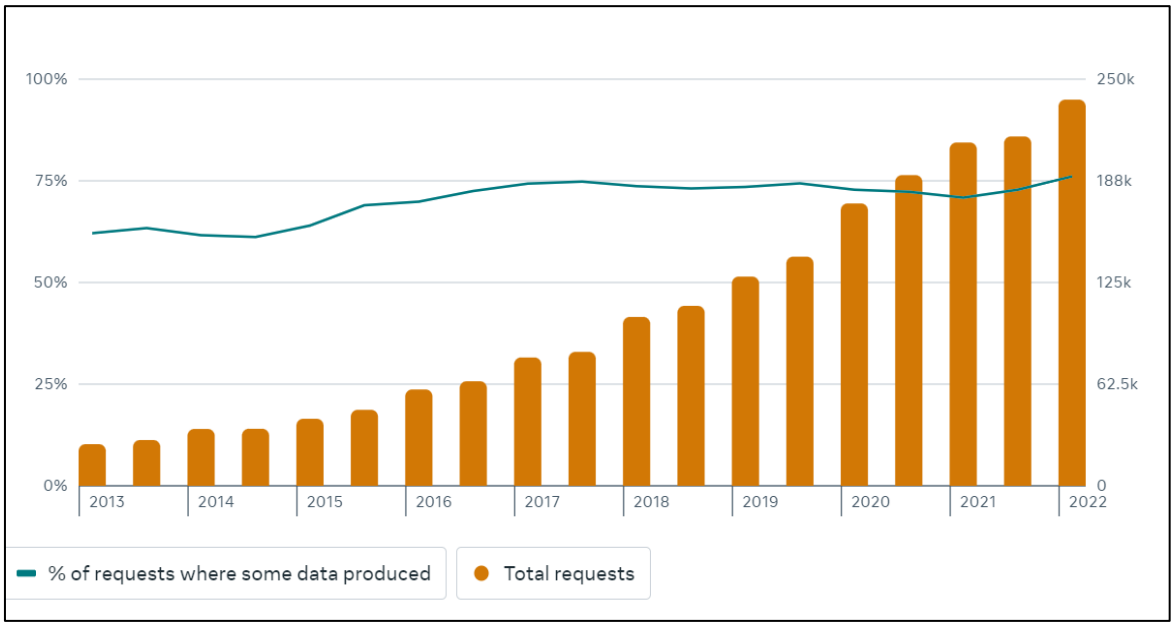


[497] *Richieste inviate in casi di emergenza ai provider da Stati UE nel 2022, distinte per compagnia*

[495] *SIRIUS EU Electronic Evidence Situation Report 2023,* cit., p. 67.
[496] *Ibidem.*
[497] *SIRIUS EU Electronic Evidence Situation Report 2023,* cit., p. 68.

Facebook è stato sostituito da *Meta*, azienda che ingloba attualmente tutta la compagine relativa a *Facebook, Instagram, Whatsapp* e *Messenger*.

Anche il *transparency report* di tale azienda ha evidenziato un *trend* in crescita, come si può rilevare dai grafici riportati:



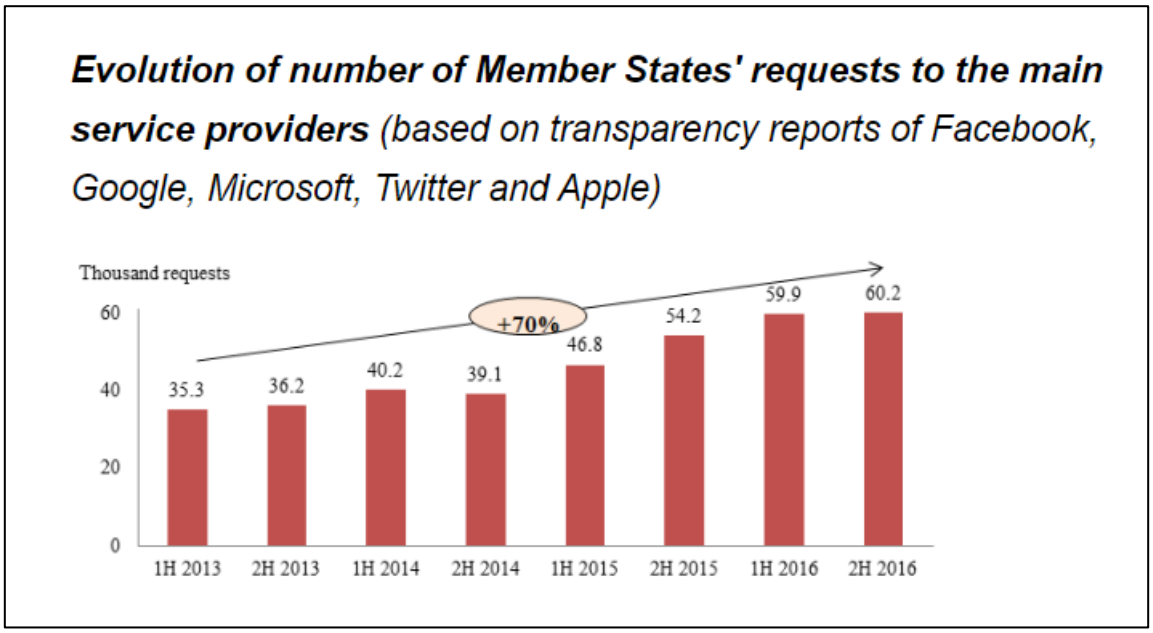
[498] *Richieste di consegna dei dati giunte a Meta dal 2013 al 2022 e indicazione della percentuale di richieste a cui è stata data risposta*

Alle menzionate aziende si sono poi aggiunte, nel 2021, *Snapchat* e *Tiktok*[499], quest'ultima con sede legale in Cina.

Di seguito, si riporta il *trend* in ordine alle richieste indirizzate ai principali *service provider*, dal 2013 al 2016, con dati che testimoniano la costante crescita del fenomeno.

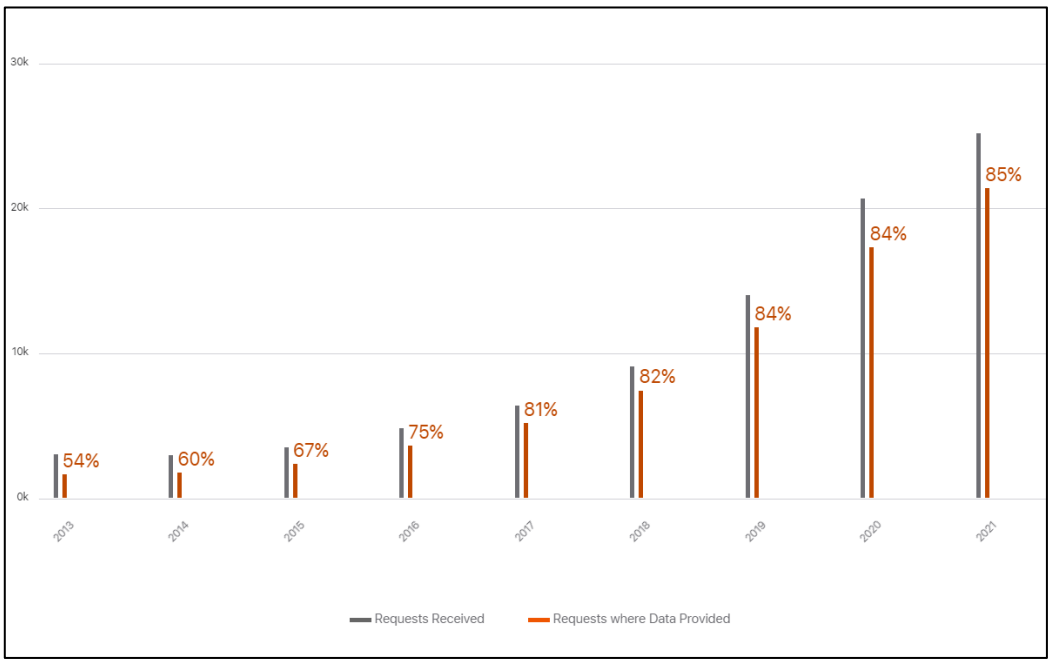
[498] META – *Transparency center, Government Requests for User Data – Global overview*, https://transparency.fb.com/data/government-data-requests/ .

[499] Per approfondimenti DE RUVO G., *Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso Tiktok come paradigma*, in *Riv. italiana di informatica e diritto*, 2022,1.



500 *Evoluzione del numero di richieste di Stati UE ai principali provider dal 2013 al 2016.*

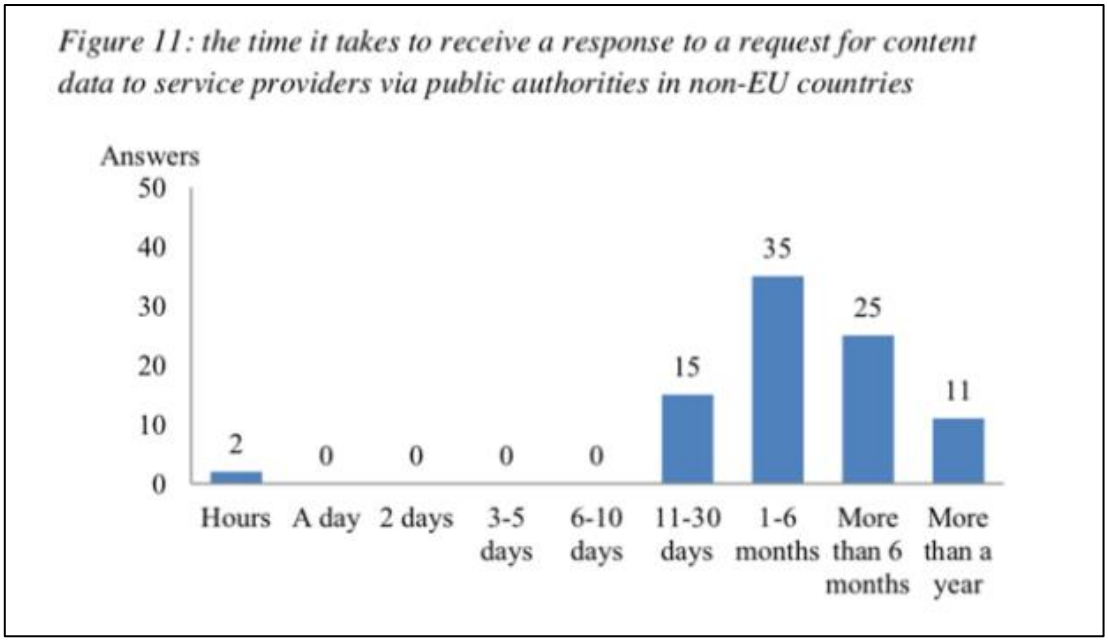
Una ulteriore conferma si può trarre dalle statistiche di *Apple*, relative al periodo 2013- 2021:



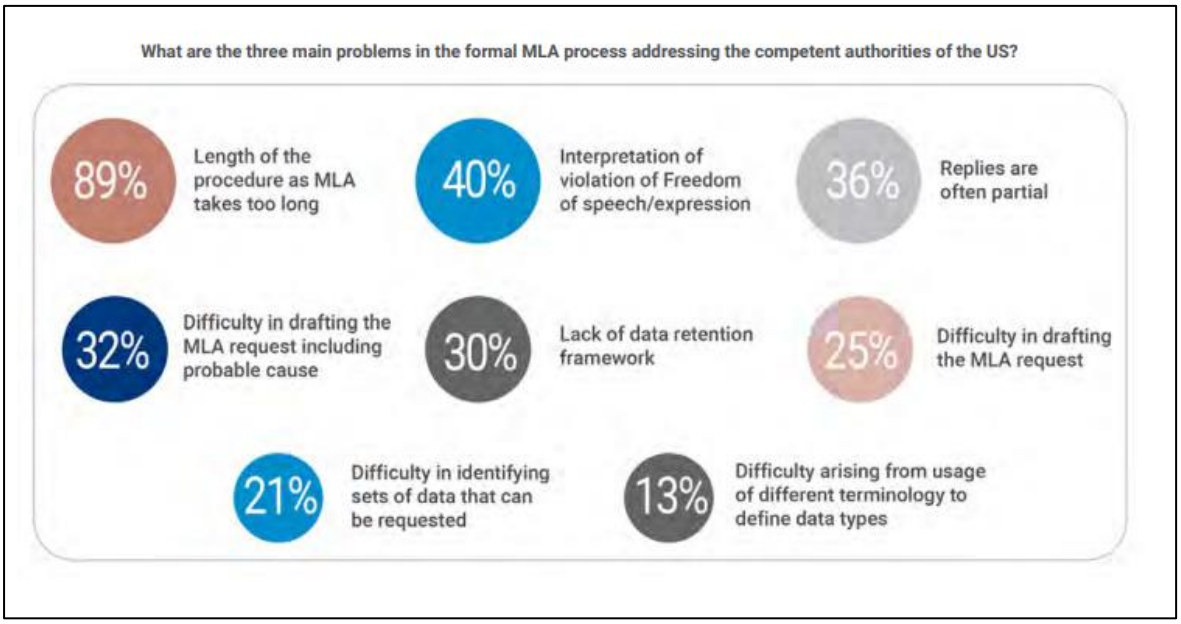
501 *Percentuali dei dati richiesti ad Apple dal 2013 al 2021 e delle risposte*

500 *Frequently asked questions: new EU rules to obtain electronic evidence*, 17 aprile 2018, https://ec.europa.eu/commission/presscorner/detail/el/MEMO_18_3345 .
501 *Apple Transparency Report,* https://www.apple.com/legal/transparency/ .

Sul fronte della collaborazione tra USA e UE, nel 2003 è stato concluso un accordo di *mutual legal assistance*, entrato in vigore nel 2010[502]. L'accordo quadro stabilisce le condizioni relative all'assistenza giudiziaria tra i due Stati, da integrare con le disposizioni degli accordi bilaterali tra USA e Stati UE.



[503]*Tempi di risposta per non -content data richiesti ai provider attraverso procedure di MLA*



[504]*Principali problemi nell'esperimento di procedure di MLA con gli USA*

[502] *Agreement on mutual legal assistance between the European Union and the United States of America*, 22003A0719(02), in G.U. L 181 del 19 luglio 2003. Vedasi *Review of the 2010 EU-U.S. Mutual Assistance Agreement*, 7 aprile 2016, 7403/16.
[503] GONZÁLEZ FUSTER G., VÁZQUEZ MAYMIR S., *Cross-border access to e-evidence: framing the evidence*, in *Liberty and Security in Europe,* 2020, 2, p. 9.
[504]*Ibidem*, p. 48.

Preme specificare che, tra le altre vie percorribili per ottenere dati, le autorità europee possono ricorrere alla cooperazione diretta o all'accesso diretto.

L'accesso diretto pone, tuttavia, dei dubbi sulla lesione della sovranità statale, in quanto permetterebbe di accedere ai *server* o ai dati conservati attraverso l'installazione di *spyware*.

La collaborazione diretta, invece, è eseguibile per lo più in relazione ai *non content data* sulla base delle *policy* e della volontà di ogni specifica compagnia.

Non è, tuttavia, previsto un obbligo di collaborazione con le autorità straniere e vi è, peraltro, un divieto di consegna dei dati di contenuto[505]. Questi ultimi, infatti, possono essere consegnati solo alle autorità statunitensi in risposta a un mandato (*warrant)*.

I casi *Yahoo* e *Microsoft* sono emblematici delle difficoltà incontrate da UE e USA in relazione all'acquisizione dei dati digitali.

La compagnia *Yahoo*[506], con sede legale negli Stati Uniti, veniva sollecitata dal pubblico ministero belga alla consegna di dati di traffico per stabilire l'identità di alcuni soggetti sospettati di frodi informatiche. L'azienda, tuttavia, si rifiutava di adempiere alla richiesta, ritenendo che, trattandosi di *traffic data*, non potesse applicarsi l'art. 18 della Convenzione di Budapest, destinato unicamente alla richiesta di *subscriber data*.

La Corte Suprema belga, ritenendo l'accesso ai dati legittimato dalla normativa interna, stabiliva che *Yahoo* – azienda qualificata come un *provider* di comunicazione elettronica, commercialmente attiva in Belgio e diretta ai consumatori dello stesso Stato –

---

[505] *Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, 5 febbraio 2019, COM (2019) 70 *final*, https://commission.europa.eu/system/files/2019-02/recommendation_council_decision_eu_us_e-evidence.pdf : «*In terms of content data, as outlined above, U.S. law (Stored Communications Act of 1986) as it currently stands, bars U.S. service providers from responding to requests from foreign law enforcement authorities. U.S. law currently requires that probable cause be shown before a Mutual Legal Assistance request from a third country can be executed. European Union Member State service providers cannot currently respond to direct requests from third country authorities. An EU-U.S. Agreement would complement the objective and the effectiveness of the e-evidence proposals, in particular when it comes to content data held by U.S. service providers in the United States of America. It would allow direct cooperation with a service provider by creating a more efficient legal framework for judicial authorities as EU practitioners currently face difficulties in obtaining content data through Mutual Legal Assistance requests. As regards non-content data, due to the growing number of Mutual Legal Assistance requests addressed to the United States of America, the U.S. authorities have encouraged EU law enforcement and judicial authorities to request non-content data from U.S. service providers directly, and U.S. law allows but does not require U.S.-based service providers to respond to such requests. An EU-U.S. Agreement would provide more certainty, clear procedural safeguards and reduce fragmentation for EU authorities to access non-content data held by U.S. service providers. It would also allow for reciprocal access by U.S. authorities to data held by EU service providers*».

[506] *Hof van Cassatie van België* (Corte di cassazione belga), 1° dicembre 2015, P.13.2082.N, in www.juricaf.org.

avrebbe dovuto rispondere alla richiesta per non incorrere in un reato ai sensi dell'art. 46-*bis* del *Code d'instruction criminelle* [507].

Escludeva peraltro, che la richiesta dei dati e l'eventuale applicazione di una sanzione, configurassero un esercizio di giurisdizione extraterritoriale, non essendosi concretizzate nello svolgimento di atti di indagine in territorio straniero.

Una questione analoga è stata al centro della vicenda *Microsoft* negli Stati Uniti d'America. Il caso riguardava un mandato (*warrant*), emesso conformemente al § 2703 dello *US Stored Communications Act* del 1986 (SCA) [508], con il quale si ingiungeva a *Microsoft* di consegnare alcuni dati alle autorità statunitensi; nello specifico, il contenuto di tutte le *email* archiviate in un *account*, i metadati e i dati di traffico associati[509]. *Microsoft*, in esecuzione del mandato, effettuava la *disclosure* relativamente ai metadati e ai dati sulle comunicazioni connessi *all'account*, ma respingeva l'ordine in merito alla consegna dei *content data* e dei rimanenti dati sulle comunicazioni, archiviati in un *server* localizzato in Irlanda. Nel procedimento davanti alla Corte d'Appello, l'azienda eccepiva che il mandato non era idoneo ad ottenere dati conservati al di fuori del territorio statunitense, poiché l'ambito di applicazione dello SCA doveva ritenersi limitato ai confini nazionali. L'esecuzione del *warrant,* peraltro, veniva considera alla stregua di una violazione della sovranità dell'Irlanda, in assenza dell'utilizzo di procedure di MLA e, conseguentemente, la Corte riteneva che il mandato fosse illegittimo.

La questione, successivamente, giungeva davanti alla Corte Suprema che, tuttavia, non riusciva a pronunciarsi, poiché nel frattempo il legislatore aveva emanato il *CLOUD*

---

[507] «*En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients des acteurs visés à l'alinéa 2, premier et deuxième tirets, à:*

1. l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé;

2. l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration:

- *de l'opérateur d'un réseau de communications électroniques, et*
- *toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques. […]*

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie [4 d'une amende de cent euros à trente mille euros».

[508] Emanato il 21 ottobre 1986 come parte dell'*Electronic Communications Privacy Act* del 1986, nello specifico al Titolo II.

[509] *18 U.S. Code § 2703 - Required disclosure of customer communications or records*. Ai sensi di tale articolo, attraverso un apposito *warrant*, l'autorità giudiziaria statunitense può chiedere la *disclosure* di contenuti di comunicazioni o di registrazioni in possesso del *provider*.

Act[510]. L'atto in questione, attraverso una modifica allo SCA, ha offerto la base giuridica per un'applicazione extraterritoriale della normativa in modo che i *service provider* conservino e consegnino i contenuti di comunicazioni telefoniche o elettroniche e ogni registrazione o informazione relativa ai consumatori o utenti, in loro possesso, controllo o custodia, indipendentemente dalla loro localizzazione all'interno o all'esterno degli USA[511].

Il *CLOUD Act* ha offerto la possibilità di stipulare accordi con "*foreign governments*", basati sul principio di reciprocità, che permettano alle autorità di richiedere direttamente i dati al *provider* con sede nello Stato con il quale è stato concluso l'accordo e viceversa.

L'extraterritorialità riconosciuta allo SCA, se ha permesso di risolvere alcune problematiche legate all'acquisizione dei dati, non ha però mancato di sollevare ulteriori problemi sul campo delle relazioni internazionali. In particolare, è stato evidenziato un contrasto con l'art. 48[512] del Regolamento 2016/679/UE (GDPR). Questa disposizione è stata introdotta per le ipotesi di ordini di produzione emanati da Stati terzi, non appartenenti all'UE, e prevede che sentenze e decisioni di autorità non UE che dispongano il trasferimento di dati personali, possano essere riconosciute o eseguite solo se legittimate da un accordo internazionale tra gli Stati o un accordo di MLA. In tal senso, tale articolo osterebbe alla richiesta di dati fatta da un'autorità statunitense, salvo l'attivazione delle procedure di MLA. Sono, tuttavia, previste delle deroghe all'interno del GDPR: la presenza di una decisione di adeguatezza o di garanzie idonee, il trasferimento sulla base di norme vincolanti d'impresa, o specifiche condizioni *ex* art. 49 GDPR[513]. Ai sensi di tale articolo, l'unica deroga all'art.

---

[510] *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, 23 marzo 2018. È parte del *Consolidated Appropriations Act*, 2018, Pub. L. 115-141, https://www.congress. gov/115/plaws/publ141/PLAW-115publ141.pdf.

[511] ALLEN S., *Enforcing criminal jurisdiction in the clouds and international law's enduring commitment to territoriality*, cit..

[512] Art. 48: «***Trasferimento o comunicazione non autorizzati dal diritto dell'Unione.***
Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un Paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il Paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo».

[513] Art. 45 co. 1: «***Trasferimento sulla base di una decisione di adeguatezza.***
Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche».

Art. 46: «***Trasferimento soggetto a garanzie adeguate.***
In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi».
Art. 47 co. 3: «***Norme vincolanti d'impresa.***

48 GDPR è ammessa quando il trasferimento sia necessario per fondamentali ragioni di interesse pubblico, che devono essere riconosciute nel diritto dell'Unione o dello Stato membro in cui si trova il titolare dei dati.

In tal caso, l'interesse a reprimere un crimine non è di per se sufficiente, a meno che si tratti di delitti gravi a carattere transnazionale, come identificati dall'art. 83 TFUE[514].

Va, tuttavia, evidenziato che un *provider* al quale venga indirizzata una richiesta dall'autorità statunitense, difficilmente potrà stabilire in maniera adeguata quale sia la disciplina applicabile e se, per esempio, rientri in uno dei casi di deroga motivata da fondamentali ragioni di interesse pubblico. Pertanto, considerando le deroghe come ipotesi residuali e non immediatamente identificabili dai *provider*, si potrebbe ritenere che il GDPR operi a tutti gli effetti come un *blocking statute*. Allo stesso modo, un ordine di produzione emanato da uno Stato membro dell'Unione per l'acquisizione di *content data*, sarebbe ostacolato dalle previsioni dello SCA.

Il *CLOUD Act*[515], tuttavia, prevede la possibilità di consegnare legittimamente *content data* ai "*foreign governments*" con cui il Governo, sulla base della valutazione dell'*Attorney General*, abbia concluso degli accordi.

La Commissione può specificare il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa ai sensi del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.».

Art. 49, co. 1: «***Deroghe in specifiche situazioni***.

In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;

b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;

d) il trasferimento sia necessario per importanti motivi di interesse pubblico;

e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri».

[514] Terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata.

[515] Per approfondimenti BILGIC S., *Something old, Something new and something moot: the privacy crisis under the cloud act*, in *Harvard Journal of Law & Technology*, 2018, 31, 1; DI PAOLO G., *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, CEDAM, 2008.

Nello specifico, la condizione necessaria è che l'*Attorney General* ritenga che lo Stato in questione offra adeguate tutele sostanziali e procedurali in tema di tutela delle libertà civili e che vegli sul rispetto dei diritti umani[516].

Un simile accordo tra UE e USA sarebbe idoneo a superare il blocco previsto sia dal GDPR sia dallo SCA, così permettendo un efficace scambio dei dati[517].

È però dubbio se l'Unione europea rientri nella definizione di *foreign governments*.

Se, da un lato, l'Unione preferirebbe concludere un accordo generale per tutti gli Stati membri[518] , dall'altro, gli Stati Uniti tendono a stipulare accordi di natura bilaterale che permettano di valutare di volta in volta il rispetto dei diritti in relazione a ciascuno Stato.

Una soluzione potrebbe essere quella di stipulare un accordo quadro che possa poi essere adottato da ogni Stato membro[519]. A tal fine, la Commissione ha ricevuto mandato

---

[516] Sulla discrezionalità del *General Attorney* v. MAILLART J. B., *The limits of subjective territorial jurisdiction in the context of cybercrime,* in *ERA Forum*, 2018, 18, p. 387: « *Aside from side-lining Congress, the CLOUD Act also bestows virtually unchecked powers to the Attorney General since it merely lists "factors to be considered" rather than imposing mandatory standards. Though § 2523(b)(1)(B) lists several factors that the Attorney General must consider before such certification, the non-binding nature of these factors led many commentators to state that the Executive can enter into an agreement with any Country — even those without high human rights standards. For instance, the Attorney General must consider the "domestic law of the foreign government" and whether it "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection." However, since the CLOUD Act neither adopts U.S. legal standards nor refers to international human rights treaties, the meaning of the words "robust," "protection," and "privacy" is left entirely to the discretion of the Attorney General. Moreover, a determination or certification by the Attorney General is not subject to judicial or administrative review. As the dearth of checks on the Attorney General shows, this bilateral agreement scheme puts overly broad discretion in the hands of the executive branch».*

[517] Tuttavia, la dottrina mette in luce alcuni dei principali problemi che potrebbero scaturire dall'approvazione del CLOUD Act. MAILLART J. B., *The limits of subjective territorial jurisdiction in the context of cybercrime*, cit., p. 387: «*Overall, the new scheme created by the CLOUD Act raises three major privacy concerns. First, it gives unlimited access to qualifying foreign governments. Second, by excluding non-qualifying foreign governments while allowing the U.S. to access data everywhere, it creates an unwelcoming U.S. exceptionalism to foreign governments, which will likely lead to an increase in other countries' efforts to enact data localization laws — that is, mandating that data is stored on servers physically located within the country where the data was created. As I will explain in Section IV.C, these laws will also threaten the digital privacy of foreign citizens. Third, by giving global access to the U.S. government, the Act frustrates efforts by other countries to protect their citizens' data from surveillance by the U.S. Thus, the CLOUD Act is not the resolution of the Microsoft Ireland case, but only the beginning of a future privacy crisis, especially for foreign citizens*».

[518] Questo, infatti eviterebbe una frammentazione legislativa e assicurerebbe il medesimo trattamento per tutti i cittadini dell'UE.

[519] SHURSON J., *Data protection and law enforcement accesso to digital evidence: resolving the reciprocal conflicts between EU and US law*, in *International Journal of Law and Information Technology*, 2020, vol. 28, 2, p. 182: «*If the EU does not wish to proceed under the Cloud Act framework, the remaining options would take more time and require more legislative process on the US side. Either a new treaty, a new executive agreement or a new law (likely an amendment to the Cloud Act) would have to be passed by the Senate and House of Representatives and signed by the President. Or in the case of a Presidential veto, each option would require a two-thirds vote in both the Senate and House. Given the difficulties associated with these options, the most efficient and expeditious solution to the cross-border digital evidence problem is clearly a Cloud Act agreement*». V. anche DASKAL J., *Unpacking the CLOUD Act*, in www.eucrim.eu, 2019., ABRAHA H.H., *Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiative*, in *International Journal of Law and Information Technology,* 2021, vol. 29, n. 2.

per la conclusione di un accordo con gli Stati Uniti per ottenere le prove digitali nell'ambito dei procedimenti penali[520].

L'accordo con gli USA genererebbe i seguenti benefici:

- un reciproco accesso ai dati di contenuto;
- accesso ai *non-content* data sulla base di ordini della autorità giudiziarie, disciplinando le condizioni e le tutele per la cooperazione diretta con i *provider*;
- accesso rapido ai dati per le autorità giudiziarie;
- maggior certezza per la risoluzione dei conflitti di legge;
- riduzione della frammentazione di regole e procedure;
- armonizzazione dei diritti e delle garanzie;
- maggiore chiarezza sulla natura vincolante degli ordini e l'esecuzione[521].

La Commissione ha precisato che l'accordo deve essere condizionato al rispetto dei diritti umani[522] e all'esistenza di solidi meccanismi di protezione e finalizzato a migliorare la certezza giuridica per autorità, *provider* e soggetti coinvolti, assicurando il rispetto dei principi di proporzionalità, trasparenza e di responsabilità.

---

[520] *European Commission, Recommendation for a Council decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime* (CETS n. 185), 5 febbraio 2019, COM (2019) 71 final, https://commission.europa.eu/system/files/2019-02/recommendation_budapest_convention.pdf. E anche *Annex to the Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime* (CETS n. 185), 5 febbraio 2019, COM (2019) 71 final, https://commission.europa.eu/system/files/2019-02/annex_recommendation_budapest_convention.pdf; *Questions and Answers: Mandate for the EU-U.S. cooperation on electronic evidence*, https://ec.europa.eu/commission/presscorner/detail/en/memo_19_863 . Per approfondimenti CHRISTAKIS T., TERPAN F., *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in International data privacy law, 2021, 11, 2.; PROPP K., *Contextualizing an EU-US E-evidence accord relationships to existing law enforcement agreements*, in *Cross-border data forum*, 22 gennaio 2021; WAHL T., E-*evidence: Commission obtains mandates for EU-US agreement and negotiations in Council of Europe*, *in www.eucrim.eu*, 10 settembre 2019; *European Data Protection Board – European Data Protection Supervisor, Joint response to the US CLOUD Act, https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_joint_response_us_cloudact_coverletter.pdf ; Annex I https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf . Commissione europea, Criminal justice: Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence, STATEMENT/19/5890, https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vl28owweesx0?ctx=vga3buzdwirl&v=1&start_tab0=20.*

[521] *Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, cit., p.5.

[522] «*The agreement should respect the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and Charter of Fundamental Rights, procedural rights including right to an effective remedy and to a fair trial, presumption of innocence and right of defence, principles of legality and proportionality of criminal offences and penalties and any obligations incumbent on law enforcement or judicial authorities in this respect. As regards the necessary data protection safeguards for personal data transferred from the European Union to U.S. law enforcement authorities, the applicable provisions of the EUU.S. Data Protection and Privacy Agreement will be complemented by additional safeguards to take into account the level of sensitivity of the categories of data concerned and the unique requirements of the transfer of electronic evidence directly by service providers*».

I principali diritti coinvolti sono:

- quelli dei soggetti titolari dei dati,
  - diritto alla protezione dei dati personali,
  - diritto al rispetto della vita privata e familiare, del domicilio e delle comunicazioni;
  - libertà di espressione;
  - diritto a un rimedio effettivo e ad un equo processo;
  - presunzione di innocenza e diritto di difesa;
  - principio di legalità e proporzionalità dei delitti e delle sanzioni;

- quelli dei *provider*,
  - libertà economica,
  - diritto ad un rimedio effettivo;

- il diritto alla libertà e sicurezza degli individui[523].

L'accordo dovrà, inoltre, essere compatibile con gli strumenti adottati dall'UE e con il Regolamento che introduce l'EPO e l'EPO-PR. Proprio per questa ragione, l'UE ha preferito concludere il procedimento legislativo, prima di avanzare ulteriormente con i negoziati.

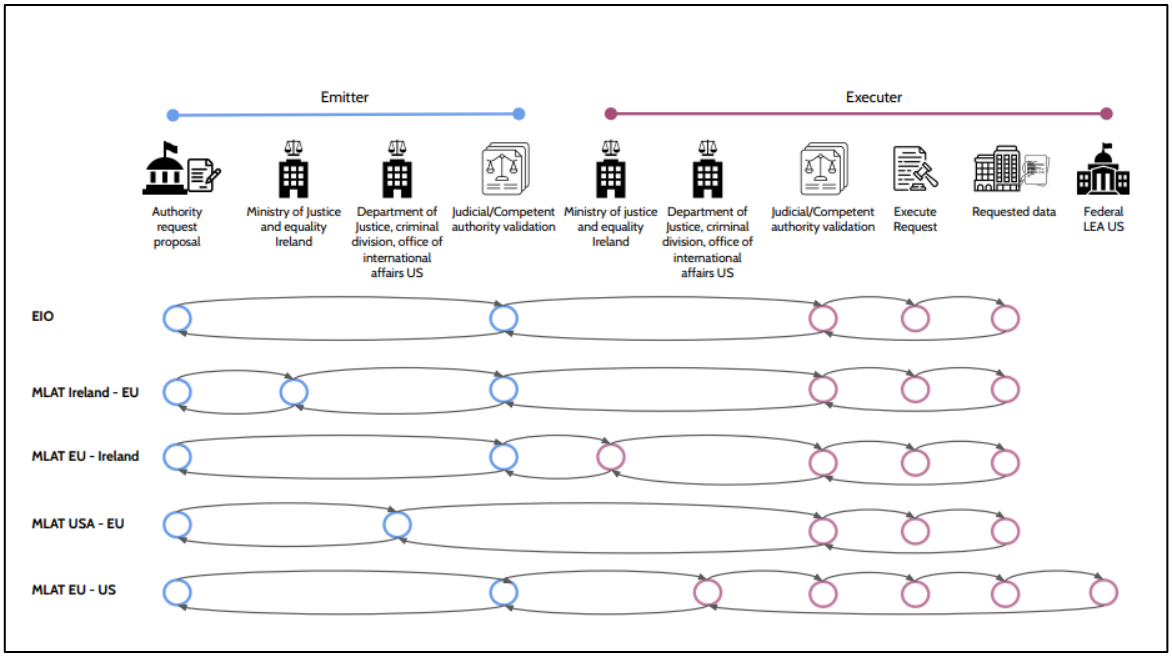
Punti cruciali dell'accordo saranno le definizioni e le tipologie di dati; i delitti per i quali possono essere richiesti e le soglie sanzionatorie; le condizioni di emissione di un ordine ai *provider*; le possibilità di rifiuto e i rimedi esperibili.

I negoziati, ufficialmente iniziati a settembre 2019, sono ripresi a marzo 2023, dopo un periodo di stasi[524].

Si riportano di seguito le infografiche relative al funzionamento dell'OEI e delle procedure di MLA tra UE e US.

[523] *Ibidem.* V. anche *Annex to to the Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the Europea Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matter,* https://commission.europa.eu/system/files/2019-02/annex_eu-us_evidence.pdf .

[524] https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en .



525 *Infografica sul funzionamento e sui soggetti coinvolti in caso di emissione di un OEI e delle procedure di MLA tra gli Stati membri, l'Irlanda e gli Stati Uniti*

Di seguito un grafico relativo al funzionamento di MLA con gli USA:

526

4.3. Il principio di territorialità: un principio anacronistico?

525 CASINO F., PINA C., LOPEZ AGUILAR P., BATISTA E., SOLANAS A., PATSAKIS C., *SoK: cross-border criminal investigations and digital evidence,* in *Journal of Cybersecurity*, 2022, p. 5.
526 *Frequently Asked Questions: New EU rules to obtain electronic evidence*, cit.

Gli strumenti che l'Unione europea ha adottato, in uno al CLOUD Act e al secondo Protocollo della Convenzione di Budapest, hanno segnato il tramonto del principio di territorialità[527], peraltro, non sempre di agevole identificazione neppure all'interno dei confini statuali[528].

L'art. 22 co. 1 della Convenzione di Budapest stabilisce, infatti, che: «Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per stabilire la propria competenza per tutti i reati previsti in conformità agli artt. da 2 a 11 della presente Convenzione, quando i reati siano commessi:

a. nel proprio territorio;
b. a bordo di una nave battente bandiera della Parte;
c. a bordo di un aeromobile immatricolato presso quella Parte;
d. da un proprio cittadino, se l'infrazione è penalmente punibile là dove è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato».

Nella realtà attuale, questa connessione ad un luogo fisico si scontra inevitabilmente con la natura dei reati informatici e delle prove digitali. Come detto, infatti, la transnazionalità della prova digitale non permette di definire i confini fisici e di delimitarli all'interno di precise coordinate geografiche. Pertanto, nell'epoca del *cloud computing*, risulta difficile vincolare i "cyber-elementi" a luoghi specifici, e tale circostanza non può che riflettersi sulla giurisdizione.

Questa è tradizionalmente ancorata all'esercizio del potere statale all'interno dei confini e al fatto che un crimine sia stato commesso nel territorio nazionale (principio di territorialità soggettiva) o ivi abbia prodotto i suoi effetti (principio di territorialità oggettiva), o ancora l'attore del delitto vi risieda o in quel luogo sia stato ritrovato.

La *ratio* è data dalla maggiore facilità di reperire gli elementi di prova nel *locus commissi delicti*. Se pensiamo al mondo digitale, tuttavia, il principio di territorialità soggettiva entra in crisi a causa della difficoltà di individuare esattamente il luogo di azione dei criminali.

La *scena criminis* è, nel caso dei *cybercrime*, intangibile.

---

[527] *European Data Protection Board, Opinion of the EDPB on Commission proposal of the EP and for the Council on European Production and preservation orders for electronic evidence in criminal matter*, 18 ottobre 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13317_2018_INIT, p. 6: «*disappearance of the location criteria*».

[528] Per un approfondimento su *cybercrime* e giurisdizione, v. ARNELL P., FATUROTI B., *The prosecution of cybercrime – why trasnantional and extraterritorial jurisdiction should be resiste*d, in *International review of law, computers and technology*, 8 giugno 2022.

In più, i criminali non operano attraverso il loro reale indirizzo IP, ma utilizzano dei *proxy* che permettono di nasconderlo o altre tecniche che rendono manifesto un indirizzo IP fittizio[529].

Nella situazione attuale, caratterizzata da "*loss of data*" e "*loss of location*", risulta arduo determinare quale Stato debba esercitare la propria giurisdizione e, di conseguenza, identificare la disciplina in tema di acquisizione probatoria[530].

Parte della dottrina[531] ritiene che «accogliere la sfida tecnologica ad oggi significa avere il coraggio di raggiungere uno *step* successivo rispetto a quelli tradizionali dell'accordo internazionale e dell'armonizzazione».

In sostanza, occorrerebbe distinguere tra *enforcement jurisdiction*, relativa all'applicazione delle leggi da parte delle autorità, e *investigative jurisdiction*, relativa alla conduzione delle indagini.

Se, da un lato, si ritiene comprensibile che la *enforcement jurisdiction* vada legittimamente limitata al territorio nazionale, d'altro canto, l'attività investigativa dovrebbe operare senza essere ostacolata dai limiti territoriali e nazionali, estendendosi a tutti i luoghi ove sia possibile trovare dati necessari all'indagine, sempre nel rispetto dei diritti fondamentali[532].

---

[529] MAILLART J. B., *The limits of subjective territorial jurisdiction in the context of cybercrime*, cit., p. 381: «*there are many 'open proxies' on the Internet which can be accessed by anyone. This technique, called 'IP spoofing', is relatively easy to implement. Another technique is the use of proxy servers, public or private, which enables cybercrime offenders to establish a connection to a network via an intermediary server and thereby conceal their online activity. That said, the most commonly used and efficient method to hide the geographical origin of an offence committed in cyberspace is still to take control over a remote computer system in a foreign country and then use that computer as a staging ground from which to perpetrate the offence. This computer system, which is said to be 'zombified', is often the last link in a very long chain involving numerous computer systems and jurisdictions.*».

[530] *EUROJUST, Overview Report- Challenges and best practices from Eurojust's casework in the area of cybercrime, November 2020, p. 5.* LEONHARDT dos SANTOS D., *Territoriality in the context of global crime: Reflections of the impact of cyberspace on jurisdictional delimitation*, in *Rev. Brasileira de Direito Processual Penal,* 2019, 5, 2, p- 597; LUBIN A. *The prohibition on extraterritorial enforcement jurisdiction in the datasphere*, in PARRISH A, RYNGAERT C. (a cura di), *Research handbook on extraterritoriality in international law,* Elgar Publishing, 2022, p 339; ORTIZ PRADILLO J.C., *Problemas procesales de la ciberdelincuencia*, Colex, 2014, p. 19.

[531] CONTI C., TORRE M., *Spionaggio digitale nell'ambito dei social network*, in SCALFATI A. (a cura di), *Le indagini atipiche,* Giappichelli, 2019, p. 558.

[532] In proposito anche MIFSUD BONNICI J., TUDORICA M., CANNATACI J., *The european legal framework on electronic evidence: complex and in a need of reform*, in BIASIOTTI M.A., MIFSUF BONNICI J., CANNATACI J., TURCHI F., (a cura di), *Handling and exchanging electronic evidence across Europe*, cit., p.204: «*While from a law enforcement access to cross-border data this development of 'investigative jurisdiction' may make sense in some cases, in others the current problems may still not be overcome. One scenario where the notion of 'investigative jurisdiction' may work is when a law enforcement agent is following a trail in real time: the investigation should not stop because the suspect or suspected information shifts servers and is on a server outside the territorial reach of the law enforcement agent. Having an 'investigative jurisdiction' would allow the agent to follow the trail irrespective of territorial concerns. One scenario where this notion of 'investigative jurisdiction' may be less useful is when requiring information directly from a private actor: which rules would the private actor be expected to follow (of location or of the investigating party) is not immediately clear and would still be dependent on some form of legal agreement. Furthermore, as Svantsson notes "it should*

Vi è poi chi[533] ipotizza una rivoluzione copernicana che porti all'abbandono del principio di territorialità. E infatti, si ritiene che il CLOUD Act e il nuovo Regolamento UE muovano comunque da questa idea, ma la relativizzino permettendo ugualmente l'accesso ai dati in virtù della legge o di accordi. In tal senso, si ipotizza uno spostamento dal principio di territorialità a quello di pertinenza, utilizzato in ambito comunitario nel GDPR[534] e, inoltre, dai giudici belgi nella sentenza *Yahoo*. Pertanto, non dovrebbe più essere dato rilievo alla localizzazione del dato, mutevole o spesso ignota, ma alla connessione con un caso o dei soggetti.

Questa potrebbe essere solo una delle possibili strade[535], ma resta fuor di dubbio che non si possa più far riferimento al principio di territorialità, mentre tutto attorno lo scenario è cambiato e continua ad evolversi. Peraltro, non si può che evidenziare la difficoltà di tale operazione, posto che ridefinire e cristallizzare nuove categorie genererebbe in futuro le stesse problematiche, in ragione della continua evoluzione delle tecnologie e della società.

La risposta ai dubbi manifestati non potrà che intervenire progressivamente.

---

be acknowledged that some (coercive) investigate measures may fall within a grey zone between investigative jurisdiction and enforcement jurisdiction. This is an area requiring further work».

[533] V. SOANA G., *L'accesso transfrontaliero alla prova informatica. Oltre il principio di territorialità*, in *Riv. Semestrale di diritto*, 2020, 2.

[534] *Ibidem,* p. 271: «Il regolamento sposta, quindi, il fulcro dell'indagine in merito alla territorialità dall'oggetto all'azione. In tal senso rientrano nell'ambito di applicazione del regolamento non i dati che si trovino nel territorio dell'Unione, bensì quelli che riguardino l'Unione. In tal senso, si potrebbe parlare di uno spostamento del fuoco dall'ubicazione territoriale alla pertinenza del dato rispetto all'ente sovrano. Lo Stato ha interesse a controllare solo quei dati che sono ad esso pertinenti».

[535] Sulle sfide legate alla raccolta dei dati ed alla territorialità DE LA CHAPELLE B., FEHLINGER P., *Jurisdiction on the Internet: from legal arms race to transnational cooperation,* in FROSIO G. (a cura di) *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, 2020 : «*two major challenges: how to preserve the global nature of cyberspace, with its cross-border data flows and services, while respecting national laws; and how to fight misuses and abuses of the internet while ensuring the protection of human rights. Both challenges require cooperation, as well as policy standards and clear procedures across borders, to ensure efficiency and due process. At least four territorial factors can play a role in determining applicable law: the location(s) of internet end-user(s) or connected devices; the location(s) of the servers or devices that store or process the actual data; the locus of incorporation of the internet companies that run the service(s) in question; and, in the case of the world wide web, the registrars or registries through which a domain name was registered. These overlapping and often conflicting territorial criteria make both the application of national laws in cyberspace and the resolution of internet-related disputes difficult and inefficient. The principles of separation of sovereignties and non-interference between states that underpin the international system not only render court decisions difficult to enforce but also prevent the cooperation across borders necessary to efficiently deal with crimes and abuses online. Maintaining a global internet by default, which fulfils the ambitions of the Universal Declaration of Human Rights, notably Article 19, and boosts innovation and growth through cross-border data flows and cloud-based services, requires transnational legal cooperation*».

Riflessioni conclusive

L'analisi sin qui condotta sulla prova digitale e la sua acquisizione al processo penale ci restituisce un quadro normativo in continua evoluzione, a livello soprattutto sovranazionale e internazionale. Lo dimostrano i più recenti strumenti adottati con l'intenzione di velocizzare e rinnovare le procedure di cooperazione giudiziaria, per una più efficace persecuzione dei reati.

Diversamente, a livello nazionale – se si guarda soprattutto all'esperienza italiana – si assiste a una sorta di "immobilismo" da parte del nostro legislatore. Infatti, se si eccettua il "microintervento" a opera della l. n. 48/2008 – con il quale si è data attuazione alla Convenzione sul *cybercrime* – di fatto si è conferita una sorta di delega in bianco ai giudici per adeguare gli strumenti processuali tradizionali (ispezioni, perquisizioni, sequestri, intercettazioni, ecc.) alle nuove sfide del crimine "informatico". Tanto che, in alcune occasioni, la giurisprudenza ha sostituito il legislatore, mossa dalla necessità di colmare le lacune normative dell'ordinamento.

Sulla stessa lunghezza d'onda si pone il sistema spagnolo, oggetto di specifica analisi. I due ordinamenti – italiano e spagnolo – sono accomunati dalla mancanza di una definizione di prova digitale: questa carenza porta, in alcune ipotesi, all'applicazione di istituti tradizionali che poco si adattano alle caratteristiche – immaterialità, volatilità, facile alterabilità e ubiquità – tipiche della prova digitale.

L'ultimo intervento riformatore del legislatore spagnolo si deve alla *Ley Orgànica* 13/2015 che, nell'innovare il codice di rito, ha opportunamente dedicato una specifica disciplina al tema delle prove tecnologiche. Tuttavia, la riforma ha lasciato irrisolte numerose questioni e, tra queste: il catalogo di delitti che può legittimare il ricorso alle indagini tecnologiche, la discrezionalità del giudice nell'acquisizione di dati connessi alle intercettazioni e l'applicabilità della disciplina delle intercettazioni all'acquisizione dei dati di traffico. Ciò ha richiesto l'adozione di alcune circolari da parte della *Fiscalìa General* con le quali si è precisato come debba applicarsi la disciplina delle intercettazioni per l'acquisizione dei dati connessi alle comunicazioni, raccolti contestualmente alla captazione; rendendo così fondamentali l'autorizzazione del giudice e la specifica motivazione sulla necessità di tali dati. Viceversa, nel caso di dati non connessi alla comunicazione, la *Fiscalìa General* ha ritenuto non applicabile la disciplina delle intercettazioni, tanto nella parte relativa all'autorizzazione del giudice, quanto per la limitazione a un espresso catalogo di

reati. Infine, ha colmato le lacune normative delineando, più precisamente, i profili relativi al conseguimento di indirizzi IP e codici IMSI e IMEI.

Nel silenzio del legislatore, il *Tribunal Supremo* spagnolo ha, inoltre, sancito l'esistenza di un "*derecho al propio entorno virtual"*[536], ricomprendendovi tutte le informazioni in formato elettronico che, attraverso le nuove tecnologie, vengono prodotte dall'utilizzatore fino a lasciare un'impronta indelebile. L'ampliamento dello spazio dell'intimità ha provocato un'evoluzione del diritto in questione, inteso non già come mero diritto a essere lasciato solo, vincolato a spazi fisici e corporei, ma come diritto a esercitare un controllo sulle informazioni e sui dati di un determinato soggetto, con il potere di stabilire quali informazioni rendere pubbliche: una sorta di "*habeas data*".

Sul piano sovranazionale, non può che guardarsi con favore al Secondo Protocollo della Convenzione di Budapest e ai negoziati avviati con gli Stati Uniti, attraverso i quali si potrà mettere un freno alle iniziative statuali individuali. Infatti, si ritiene che l'utilizzo di strumenti unilaterali, quali l'ordine europeo di produzione e lo SCA *warrant*, come modificato dal CLOUD Act, vada accompagnato da accordi bilaterali e multilaterali, idonei a superare gli ostacoli dei *blocking statutes* e a garantire che vi sia una visione comune che alimenti la *mutual trust*, per legittimare eventuali restrizioni della sovranità statale.

Sul fronte dell'Unione europea, va accolta positivamente l'approvazione del nuovo pacchetto *e-evidence* che, all'esito di un complesso negoziato, regola il nuovo strumento dell'ordine europeo di produzione dei dati elettronici indirizzato ai *service provider*, seppure non manchino alcune criticità che spetterà ai singoli Stati sciogliere in sede di "implementazione" della disciplina.

Sia il Secondo Protocollo sia il Regolamento UE sull'ordine di produzione, permetteranno di acquisire i dati in possesso dei *provider*, localizzati in un altro Stato o "nel *cloud*", superando le tecniche adottate dalle singole autorità e che si sostanziano nell'utilizzo di *spyware* e *trojan*. Queste attività sono, infatti, da considerarsi lesive della sovranità statale e, oltretutto, come illustrato nel caso italiano, non sono state ancora compiutamente disciplinate in tutte le loro potenzialità, ancorché siano particolarmente invasive.

La definizione, nel Regolamento sull'ordine di produzione, della prova elettronica e delle diverse tipologie di dati, contribuisce a fare chiarezza, ma persistono delle ombre in

536 *Tribunal Súpremo,, Sala de lo Penal,* 13 aprile 2013, n. 342/2013: «*En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital».* Vedasi anche Tribunal Supremo, 19 maggio 2016 n. 426.

relazione ai dati di traffico e, in particolar modo, agli indirizzi IP, il cui tracciamento permette di definire un quadro chiaro della personalità degli utenti. Per ridurre l'intrusività nella sfera personale degli individui causata dall'accesso ai dati di traffico, la proposta originaria dell'EPO è stata emendata, equiparando la disciplina dei *subscriber data* e dei dati di traffico richiesti ai soli fini dell'identificazione di un soggetto. Tale scelta deriva, da un lato, dalle pronunce della Corte di Giustizia che richiedono tutele rafforzate per i dati di traffico e, dall'altro, dal riconoscimento dell'importanza di tali dati nelle prime battute delle indagini. E infatti, muovendo dalla consapevolezza che i dati di traffico e sugli utenti sono quelli più utili quando si ha necessità di identificare un soggetto, è stata inserita la categoria dei "dati richiesti per il solo scopo di identificare l'utente". In questa categoria sono ricompresi gli indirizzi IP e le informazioni utili a individuare l'*user*: questi, generalmente ritenuti dati di traffico, sono assimilati nel caso specifico ai *subscriber data* in ragione della mera finalità di identificazione, con tutele ridotte rispetto alle categorie dei *traffic* e *content data.*

Il Regolamento sull'ordine europeo di produzione e le nuove misure introdotte dal Secondo Protocollo alla Convenzione di Budapest non trascurano i diritti degli utenti nel caso di acquisizione dei dati dai *provider* e specificano che questi debbano essere garantiti in conformità alla Convenzione europea dei diritti umani e alla Carta di Nizza, prevedendo anche dei motivi di rifiuto e specifici rimedi da attivare in caso di violazioni.

Le considerazioni su un eventuale rifiuto sono, tuttavia, rimesse in larga parte alla discrezionalità dei soggetti privati, che non possono però diventare garanti dei diritti, ruolo che deve essere ricoperto anzitutto dagli Stati. Si accoglie, pertanto, con favore la previsione, per l'EPO, della notifica contestuale alle autorità competenti dello Stato di esecuzione quando si richiedano dati di traffico o di contenuto. Le tempistiche previste, affinché le autorità possano opporsi alla consegna (10 giorni), tuttavia, non sembrano confacenti a quanto ragionevolmente servirebbe per valutare la richiesta e i suoi effetti.

Alla questione, nondimeno, non si può dare una risposta soddisfacente, posto che un allungamento dei tempi deve inevitabilmente fare i conti con la possibilità di perdita dei dati o con il rallentamento delle indagini e, pertanto, spetterà al legislatore effettuare le scelte di opportunità politica.

La direzione intrapresa dal legislatore europeo con l'emanazione del paccchetto *e-evidence* ruota attorno al principio di mutuo riconoscimento, il quale si conferma come pietra "angolare" della cooperazione giudiziaria in materia penale, in alternativa all'armonizzazione delle legislazioni nazionali. Quest'ultima risulta, tuttavia, fondamentale per alimentare la *mutual trust*, tanto più nel presente momento dove si profila una tendenza dei giudici nazionali – in Spagna, Italia, Germania e Portogallo – a privilegiare un'adesione

"cieca" ai provvedimenti dell'autorità straniera. È quanto avvenuto nelle sentenze connesse al caso *Encrochat*. I giudici nazionali hanno, infatti, ritenuto non sindacabili nel merito gli atti delle autorità francesi – le cui modalità operative erano coperte dal segreto di Stato – che hanno portato all'acquisizione e alla decriptazione delle comunicazioni di migliaia di utenti, ritenendole legittime, proprio in virtù del principio di riconoscimento reciproco e della fiducia tra Stati membri. Tale orientamento genera, inevitabilmente, dei dubbi sul piano della tutela dei diritti fondamentali, poiché non prevede un contraddittorio *ex post* idoneo a garantire il diritto di difesa.

Proprio sul caso *Encrochat* e sulla decriptazione, la recente pronuncia della Corte di Giustizia[537] relativa al rinvio operato dai giudici tedeschi, ha stabilito la legittimità dell'acquisizione a mezzo OEI pur quando l'autorità dello Stato di esecuzione non possa verificare l'integrità dei dati a causa dell'assoluta riservatezza delle operazioni. Questa sentenza, se pur chiarisca alcuni dubbi dei giudici nazionali, non può considerarsi la risposta definitiva e, anzi, si ritiene che il bilanciamento tra tutela dei diritti e persecuzione dei reati non possa che provenire dall'armonizzazione e, inoltre, dalla definizione di *standard* procedurali sull'acquisizione e sull'utilizzo delle prove digitali.

Il mutuo riconoscimento e la primazia del diritto UE non dovrebbero, infatti, essere di ostacolo al diritto alla difesa e al principio del contraddittorio.

Peraltro, bisogna sottolineare come l'evolversi della tecnologia abbia concorso alla definizione o alla nascita di nuovi diritti, il cui nucleo è strettamente connesso all'intimità dei soggetti. Non solo il diritto alla segretezza delle comunicazioni, ma anche il sopra citato *derecho al proprio entorno virtual*, il diritto all'onore, all'intimità personale, alla propria immagine, alla protezione dei dati personali e il diritto alla libertà di espressione.

Il mondo digitale, che ci rende ormai impossibile vivere una vita "*offline*", ha determinato un'estensione del domicilio, rendendo quasi automatica l'idea che a quello fisico ne corrisponda uno virtuale. E infatti, se si considera che nel domicilio il soggetto protegge la propria intimità al riparo dallo sguardo dei terzi, tale circostanza si manifesta in modo altrettanto pregnante rispetto ai dispositivi digitali, custodi di immagini, testi, audio o video appartenenti al nostro vissuto quotidiano, talvolta racchiusi in cartelle private o protette da codici. Allo stato, vi è una palese asimmetria tra il mondo fisico e quello virtuale: in quest'ultimo rimane traccia di tutto quello che viene effettuato. Da qui la necessità di apprestare specifiche tutele [538].

[537] CGUE, 30 aprile 2024, C-670/2022.

[538] Vedasi GUERRERO PALOMARES S., *La protección del derecho a la intimidad en el marco de la investigación tecnológica en el proceso penal*, in FONTESTAD PORTALÈS L., JIMÈNEZ LÓPEZ M., *La transformación digital de la cooperación jurídica penal internacional*, Aranzadi, 2021.

In questa corsa agli armamenti per poter acquisire le prove digitali al di fuori dei confini nazionali, si rende, pertanto, necessario armonizzare i vari aspetti connessi alle prove elettroniche e alle indagini "tecnologiche", così da rafforzare le basi su cui poggiare la cooperazione giudiziaria. *In primis*, è forte la necessità di definire, non solo a livello europeo, la categoria della prova digitale, trovando una definizione omogenea che sia valida e accettata sul piano internazionale dagli Stati, dalle autorità giudiziarie e di polizia e anche dagli operatori privati, come i *service provider.* Altro tema sul quale occorrerebbe avviare una riflessione comune è quello delle categorie di dati sui quali dovrebbe esservi una disciplina omogenea. Questo faciliterebbe l'affermazione di un livello di protezione dei diritti analogo in tutti gli Stati, con riflessi sulla *mutual trust*, elemento necessario per attuare una cooperazione giudiziaria effettiva.

Non meno importante è l'aspetto legato alle procedure utilizzate per l'acquisizione della prova digitale, la cui disciplina andrebbe uniformata per evitare dislivelli sul piano delle garanzie dei diritti fondamentali. Se, infatti, vi fossero degli *standard* procedurali adottati in maniera omogenea dalle autorità di polizia e dagli operatori di *digital forensics*, si potrebbe confidare in un generalizzato rispetto dei diritti fondamentali. Delle linee-guida sarebbero utili anche per la fase di conservazione e protezione della prova e, per garantirne la massima affidabilità, queste dovrebbero essere seguite non solo dalle autorità di polizia, ma anche dai soggetti privati. Ciò permetterebbe di dissolvere i dubbi relativi ai dati consegnati da un *provider*, non vincolato a specifiche procedure e, pertanto, *tradens* dei dati, estrapolati dai sistemi senza la certezza che, in tale attività, siano stati garantiti i diritti e le libertà fondamentali e che la prova sia rimasta inalterata.

Il rispetto delle procedure da parte di soggetti pubblici e privati va esteso alla catena di custodia che deve essere garantita affinché, in qualunque momento, sia possibile verificare l'affidabilità delle prove.

A oggi, emerge in maniera chiara la presenza di un *gap* nell'acquisizione, conservazione, protezione e utilizzabilità della prova digitale che va colmato mediante una disciplina autonoma. Alla luce dell'analisi effettuata, infatti, non si può ritenere che il rinvio agli istituti probatori tradizionali o la modifica di questi possa essere soddisfacente e adeguata alle caratteristiche intrinseche della prova digitale e del mondo virtuale.

Il *deficit* legislativo ha, senza dubbi, dei risvolti sul piano dell'ammissibilità, elemento non ancora adeguatamente attenzionato sul piano europeo, posto che il regolamento EPO e il Secondo Protocollo alla Convenzione di Budapest non hanno

certamente affrontato in maniera adeguata la questione, che si fa sempre più viva nelle Corti nazionali e rischia di vanificare l'acquisizione transnazionale della prova.

A tal proposito, di recente, è stata formulata una proposta di direttiva europea da parte della dottrina[539], finalizzata a trovare delle soluzioni idonee a bilanciare gli interessi in gioco, evitando, inoltre, che la transnazionalità del procedimento penale implichi un affievolimento dei diritti della difesa[540]. La proposta segue tre direttrici: per un verso, mira a illustrare quali regole vadano osservate in ambito nazionale per l'ammissibilità delle prove legittimamente acquisite secondo la *lex loci*, pur nel rispetto dei diritti fondamentali; inoltre, mette in luce la necessità di fissare a livello europeo delle norme precise che disciplinino la raccolta e la trasmissione delle prove, per garantire l'integrità e l'autenticità; infine, è finalizzata a predisporre rimedi legali effettivi attraverso i quali la difesa possa contestare le prove ammesse in violazione di tali regole.

Vi sono, inoltre, delle questioni che rimangono aperte, ma che si impongono con insistenza nello scenario attuale. *In primis*, il principio di territorialità può ancora ritenersi idoneo nella definizione della giurisdizione degli Stati? I confini nebulosi del cyberspazio non sembrano lasciare dubbi sul fatto che questo sia totalmente scisso da ogni coordinata spazio-temporale e l'avvento del Metaverso non fa che confermare e amplificare tale affermazione.

Come bisognerà, quindi, ridefinire la competenza degli Stati?

Mentre, da un lato, la dottrina profila l'ipotesi della distinzione tra *enforcement jurisdiction* e *investigative jurisdiction*, dall'altro viene delineata la possibilità di utilizzare un criterio di pertinenza, legato a fattori ulteriori rispetto al luogo fisico. Le due ipotesi non si escludono. Nel primo caso, tuttavia, se uno Stato ottenesse dei dati da un *provider* in violazione dei diritti umani, pregiudicando il cittadino di un altro Stato, chi dovrebbe garantirne il rispetto in virtù degli obblighi positivi a carico delle autorità statali? L'ipotesi della *investigative jurisdiction,* infatti, rischia di amplificare eventuali abusi e si ritiene attuabile solo allorquando sia stata realizzata l'armonizzazione già richiamata.

---

[539] Nell'ambito dello *European Law Institute* è stato infatti portato avanti un progetto finalizzato alla creazione di una proposta di direttiva: *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings,* https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf .

[540] V. BACHMAIER WINTER L, *Mutual Admissibility of Evidence and Electronic Evidence in the EU - A New Try for European Minimum Rules in Criminal Proceedings*? in *www.eucrim.eu*, 2023, 2, p. 223; ORLANDO C., *Mutua ammissibilità della prova tra gli Stati membri dell'Unione europea ed e-evidence: riflessioni a margine della proposta di direttiva dello European Law Institute*, in *www.sistemapenale.it*, 21 novembre 2023.

Pur avvertendo la necessità di pensare secondo schemi nuovi, siamo ancora rigidamente ancorati a quelli tradizionali ai quali, d'altronde, abbiamo sempre fatto riferimento. Il cambiamento in atto, tuttavia, ci chiede di ricostruire il rapporto tra giurisdizione e mondo digitale e, di conseguenza, la stessa disciplina in tema di prove digitali, creando un sistema normativo *ad hoc.* Questo dovrà sicuramente essere il prossimo passo, verificando, nel frattempo, come gli Stati implementeranno le misure del Secondo Protocollo alla Convenzione di Budapest e la disciplina sulla prova elettronica. Nel frattempo, nuovi interrogativi si pongono in relazione all'utilizzo del Metaverso[541], luogo immateriale in cui ogni utente può interagire percependo gli avvenimenti come nel mondo reale.

Spetta al legislatore trovare il giusto bilanciamento tra le diverse istanze in gioco che, in tanto potrà attuarsi, in quanto si avvii un processo di armonizzazione normativa che, nel rispetto dei diritti dei soggetti coinvolti, possa poi facilitare l'ammissibilità della prova digitale nel processo nazionale.

[541]Per approfondimenti FUMI V., *Metaverso e fenomenologia*, in www.sicurezzaegiustizia.com, 24 agosto 2022; LAZZARI S., *Metaverso: brevi riflessioni sui profili di diritto penale*, in www.filodiritto.com, 8 giugno 2022; ORLANDINI M.E., Social network *e molestie online: il Metaverso come nuovo* "locus commissi delicti?", in www.iusinitinere.it, 28 dicembre 2021.

Bibliografia

ABEL LLUCH X. (a cura di), *La prueba electrónica*, Bosch, 2011.

ABRAHA H.H., *Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiative*, in *International Journal of Law and Information Technology*, 2021, 2, p. 118.

AGUILERA MORALES M.*, Las diligencias de investigación fiscal*, Aranzadi, 2015.

AGUILERA MORALES M., *El Exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas*, in *Boletín del Ministerio de Justicia*, 2021, 2145.

ALIMONTI V., *Evaluando el nuevo Protocolo al Convenio sobre la Ciberdelincuencia en América Latina: Preocupaciones, consideraciones respecto a los derechos humanos y estrategias de mitigación*, Electronic Frontier Foundation, 2022.

ALLEN S., *Enforcing criminal jurisdiction in the clouds and international law's enduring commitmet to territoriality*, in ALLEN S., COSTELLOE D., FITZMAURICE M., GRAGL P., GUNTRIP E., *The Oxford Handbook of Jurisdiction in International Law*, Oxford University Press, 2019.

ANDOLINA E., *La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di* data retention?, in *Proc. Pen. Giust*., 2021, 5, p. 1204.

ARNELL P., FATUROTI B., *The prosecution of cybercrime – why trasnantional and extraterritorial jurisdiction should be resisted*, in I*nternational review of law, computers and technology*, 8 giugno 2022.

ARRABAL PLATERO P.*, La prueba tecnológica: aportación, practica y valoración,* Tirant Lo Blanch, 2020.

ARRABAL PLATERO P., *La tecnología y el derecho procesal: la prueba tecnologìca en la actualidad y la IA en el futuro*, in RAMIREZ CARVAJAL D.M. (a cura di*), Justicia Digital. Un análisis internacional en época de crisis,* Universidad de Salamanca: Editorial Justicia y Proceso, 2020.

ATERNO S., CAJANI F., COSTABILE G., CURTOTTI D., (a cura di) Cyber Forensics *e Indagini digitali. Manuale tecnico-giuridico e casi pratici,* G. Giappichelli Editore, 2021.

BACHMAIER WINTER L., *La orden europea de investigación y el principio de proporcionalidad*, in *Revista General de Derecho europeo*, 2011, p. 25.

BACHMAIER WINTER, L., *The Role of proportionality principle in cross-border investigations involving fundamental rights*, in RUGGERI S. (a cura di), *Transnational inquiries and the protection of fundamental rights in criminal proceedings. A study in memory of Vittorio Grevi and Giovanni Tranchina*, Springer, 2013, p. 85.

BACHMAIER WINTER L., *The proposal for a directive on the european investigacion order and the grounds for refusal: a critical assessment,* in RUGGERI S., (a cura di), *Transnational evidence and multicultural inquiries in Europe*, Springer, 2014.

BACHMAIER WINTER L., *Prueba transnacional penal en Europa: la Directiva 2014/41 relativa a la Orden europea de investigación,* in *Revista General de Derecho Europeo*, 2015, 36.

BACHMAIER WINTER L., *Transnational evidence: towards the transposition of the Directive 2014/41 regarding the European Investigation Order in criminal matters*, in *www.eucrim.eu,* 2015, p. 47.

BACHMAIER WINTER L., *Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015*, in *Boletìn del Ministerio de Justicia*, 2017, 2195, p. 3.

BACHMAIER, L., *Mutual recognition and cross-border interception of communications: the way ahead for the European Investigation Order*, Hart Publising, 2017.

BACHMAIER WINTER L, *Mutual Admissibility of Evidence and Electronic Evidence in the EU - A New Try for European Minimum Rules in Criminal Proceedings?* in *www.eucrim.eu*, 2023, 2, p. 223.

BARBIERI A., *I limiti di utilizzabilità dei messaggi crittografati scaricati da un* server *estero ed acquisiti mediante ordine europeo di indagine,* in *Giurisprudenza Penale Web*, 2023, 2.

BARONA VILAR S. (a cura di), *Justicia civil y penal en la era global*, Tirant Lo Blanch, 2017.

BARTOLI L., MAIOLI C., *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti,* in *Informatica e diritto*, 2015, vol. XXIV, p. 139.

BELFIORE R., *La prova penale "raccolta" all'estero*, Aracne editrice, 2014.

BELFIORE R*., Su alcuni aspetti del decreto di attuazione dell'ordine europeo di indagine penale*, in *Cass. Pen.,* 2018, p. 400.

BENE T., LUPARIA L., MARAFIOTI L., *L'ordine europeo di indagine,* G. Giappichelli Editore, 2016.

BERNARDI S*., Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624-bis c.p*., in *Dir. Pen. Cont.*, 4 luglio 2017.

BIASIOTTI M.A., *Present and future of the exchange of electronic evidence in Europe*, in BIASIOTTI M.A. MIFSUF BONNICI J.P., CANNATACI J., TURCHI F., (a cura di), *Handling and exchanging electronic evidence across Europe,* Springer, 2019.

BILGIC S., *Something old, Something new and something moot: the privacy crisis under the cloud act,* in *Harvard Journal of Law & Technology*, 2018, vol. 32, 1, p. 321.

BLANCO A.E., *La jurisprudencia del Tribunal Constitucional español sobre el principio de proporcionalidad en el proceso penal*, in *Anuario de derecho penal y ciencias penales*, 2021, 1, p. 707.

BONCINELLI V., *Modelli tecnici e disciplina giuridica del c.d.* cloud computing, in *Riv. italiana di informatica e diritto*, 2021, 1, p. 27.

BORGES BLAZQUEZ R., *La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajeria instantánea*, in *Rev. Boliv. de Derecho*, 2018, 25, p. 536.

BUCCARELLA M., *Il secondo protocollo addizionale alla Convenzione di Budapest alla luce del diritto internazionale e dei trattati*, in *Dir. Pen. Proc*., 2022, 9, p. 1160.

BUENO DE MATA F., *Prueba Electronica y Proceso 2.0*, Tirant Lo Blanch, 2014.

BUENO DE MATA F., *Las diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos*, Aranzadi, 2019.

BUENO DE MATA F., *Datos personales y proceso penal: diligencias de investigación y tecnologías disruptivas*, in PEREIRA PUIGVERT S., ORDÓÑEZ PONZ F., PESQUEIRA ZAMORA M. J. (a cura di), *Investigación y proceso penal en el siglo XXI. Nueva tecnologías y protección de datos,* Aranzadi, 2021, p. 494 ss.

BUONO L., *The genesis of the European Union's new proposed legal instrument(s) on e-evidence, towards the EU Production and Preservation Orders*, in *ERA Forum*, 2019,19, p. 307.

BURGOS LADRÓN DE GUEVARA J., *La orden europea de investigación penal en España: aplicación y contenido. Posible relación con la orden europea de protección,* in *Diario La Ley,* 2015, 8660.

CAIANIELLO M., *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Proc. Pen. Giust.,* 2015, 3, p. 2.

CAIANIELLO M., *L'attuazione della direttiva sull'ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio*, in *Cass. Pen.*, 2018, 6, p. 2197.

CAIANIELLO M., CAMON A. (a cura di), *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, Cedam, 2021.

CAMALDO L., *La normativa di attuazione dell'ordine europeo di indagine penale: le modalità operative del nuovo strumento di acquisizione della prova all'estero*, in *Cass. Pen.*, 2017, 11, p. 4196.

CAPRIOLI F., *Il "captatore informatico" come strumento di ricerca della prova in Italia,* in *Rev. Brasileira de dereito processual penal,* 2017, vol. 3, 2, p. 483.

CARLIZZI G., TUZET G. (a cura di), *La prova scientifica nel processo penale*, G. Giappichelli Editore, 2018.

CARPANELLI E., LAZZERINI N. (a cura di), *Use and Misuse of New Technologies. Contemporary Challenges in International and European Law*, Springer, 2019.

CASEY E., *Digital Evidence and Computer Crime. Forensics Science, Computer and the Internet,* Elsevier, 2011.

CASINO F., PINA C., LÓPEZ AGUILAR P., BATISTA E., *SoK: Cross-border Criminal Investigations and Digital Evidence*, in J*ournal of Cybersecurity*, 2022, 8.

CEDEÑO HERNÁN, M. (a cura di), *Nuevas tecnologías y derechos fundamentales en el proceso,* Aranzadi, 2017.

CELOTTO A., *Sulla conversione in legge del decreto-legge 10 agosto 2023, n. 105 (disposizioni urgenti in materia di processo penale*), in *Giurisprudenza Penale*, 2023, 9.

CENTORAME V., *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. It. Dir. e Proc. Pen.*, 2022, 2, p. 499.

CHABANEIX L., *EncroChat: aproximación al estado de la cuestión en perspectiva comparada*, in *www.elderecho.com,* 21 dicembre 2022.

CHRISTAKIS T., TERPAN F., *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in *International data privacy law*, 2021, 11, 2, p. 81.

COLAIOCCO A., *La rilevanza delle* best practices *nell'acquisizione della* digital evidence *alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. Pen.*, 2019, 1.

COLAROCCO V., GROTTO T., VACIAGO G. (a cura di), *La prova digitale. La casistica civile e penale e gli strumenti di acquisizione in ambito cloud,* Giuffrè Francis Lefebvre, 2020.

COLOMBO E., *Ordini europei di produzione e conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, in *Cass. Pen.*, 2019, 7, p. 2722.

CONDE FUENTES J, SERRANO HOYO G. (a cura di), *La justicia digital en Espana y la Uniòn Europea*, Atelier, 2019.

CONTI C., TORRE M., *Spionaggio digitale nell'ambito dei social network*, in SCALFATI A. (a cura di), *Le indagini atipiche,* Giappichelli, 2019, p. 558.

CONTI S., *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, 2015, 1-2, p.153.

COSTABILE G., Scena criminis*, documento informatico e formazione della prova penale*, in *Diritto dell'informazione e dell'informatica*, 2005, p. 531.

CUOMO L., GIORDANO L., *Informatica e processo penale*, in *Proc. Pen. Giust.*, 2017, 4, p. 716.

CURTOTTI D., RIZZI V., NOCERINO W., RUSSITTO A., GILIBERTI G., SCARPA G., *Piattaforme criptate e prova penale,* in *www.sistemapenale.it*, 26 giugno 2023.

DANIELE M., *La prova digitale nel processo penale*, in *Riv. Dir. Proc*., 2011, p. 286.

DANIELE M., *La metamorfosi del diritto delle prove nella Direttiva sull'ordine europeo di indagine penale*, in *Diritto Penale Contemporaneo*, 20 novembre 2014,

DANIELE M., *L'impatto dell'ordine europeo di indagine penale sulle regole probatorie nazionali,* in *Dir. Pen. Cont.- Rivista trimestrale*, 2016, 3, p. 63.

DANIELE M., *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d.lgs. n. 108 del 2017,* in *Dir. Pen. Cont.,* 28 luglio 2017.

DANIELE M., *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. Pen. Giust*, 2018, 5, p. 831.

DANIELE M., *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Brasileira de Direito Procesal Penal*, 2019, vol. 5, 3, p. 1277.

DANIELE M., *Il controllo giurisdizionale sull'emissione dell'ordine europeo di indagine: la necessaria simmetria con la disciplina nazionale nei casi interni analoghi*, in *www.sistemapenale.it*, 31 marzo 2022.

DANIELE M., *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite,* in *www.sistemapenale.it*, 11 dicembre 2023.

DASKAL J., *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, in *www.jnslp.com,* 2016.

DASKAL J., *Unpacking the CLOUD Act*, in *www.eucrim.eu*, 2019.

DE AMICIS G., *Limiti e prospettive del mandato europeo di ricerca della prova*, in *Dir. Pen. Cont.*, 5 aprile 2011.

DE AMICIS G., *Dalle rogatorie all'ordine europeo di indagine: verso un nuovo diritto della cooperazione giudiziaria penale*, in Cassazione penale, 2018, 1, p. 26.

DE BUSSER E., *The digital unfitness of mutual legal assistance*, in *Security and human rights*, vol. 2017, 28, 1, p. 161.

DE LA CHAPELLE B., FEHLINGER P., *Jurisdiction on the Internet: from legal arms race to transnational cooperation*, in FROSIO G., (a cura di) *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, 2020.

DE LUCA C., *La Corte di giustizia si pronuncia nuovamente sull'ordine europeo di indagine penale: la tutela dei diritti fondamentali prevale sull'efficienza investigativa*, in *www.sistemapenale.it*, 9 marzo 2022.

DE RUVO G., *Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso Tiktok come paradigma*, in *Riv. italiana di informatica e diritto*, 2022,1, p. 113.

DELLA TORRE J., *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in *www.sistemapenale.it*., 29 aprile 2021.

DI PAOLO G., *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, CEDAM, 2008.

DELGADO MARTIN J., *La prueba digital. Concepto, clases, aportación al proceso y valoración,* in *Diario La Ley, Sección Ciberderecho*, 2017, 6.

DELGADO MARTIN J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Wolters Kluwer, 2018.

DIAZ LIMON J.A., *Incorporación de la prueba cibernética e informática: electrónica y digital,* in *IUDICIUM – Revista de derecho procesal de la asociación iberoamericana de la Universidad de Salamanca*, 2019, 2, p. 13.

DIDDI A., *Le novità in materia di intercettazioni telefoniche*, in *www.penaledp.it*, 31 agosto 2020.

DINACCI F. R., *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Proc. Pen. Giust.*, 2022, 2, p. 301.

ESPINA RAMOS J.A., *The European investigation order and its relationship with other judicial cooperation instruments*, in *www.eucrim.eu*, 2019.

ESPOSITO G., *Analisi del "*Report on Eurojust´s casework in the field of the European Investigation Order", in *Proc. Pen. Giust.*, 2021, 3, p. 677.

FELICIONI P., *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. Pen. Giust.*, 2016, 5, p. 118.

FERNANDEZ BERMEJO D., MARTINEZ ATIENZA G., *Ciberseguridad, ciberespacio y ciberdelincuencia,* Aranzadi, 2018.

FERNÁNDEZ RODRÍGUEZ A.P., *Algunas consideraciones a partir de la regulación del registro de dispositivos de almacenamiento masivo de la información*, in *Diario La Ley*, 2019, 9433.

FILIPPI L., *Il virus* trojan*: uno strumento nelle mani incontrollabili della polizia giudiziaria*, in *www.penaledp.it* , 30 novembre 2020.

FILIPPI L., *La disciplina italiana dei tabulati telefonici e telematici contrasta con il diritto U.E.,* in *www. dirittodidifesa.eu*, 20 marzo 2021.

FILIPPI L., *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in www.penaledp.it, 1ottobre 2021.

FILIPPI L., *Il cavallo di Troia e l'ispe-perqui-intercettazione*, in *www.penaledp.it,* 21 marzo 2022.

FILIPPI L., *Riservatezza e* data retention*: una storia infinita*, in www.penaledp.it, 23 giugno 2022.

FILIPPI L., *Quattro miti da sfatare sull'intercettazione dei cellulari Blackberry*, in *www.penaledp.it*, 28 aprile 2023.

FORLANI G., *The E-evidence Package - The Happy Ending of a Long Negotiation Saga*, in *www.eucrim.eu,* 2023,2, p. 174.

FLOR R., *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "*Data retention*" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, *in Dir. Pen. Cont.*, 28 aprile 2014.

FLOR R., Data retention *e art. 132 cod.* privacy: vexata quaestio?, in *Dir. Pen. Cont.*, 29 marzo 2017.

FLOR R., MARCOLINI S., *Dalla* data retention *alle indagini ad altro contenuto tecnologico*, G. Giappichelli Editore, 2022.

FONTESTAD PORTALÈS L., JIMÈNEZ LÓPEZ M., *La transformación digital de la cooperación jurídica penal internacional,* Aranzadi, 2021.

FROVA G., *La Cassazione sulla riconducibilità all'art. 266 c.p.p. degli* screenshot *tramite captatore informatico*, in *www.sistemapenale.it*, 2 giugno 2022.

FUENTES SORIANO O., *The (future) European Electronic Evidence Delivery Order*, in *Journal of Applied Business & Economics*, vol. 22, 8, 2020

FUMI V., *Metaverso e fenomenologia*, in *www.sicurezzaegiustizia.com*, 22 agosto 2022.

GALLUCCIO A., *L. 23 giugno 2017, n. 103, in G.U., serie generale, 4 luglio 2017, n. 154,* in *Dir. Pen. Cont.*, 6 luglio 2017.

GARCIMARTIN MONTERO R., *The european investigation order and the respect for fundamental rights in criminal investigations,* in *www.eucrim.eu,* 2017*,* 1.

GATTO C.E., *Il principio di proporzionalità nell'ordine europeo di indagine penale*, in *Dir. Pen. Cont.*, 12 febbraio 2019.

GERACI R.M., *Primi disorientamenti interpretativi in tema di OEI: la Cassazione interviene sulle corrette modalità del giudizio di riconoscimento*, in *Proc. Pen. Giust.,* 2019, 5, p. 1157.

GERACI R. M., *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento E-evidence*, in *Cass. Pen.*, 2019.

GERACI R. M., *Il mutuo riconoscimento nella cooperazione processuale: genesi, sviluppi, morfologich*e, Cacucci Editore, 2020.

GIALUZ M., CABIALE A., DELLA TORRE J., R*iforma Orlando: le modificazioni attinenti al processo penale, tra codificazione della giurisprudenza, riforme attese da tempo e confuse innovazioni*, in *Dir. Pen. Cont.*, 20 giugno 2017.

GIALUZ M., DELLA TORRE J., *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. Pen. Cont.*, 31 maggio 2018.

GIORDANO L., *L'intercettazione delle* e-mail *(già) ricevute o inviate e l'acquisizione di quelle parcheggiate nella cartella "bozze*", in *www.ilpenalista.it*, 14 novembre 2016.

GIORDANO L., *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, *in Dir. Pen. Cont.*, 20 marzo 2017.

GIORDANO L., *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in *Dir. Pen. Cont.*, 27 settembre 2017.

GIORDANO L., *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *www.sistemapenale.it*, 21 aprile 2020.

GIORGI E., *Il principio del mutuo riconoscimento nell'ordinamento dell'Unione europea*, Firenze University Press, 2020.

GONZALEZ CANO M.I., *Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680*, *in Rev. Brasileira de Direito Processual Penal*, 2019, vol. 5, 3, p. 1331.

GONZÁLEZ FUSTER G., VÁZQUEZ MAYMIR S., *Cross-border access to e-evidence : framing the evidence*, in *Liberty and Security in Europe*, 2020, 2, p. 9.

GONZALEZ GRANDA P. (a cura di), *Exclusiones probatorias en el entorno de la investigación y prueba electrónica*, Editorial Reus, 2020.

GRANDI C., *Il mutuo riconoscimento dei provvedimenti di confisca alla luce del Regolamento (UE) 2018/1805*, in *www.lalegislazionepenale.eu*, 2021.

GRANOZIO L., *Corte di Giustizia sui tabulati: soluzioni contrastanti*, in *www.penaledp.it*, 18 maggio 2021.

GRIFANTINI F.M., *Ordine europeo di indagine penale e investigazioni difensive*, in *Proc. Pen. Giust.*, 2016, 6.

GRIFFO M., *Perquisizione informatica…e dintorni*, in *Giurisprudenza Penale Web*, 2019, 5.

GRIFFO M., *Rilievi sull'impiego del* troyan *nei procedimenti per i reati contro la pubblica amministrazione*, in *Proc. Pen. Giust.*, 2020, 2, p. 482.

HASSAN N.A., *Digital Forensics Basics. A practical guide using Windows OS*, Apress, 2019.

ILARDA G., MARULLO G. (a cura di), Cybercrime*: Conferenza Internazionale : la Convenzione del Consiglio d'Europa sulla criminalità informatica. Osservatorio permanente sulla criminalità organizzata*, Giuffrè, 2004.

JIMENO BULNES M., *Aproximación legislativa versus reconocimiento mutuo en el desarrollo del espacio judicial europeo: una perspectiva multidisciplinar,* Bosch Editor, 2016.

JUSZCZAK A., SASON E., *The use of electronic evidence in the european area of freedom, security, and justice*, in *www.eucrim.eu,* 2023, 2, p.182.

KÄVRESTAD J., *Fundamentals of digital forensics. Theory, methods, and real-life applications,* Springer, 2018.

KERIMKMAE T., RULL A., (a cura di) *The future of law and eTechnologies*, Springer, 2016.

KOSTORIS E.R., *Manuale di procedura penale europea*, Giuffrè, 2019.

KRUEGER C., MCKEOWN S., *Using Amazon Alexa APIs as a source of digital evidence*, in *International Conference on cyber security and protection of digital services (cyber security)*, 2020, p. 1.

LARO GONZALÈZ M. E., *Prueba electrónica: situación actual en el proceso penal y perspectivas en el futuro*, in ARRABAL PLATERO P., CONDE FUENTES J., GARCIA MOLINA P., SERRANO HOYO G., *La justicia digital en España y la Unión Europea*, Atelier Libros Jurídicos, 2019.

LARO GONZÁLEZ E., *La orden europea de investigación en el espacio europeo de justicia,* Tirant lo Blanch, 2021.

LAZZARI S., *Metaverso: brevi riflessioni sui profili di diritto penale*, in *www.filodiritto.com,* 30 novembre 2022.

LAZZERI F., *Convertito in legge, con modificazioni, il d.l. 105/23: novità in materia di intercettazioni, incendio boschivo, ambiente e 231*, in w*ww.sistemapenale.it*, 5 ottobre 2023.

LEONHARDT dos SANTOS D., *Territoriality in the context of global crime: Reflections of the impact of cyberspace on jurisdictional delimitation,* in *Rev. Brasileira de Direito Processual Penal*, vol. 5, 2, 2019, p. 597.

LORUSSO S., Digital evidence*,* cybercrime *e giustizia penale 2.0,* in *Proc. Pen. Giust*., 2019, 4, p. 821.

LUBIN A. *The prohibition on extraterritorial enforcement jurisdiction in the datasphere*, in PARRISH A, RYNGAERT C. (a cura di), *Research handbook on extraterritoriality in international law,* Elgar Publishing, 2022.

LUDOVICI L., *I criptofonini: sistemi informatici criptati e* server *occulti*, in *www.penaledp.it*, 14 ottobre 2023.

LUPARIA L., *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I profili processuali*, in *Dir. Pen. Proc*., 2008, p. 720.

LUPARIA L. (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48),* Giuffrè, 2009.

LUPARIA L., Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè Editore, 2012.

LUPARIA L., MARAFIOTI L., PAOLOZZI G. (a cura di), *Dimensione tecnologica e prova penale,* G. Giappichelli Editore, 2019.

LUPARIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica*, Giuffrè, 2007.

MAGNO T., *Il progetto* evidence *e le principali criticità nell'accesso alla prove elettroniche transnazionali in materia penale: quale futuro?,* in *Informatica e diritto*, 2016, XXV, 2, p. 145.

MAGRO SERVET V., *¿Como aportar la prueba digital en el proceso penal?*, in *Diario La Ley – Sección Doctrina*, 2021, 9824.

MAILLART J. B., *The limits of subjective territorial jurisdiction in the context of cybercrime*, in *ERA Forum*, 2018, 18, p. 375.

MALACARNE A., *Ancora sulle ricadute interne della sentenza della Corte di Giustizia in materia di acquisizione di tabulati telefonici: il G.i.p. di Roma dichiara il "non luogo a provvedere" sulla richiesta del p.m.*, in *www.sistemapenale.it*, 5 maggio 2021.

MALACARNE A., TESSITORE G., *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di Giustizia: ancora inadeguata la disciplina interna*?, in *Arch. Pen.*, 2022, 3.

MANGIARACINA A., *A new and controversial scenario in the gathering of evidence at the european level: the proposal for a directive on the European investigation order*, in *Utrecht Law Review*, 2014, 10.

MANGIARACINA A., *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale*, in *Diritto penale e processo,* 2018, 2, p. 158.

MARAFIOTI L., PAOLOZZI G. (a cura di), '*Incontri ravvicinati' con la prova penale,* G. Giappichelli Editore, 2014.

MARTIN F., *Cass. Pen., Sez. V, 11 aprile 2023, n. 15216, sulla nozione di privata dimora con riferimento allo studio legale*, in *www.iusinitinere.it*, 2023.

MARTINEZ GARCÍA E., *La orden de investigación europea. Las futuras complejidades previsibles en la implementación de la Directiva en España*, in *La Ley Penal*, 2014, 106, p. 8.

MARTINEZ GARCÍA E., *La orden europea de investigación*, Tirant Lo Blanch, 2016.

MILITELLO V., SPENA A. (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Giappichelli Editore, 2018.

MORCELLA M.T., *Ancora questioni in tema di sequestro di* smartphone*,* in *www.penaledp.it,* 9 novembre 2023.

NADDEO G., *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "*data retention saga*" dinanzi alla Corte di Giustizia*, in *Freedom Security & Justice: european legal studies*, 2022, 2.

NAVARRO FRIAS I., *El principio de proporcionalidad en sentido estricto: ¿principio de proporcionalidad entre el delito y la pena o balance global de costes y beneficios?,* in *InDret,* 2010, 2.

NULLO L., *Sequestro probatorio di materiale documentativo e principi di adeguatezza e proporzionalità*, in *Proc. Pen. Giust.*, 2020, 3, p. 663.

OERLEMANS J.J., VAN TOOR D.A.G., *Legal aspects of the EncroChat operation: a human rights perspective*, in *European Journal of crime, criminal law and criminal justice*, 27 dicembre 2022.

ORLANDINI M.E., Social network *e molestie online: il Metaverso come nuovo* "locus commissi delicti?", in *www.iusinitinere.it,* 28 dicembre 2021.

ORLANDO C., *Mutua ammissibilità della prova tra gli Stati membri dell'Unione europea ed e-evidence: riflessioni a margine della proposta di direttiva dello European Law Institute,* in *www.sistemapenale.it, 21* novembre 2023.

ORTIZ PRADILLO J.C., *Problemas procesales de la ciberdelincuencia*, Colex, 2013.

PADUA G., *L'accesso alla casella e-mail e l'acquisizione dei contenuti: un delicato inquadramento normativo*, in *Proc. Pen. Giust*, 2018, 3, p. 590.

PALLADINI V., Data retention *e* privacy *in rete: verso una regolazione conforme al diritto UE*?, in *Riv. Italiana di Informatica e diritto,* 2022, 1, p. 103.

PARODI C., *Profili tecnico-investigativi e di diritto processuale interno: dal* transborder access to data *al nuovo art. 234*-bis *c.p.p.*, in www.ilpenalista.it, 31 maggio 2016.

PARLATO L., *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. Pen. Giust*, 2020, 2, p. 291.

PEREIRA PUIGVERT S., ORDÓÑEZ PONZ F., PESQUEIRA ZAMORA M. J. (a cura di), *Investigación y proceso penal en el siglo XXI. Nueva tecnologías y protección de datos*, Aranzadi, 2021.

PEREZ GIL J., *El proceso penal en la sociedad de la informaciòn. Las nuevas tecnologias para investigar y probar el delito*, La Ley, 2012.

PÉREZ GIL, J., *Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución*, in BRIGHI R., PALMIRANI M., SÁNCHEZ JORDÁN M.E. (a cura di), *Informatica giuridica e informatica forense al servizio della società della conoscenza: scritti in onore di Cesare Maioli*, Aracne Editrice, 2018, p. 187.

PETERSON G., SHENOS S. (a cura di), *Advances in Digital Forensics XV*, Springer, 2019.

PEZZUTO R., *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, in *Dir. Pen. Cont.*, 29 gennaio 2019.

PINTO PALACIOS F., PUJOL CAPILL P., *La prueba en la era digital*, Wolters Kluwer, 2017.

PISANI M.M., *Problemi di prova in materia penale. La proposta di direttiva sull'Ordine Europeo di Indagine,* in *Arch. Pen.,* 2011, 3.

PITTIRUTI M., *Profili processuali della prova informatica,* in L. MARAFIOTI, G. PAOLOZZI (a cura di), '*Incontri ravvicinati' con la prova penale*, G. Giappichelli Editore, 2014.

PITTIRUTI M., Digital evidence *e procedimento penale,* G. Giappichelli Editore, 2017.

PITTIRUTI M., *L'apprensione all'estero della prova digitale*, in LUPARIA L., MARAFIOTI L., PAOLOZZI G. (a cura di), *Dimensione tecnologica e prova penale*, G. Giappichelli Editore, 2019.

PITTIRUTI M., *Dalla Corte di cassazione un* vademecum *sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali* omnibus, in *www.sistemapenale*.it, 14 gennaio 2021.

POLLICINO O., BASSINI M., *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. Pen. Cont.*, 9 gennaio 2017.

RACHAVELIAS M. G., *Online financial crimes and fraud committed with electronic means of payment – a general approach and case studies in Greece*, in *ERA Forum*, 2018, p. 339.

RAYÓN BALLESTEROS M. C., *Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015*, in *Anuario Jurídico y Económico Escurialense*, 2019, 52, p. 197.

RODRIGUEZ MEDEL NIETO C., *Obtención y admisibilidad en España de la prueba penal transfronteriza,* Aranzadi, 2016.

RUGGERI E., *L'ordine europeo di indagine – EIO:come funziona?*, in *Cass. Pen.*, 1, 2017.

RUGGIERI F., *Le nuove frontiere dell'assistenza penale internazionale: l'ordine europeo di indagine penale*, in *Proc. Pen. Giust.*, 2018, 1.

SÁNCHEZ ARJONA M. L., *La Orden Europea de Investigación y su incorporación al derecho español*, Tirant lo Blanch, 2020.

SÁNCHEZ BARRIOS M.I., *Análisis sobre la protección de datos personales y el principio de disponibilidad en el ámbito de la cooperación judicial penal en la Unión Europea* in FONTESTAD PORTALÈS L., JIMÈNEZ LÓPEZ M. de las Nieves (a cura di), *A vueltas con la transformación digital de la cooperación jurídica penal internacional*, Aranzadi, 2022.

SANNA A., *La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati,* in *Discrimen*, 2022.

SCALFATI A. (a cura di*), Le indagini atipiche*, G. Giappichelli Editore, 2014.

SCOMPARIN L., CABIALE A., *The proportionality test in Directive 2014/41/EU: Present and future of a fundamental Principle*, in *www.rivista.eurojus.it* , 2022, 2.

SELVAGGI E., *La circolare del Ministero della Giustizia sul c.d. ordine europeo di indagine*, in *Dir. Pen. Cont.*, 7 novembre 2017.

SIRACUSANO F., *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, in *Arch. Pen.*, 2017, 2.

SIRACUSANO F., *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. Pen. Giust.*, 2017, p. 178.

SHURSON J., D*ata protection and law enforcement accesso to digital evidence: resolving the reciprocal conflicts between EU and US law*, in *International Journal of Law and Information Technology*, 2020, vol. 28, 2, p. 167.

SIGNORATO S., *Le indagini digitali – Profili strutturali di una metamorfosi investigativa*, G. Giappichelli Editore, Torino, 2018.

SOANA G., *L'accesso transfrontaliero alla prova informatica. Oltre il principio di territorialità,* in *Riv. Semestrale di diritto*, 2020, 2.

SPANGHER G., *Servono regole di garanzia per la prova informatica*, in *www.penaledp.it,* 12 ottobre 2023.

SPIEZIA F., *Cooperazione internazionale e tutela delle vittime nel cyberspazio*, in *Dir. Pen. Proc*., 2022, 9, p. 1137.

SPIEZIA F., *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: Il ruolo di Eurojust,* in *www.sistemapenale.it*., 14 luglio 2023.

TINOCO PASTRANA A., *El embargo preventivo y el aseguramiento de pruebas en los procesos penales en la Unión Europea. Novedades tra la Ley 23/2014, de reconocimiento mutuo de resoluciones penalesen la Unión Europea y la Directiva 2014/41/CE relativa a la orden europea de investigación en materia penal,* in *Cuadernos Europeos de Deusto,* 2015 52, p. 121.

TINOCO PASTRANA A., *L'ordine europeo di indagine penale*, in *Proc. Pen Giust.*, 2017, 2, p. 346.

TONDI V., *L'accesso transfrontaliero all'*electronic evidence*, tra esigenze di effettività e tutela dei diritti,* in *Dir. Pen. Cont.- Rivista Trimestrale*, 2019, 2, p. 439.

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*, in *www.sistemapenale.it*, 7 maggio 2021.

TONINI P., *Considerazioni su diritto di difesa e prova scientifica*, in *Arch. Pen.*, 2011, 3.

TOPALNAKOS P., *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, in *www.eucrim.eu*, 2023, 2, p.200.

TORRE M., *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, in *Informatica e diritto*, 2015, XXIV, 1-2, p. 65.

TORRE M., *Indagini informatiche e principio di proporzionalità*, in *Proc. Pen. Giust*, 2019, 6, p. 1433.

TOSZA S., *The European Commission's Proposal on Cross-Border Access to E-Evidence*, in *www.eucrim.eu*, 2018, 4, p. 212.

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*, in *New Journal of European Criminal Law*, 2020, vol. 11, p. 161.

TROGU M., *Come si intercettano le* chat pin to pin *tra dispositivi Blackberry?,* in *Proc. Pen. Giust*, 2016, 3, p. 73.

UZAROVSKA LAZETIK B G., O. KOSHEVALISKA, *Digital evidence in criminal procedures – A comparative approach*, in *Balkan Social Science Review*, 2013, 2, p. 63.

VACIAGO G., Privacy *e tutela dell'ordine pubblico in Europa e negli Stati Uniti: un differente approccio per raggiungere un compromesso,* in *Informatica e diritto*, 2009, XVIII, 1, p. 135.

VACIAGO G., Digital evidence*: i mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato,* G. Giappichelli Editore, 2012.

VALENTINI C., *L'acquisizione della prova tra limiti territoriali e cooperazione con autorità straniere*, CEDAM, 1998.

VALLS PRIETO J., *Un ejemplo de análisis empírico en el derecho penal basado en una metodología mixta: la Orden Europea de Investigación*, Editorial Comares, 2022.

WAHL T., *E-evidence: Commission obtains mandates for EU-US agreement and negotiations in Council of Europe*, in *www.eucrim.eu*, 10 settembre 2019.

WAHL T., *First CJEU judgement on European Investigation Order,* in *www.eucrim.eu* , 2020.

WAHL T., RIEHLE C., *Trojan – Encrypted device reveals criminal activities*, in *www.eucrim.eu*, 10 luglio 2021.

WAHL T., *Dismantled encryption networks: German Courts confirmed use of evidence from Encrochat surveillance,* in *www.eucrim.eu*, 20 marzo 2022.

WAHL T., *Germany: Federal Court of Justice confirms use of evidence in Encrochat cases*, in *www.eucrim.eu*, 19 maggio 2022.

WAHL T., *Encrochat turns into a case for the CJEU*, in *www.eucrim.eu,* 18 novembre 2022.

ZICCARDI G., *Crittografia e diritto*, G. Giappichelli Editore, 2003.