ANDREA COLAIOCCO

La rilevanza delle *best practices* nell'acquisizione della *digital evidence* alla luce delle novelle sulla cooperazione giudiziaria

Le recenti riforme in materia di cooperazione giudiziaria pongono nuove problematiche in ordine all'invalidità della prova digitale acquisita all'estero. Dopo aver richiamato la rilevanza, ai fini della inutilizzabilità, dell'acquisizione in Italia della *digital evidence* senza il rispetto delle *best practices*, viene analizzata la sanzione processuale per la violazione delle *best practices* nelle operazioni compiute all'estero sia attraverso la rogatoria internazionale sia attraverso l'ordine europeo di indagine. Si conclude che la sanzione applicabile nel processo italiano rimane, anche in siffatto caso, l'inutilizzabilità della prova digitale, ai sensi dell'art. 191 c.p.p.

Recent developments in judiciary cooperation arise new problems regarding the validity of the digital evidence that has been acquired outside national borders. After recalling the invalidity in the Italian system of the digital evidence that has been acquired without the respect of the best practices, the present work analyses the consequences in terms of validity in case of violation of the best practices in operations carried out outside national borders both through the letter rogatory and the European Investigation Order. In conclusion, in the Italian trial the consequence of such violation is the impossibility of utilisation of the digital evidence as stated in Article 191 of the Italian Code of Criminal Procedure.

1. Premessa: *le best practices.*

È esperienza ormai comune come sia sempre maggiore l'«esigenza, per gli organi investigativi, di ricercare elementi di prova tra i dati contenuti in sistemi informatici»[1]. La rivoluzione digitale ha avuto, infatti, un forte effetto anche nel processo penale poiché oggi sempre più attività vengono svolte e gestite tramite dispositivi telefonici, computer o comunque tramite la rete Internet; pertanto anche la prova ha necessità sempre più spesso di essere acquisita nell'ambito dei dati digitali, delle più diverse tipologie, che vengono allocati da tutti noi quotidianamente nei sistemi informatici[2].

[1] PITTIRUTI, *Digital evidence e procedimento penale*, Torino, 2017, 2.

[2] Prima dell'entrata in vigore della l. 48/2008, la Cassazione affermava che «la legge 23 dicembre 1993, n. 547, che ha introdotto nel codice penale i cosiddetti *computer crimes*, non definisce il sistema informatico, oggetto della sua tutela, dandone per presupposta la nozione. Sulla base del dato testuale pare, comunque, che si debba ritenere che l'espressione "sistema informatico" contenga in sé il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso

Con l'evolversi della tecnologia, si sono rese necessarie pertanto, anche nel diritto penale italiano, diverse riforme, a partire dalla legge 23 dicembre 1993, n. 547 in tema di criminalità informatica fino a giungere alla legge 18 marzo 2008, n. 48 recante la ratifica della Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica del 23 novembre 2001[3].

Un aspetto fondamentale di quest'ultima riforma è senza dubbio l'introduzione nel nostro ordinamento, veicolata tramite la modifica di diverse disposizioni del libro III e V del codice di procedura penale, delle *best practices*: cioè di quel comportamento, non necessariamente codificato o contenuto in manuali, che è ritenuto dalla comunità scientifica e dagli operatori tecnici come la modalità corretta per effettuare determinate operazioni informatiche su specifici dispositivi o supporti. Un altro elemento particolarmente significativo, per quel che qui interessa, introdotto in sede di riforma, consiste nella preservazione della *chain of custody*, cioè della necessità di tenere traccia del procedimento di raccolta, acquisizione ed analisi della *digital evidence* attraverso *report*, così da potersi escludere, al momento dell'ammissione della prova, l'ipotesi di alterazioni indebite dei dati digitali intervenute successivamente alla creazione, trasmissione o allocazione in un altro supporto.

Nel compiere, quindi, ispezioni, perquisizioni e sequestri al fine di acquisire al processo penale dei dati digitali, conservati sul territorio italiano, è ormai dato positivo che le autorità inquirenti dovranno rispettare le *best practices*, così come previste dal legislatore nel 2008, riassumibili in una serie di principi guida: «adottare estrema cautela nel sequestrare computer o servizi informatici che muovono servizi di telecomunicazione critici, e prediligere, se possibile, la continuità aziendale effettuando copie su supporti adeguati e non interrompendo, così, l'azione delle macchine e dei servizi; prestare attenzione a non alterare i dati durante le operazioni di ricerca delle fonti di prova; quando si effettua una duplicazione, assicurarsi che siano garantite la conformità della copia all'originale e la sua immodificabilità. Corrette modalità di conservazione, procedure di duplicazione efficaci, garanzie di non alterabilità

---

l'utilizzazione (anche in parte) di tecnologie informatiche. Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o "memorizzazione"), per mezzo di impulsi elettronici, su supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bit*) numerici ("codice"), in combinazioni diverse: tali "dati", elaborati automaticamente dalla macchina, generano le informazioni costituite "da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente"», in Cass., Sez. VI, 14 dicembre 1999, (c.c. 4 ottobre 1999), P. M. e Piersanti N., n. 3067.

[3] Cfr. LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa, Legge 18 marzo 2008, n. 48. I profili processuali,* in *Dir. pen. proc.,* 2008, 6.

ed *extrema ratio* del sequestro di servizi sono, in conclusione, i quattro principi della *forensics* introdotti nel nostro ordinamento»[4].

2. La violazione delle best practices nell'acquisizione della prova digitale raccolta in Italia.

Dottrina e giurisprudenza hanno dibattuto circa la sanzione processuale conseguente ad un'acquisizione di *digital evidence* senza il rispetto delle *best practices*; ciò a causa di una mancata previsione esplicita al riguardo da parte della l. 48/2008. Una dottrina minoritaria[5] ha sostenuto la possibilità di ricomprendere l'invalidità della *digital evidence* nella nullità, ai sensi dell'art. 178, lett. c) c.p.p.: tale tesi è stata però contrastata affermando come la suddetta nullità non afferisce «alla metodologia di acquisizione probatoria e di conservazione degli elementi raccolti in materia informatica»[6], in ciò confortati anche dalla Corte di cassazione[7]. Altro orientamento vede come sede privilegiata, per un giudizio sulle modalità acquisitive operate dagli investigatori o dalla difesa durante le indagini preliminari, quella prevista dall'art. 192 c.p.p.[8], ma la dottrina più avvertita ha posto in evidenza come una simile ricostruzione porterebbe a delle valutazioni erronee da parte del giudice, dato che il suo libero convincimento sarebbe influenzato da prove raccolte in maniera erronea[9].

---

[4] ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano*, in *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)* a cura di Luparia, Milano, 2009, 170. Approfondisce la materia MATTIUCCI, *Le indagini sui reperti invisibili. High tech crime*, in *Manuale delle investigazioni sulla scena del crimine*, a cura di Curtotti, Saravo, Torino, 2013.

[5] VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. internet*, 2008, p. 509.

[6] BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici,* in *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)* a cura di Luparia, Milano, 2009, p. 190.

[7] Cass., Sez. IV, 28 giugno 2016, Grassi ed altri, in *CED Cass.* n. 268228, n. 40903, secondo cui «non v'è alcuna norma di legge che sanzioni con la nullità tali violazioni né le stesse rientrano fra le nullità di ordine generale di cui all'articolo 178 c.p.p.».

[8] Tra gli altri DANIELE, *La prova digitale nel processo penale,* in *Riv. dir. proc.,* 2011, 288 ss., nonché CAJANI, *Il vaglio dibattimentale della digital evidence*, in *questa Rivista,* 3, 2013, BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, cit., 91. Nella giurisprudenza di merito, è particolarmente rilevante Trib. Bologna, 22 dicembre 2005, n. 1823, in *Dir. Internet*, 2005, con nota di LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali.*

[9] MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.,* 2011, 4517, secondo cui le prove acquisite senza rispettare i principi relativi alla salvaguardia dell'integrità della prova digitale, non «possono, sulla base di un malinteso utilizzo della categoria degli indizi, concorrere alla formazione del libero convincimento del giudice». In questo senso, vedi anche LORENZETTO, *Le attività urgenti di investigazione informatica e telematica,* in *Sistema penale e criminalità informatica. Profili sostanziali e proces-*

Da ultimo, è necessario porre in evidenza come la dottrina ha valutato la possibilità di ricomprendere l'invalidità della prova digitale nella *species* dell'inutilizzabilità: «occorre prendere atto della necessità di una diversa ricostruzione sistematica della nozione di inutilizzabilità. In presenza di prove informatiche, eventuali violazioni relative alla modalità di formazione della prova incidono necessariamente anche sulla sostanza della prova stessa, fino a rendere del tutto inattendibile l'accertamento frutto di tali risultanze»[10].
In tal senso, infatti, è possibile considerare i canoni di genuinità e non alterazione della prova previsti dalla l. 48/2008 non come «mere indicazioni operative prive di alcuna sanzione, ma veri e propri divieti impliciti presidiati dalla sanzione dell'inutilizzabilità»[11].
Tali divieti probatori impliciti sono identificabili, quindi, secondo tale convincente prospettazione, nei criteri operativi indicati dal legislatore nel codice di procedura penale agli articoli 244, comma 2, 247, comma 1-*bis*, 352, comma 1-*bis*, 354, comma 2, 254-*bis* e 260, comma 2: essi impongono, quindi, a pena di inutilizzabilità, di adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione e di acquisire i dati digitali mediante una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità[12].

3. L'acquisizione all'estero della *digital evidence*.

Tuttavia, accade molto spesso che i dati digitali siano immagazzinati su *server* allocati al di fuori del territorio italiano: si pensi, tra gli altri, ai dati che immettiamo nei social network. Ciò comporta che, in linea generale, nel momento in cui tali dati debbano essere acquisiti al procedimento penale, gli inquirenti dovranno servirsi degli strumenti di cooperazione giudiziaria, per richiedere ad uno Stato estero di acquisire la prova digitale[13].

---

suali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48) a cura di Luparia, Milano, 2009, 162, secondo la quale si opererebbe, così, «una compensazione impropria tra grandezze eterogenee, ritenendo sufficiente la presenza di imprecisati elementi di riscontro per colmare il *deficit* tecnico che ha pregiudicato l'integrità del risultato dell'operazione di acquisizione».

[10] MARAFIOTI, *Digital evidence*, cit., 4517.

[11] PITTIRUTI, *Digital evidence e procedimento penale*, cit., 159. Per quanto concerne la giurisprudenza di legittimità, vedi in senso conforme Cass., Sez. un., 16 maggio 1996, Sala, in *Cass. pen.,* 1996, 3268 ed in senso difforme Cass., Sez. IV, 28 giugno 2016, Grassi ed altri, in *CED Cass.* n. 268228, n. 40903.

[12] In questo senso MARANDOLA, *Le invalidità processuali*, Torino, 2015, 130.

[13] Vi sono casi in cui, invece, non sarà necessario ricorrere ai mezzi della cooperazione internazionale, ma l'autorità giudiziaria potrà acquisire i dati digitali conservati all'estero tramite gli ordinari mezzi di ricerca della prova previsti nel codice di rito. Un primo caso è quello dell'acquisizione dei messaggi scambiati tra dispositivi Blackberry, criptati tramite sistema *pin to pin*: sul tema vedi TROGU, *Come si intercettano le chat pin to pin tra dispositivi Blackberry?,* in *Proc. pen. giust.,* 2016; FILIPPI, *Questioni*

Oggi l'acquisizione della prova digitale all'estero può effettuarsi tramite due differenti strumenti: la rogatoria all'estero e l'ordine europeo di indagine penale.
In materia di cooperazione giudiziaria vi è sempre la necessità di contemperare due contrapposte esigenze: da una parte, vi è la necessità di favorire la cooperazione internazionale in materia penale, superando formalismi superflui e agevolando quanto più possibile lo scambio di informazioni e di atti processuali tra le autorità di Stati diversi; dall'altra parte, vi sono i principi fondamentali e irrinunciabili del giusto processo, disciplinato nella Costituzione italiana all'art. 111, che esigono una formazione della prova il più possibile certa e trasparente, in particolar modo nel procedimento penale. Nel tempo, conseguentemente, ogni normativa nazionale e internazionale in tema di cooperazione giudiziaria ha tentato di individuare il miglior equilibrio tra tali esigenze.
Nel corso del 2017, il legislatore è intervenuto in modo significativo in tale ambito, emanando, in un primo momento, il D.Lgs. 21 giugno 2017, n. 108, in attuazione della direttiva 2014/41/UE, contenente la disciplina dell'ordine europeo di indagine penale. In un secondo momento, con il D.Lgs. 3 ottobre 2017, n. 149 è stato riformato il libro XI del codice di procedura penale, in tema di estradizione e di rapporti con le autorità giurisdizionali estere.
La disciplina della cooperazione giudiziaria internazionale, grazie a questi recenti interventi normativi, ha subito notevoli mutamenti, realizzando un nuovo equilibrio tra l'esigenza di favorire la collaborazione fra gli Stati e l'esigenza di garantire il rispetto dei principi fondamentali in tema di giusto processo, in particolare in ordine al tema dell'invalidità nell'acquisizione della prova.

4. La violazione delle *best practices* nelle operazioni compiute all'estero attraverso rogatoria.

---

nuove in tema di intercettazioni: quid iuris sul "pin to pin" dei Blackberry?, in *questa Rivista,* n. 1, 2016; TESTAGUZZA, *Chat Blackberry: il sistema "pin to pin". Nascita di un nuovo paradiso processuale*, *ivi,* fasc. 1, 2016; PITTELLI-COSTARELLA, *Ancora in tema di chat "pin to pin" su sistema telefonico Blackberry*, *ivi*, n.1, 2016; FURFARO, *Le intercettazioni "pin to pin" del sistema blackberry, ovvero: quando il vizio di informazione tecnica porta a conclusioni univoche*, in *questa Rivista*, 1, 2016; PARODI, *Intercettazioni di Blackberry: una risposta e molte altre domande*, in *Ilpenalista.it*, fasc. 28, 2016. Una seconda ipotesi è quella dell'acquisizione dei dati digitali immessi nei *cloud* con server allocati all'estero: per un approfondimento sul tema si vedano ATERNO-MATTIUCCI, *Cloud forensics e nuove frontiere delle indagini informatiche nel processo penale*, in *questa Rivista*, 3, 2013, nonché RUOTOLO, *Hey! You! Get Off My Cloud!*, *ivi*, 3, 2013.

Per analizzare quali mutamenti abbia comportato la riforma operata con il D. Lgs. 149/2017 nell'acquisizione dei dati digitali tramite lo strumento rogatoriale è necessario accennare innanzitutto alla disciplina precedente.
La struttura previgente dell'art. 729 c.p.p., rubricato «utilizzabilità degli atti assunti per rogatoria», stabiliva quattro diverse ipotesi di inutilizzabilità[14]: innanzitutto, qualora lo Stato estero avesse posto delle condizioni all'utilizzabilità degli atti richiesti, l'autorità giudiziaria italiana sarebbe stata vincolata dalla legge al rispetto delle condizioni stesse a pena di inutilizzabilità, ai sensi del secondo comma dell'art. 729 c.p.p.; non erano utilizzabili, poi, gli atti acquisiti o trasmessi in violazione dell'art. 696 c.p.p.; la sanzione dell'inutilizzabilità, inoltre, era prevista dall'art. 729, comma 1-*bis* c.p.p., nel caso in cui lo Stato estero avesse dato esecuzione alla rogatoria con modalità diverse da quelle indicate dall'autorità giudiziaria italiana; un'ultima ipotesi di inutilizzabilità era prevista per le dichiarazioni aventi ad oggetto il contenuto degli atti assunti mediante rogatoria, ma inutilizzabili.
L'art. 729 c.p.p. è stato, come detto, riformato nel 2017; ad oggi, tale articolo stabilisce: «nei casi in cui lo Stato estero abbia posto condizioni all'utilizzabilità degli atti richiesti, l'autorità giudiziaria è vincolata al rispetto di tali condizioni. Se lo Stato estero dà esecuzione alla richiesta di assistenza con modalità diverse da quelle indicate dall'autorità giudiziaria ai sensi dell'articolo 727, comma 9, gli atti compiuti sono inutilizzabili solo nei casi in cui l'inutilizzabilità è prevista dalla legge. Non possono in ogni caso essere utilizzate le dichiarazioni, da chiunque rese, aventi ad oggetto il contenuto di atti inutilizzabili. Si applica la disposizione dell'articolo 191, comma 2».
Tale disposizione enuclea, al primo comma, la regola della specialità, che è un corollario del principio per cui ogni Stato ha il potere sovrano di regolare il compimento di atti giurisdizionali sul proprio territorio e del correlativo divieto per altri Stati di esercitare la giurisdizione sul suolo straniero. Essa stabilisce che la prova acquisita mediante rogatoria non possa essere utilizzata dallo Stato assistito in procedimenti diversi da quello per il quale è stata richiesta e acquisita dall'autorità assistente.
Inoltre, al secondo comma, viene stabilito che qualora, a norma di accordi internazionali, la domanda di assistenza giudiziaria possa essere eseguita secondo modalità previste dall'ordinamento dello Stato, l'autorità giudiziaria deve indicare gli elementi necessari per l'utilizzazione processuale degli atti richiesti. La lettera della legge è chiara nel non attribuire rilevanza ad ogni re-

[14]Approfondisce il tema PAOLUCCI, *Cooperazione giudiziaria e di polizia in materia penale*, Torino, 2011, 132 ss.

gola di assunzione, ma solo agli elementi necessari per l'utilizzazione. Sarebbe infatti irragionevole sanzionare con l'inutilizzabilità una prova che, se assunta nel territorio dello Stato, sarebbe giudicata meramente irregolare.
Si deve rilevare, a questo punto, come l'art. 729 c.p.p., come riformato nel 2017, ha una significativa incidenza nelle richieste rogatoriali di acquisizione della *digital evidence*. Infatti, si noti come nella normativa previgente, il comma 1-*bis* prevedeva la sanzione dell'inutilizzabilità nel processo penale italiano per la prova digitale acquisita con modalità diverse da quelle indicate dall'autorità giudiziaria italiana: ciò comportava due conseguenze rilevanti.
In primo luogo, che l'inutilizzabilità discendesse da parametri individuati dagli inquirenti all'interno della singola richiesta di rogatoria; l'autorità richiedente avrebbe potuto indicare tutele minime dal punto di vista della genuinità del dato digitale e con riguardo agli atti di acquisizione, senza pretendere il rispetto delle *best practices* e della *chain of custody*, così come previsto secondo la più autorevole dottrina e l'orientamento giurisprudenziale delle Sezioni Unite[15].
In secondo luogo, non sarebbe stata garantita la certezza e l'uniformità del diritto, dato che ogni autorità giudiziaria avrebbe potuto richiedere tutele e condizioni di volta in volta differenti nella richiesta di acquisizione del dato digitale.
La nuova disciplina codicistica, invece, garantisce maggiore certezza ed uniformità ai contenuti delle rogatorie inviate dall'Italia all'estero. Infatti, il secondo comma dell'art. 729 c.p.p. prevede che, a seguito dell'indicazione nella richiesta rogatoriale di particolari condizioni volte a garantire la genuinità e l'autenticità del dato digitale, «gli atti compiuti sono inutilizzabili solo nei casi in cui l'inutilizzabilità è prevista dalla legge». Quindi, solo nel caso in cui l'eventuale scostamento della condotta tenuta dall'autorità straniera nell'acquisire il dato digitale sia sanzionato in Italia con l'inutilizzabilità, allora la *digital evidence* non potrà essere posta alla base della decisione, non essendo permesso il suo ingresso nel dibattimento. Se, dunque, l'autorità italiana richiedente ponga delle condizioni particolarissime di acquisizione e conservazione del dato digitale, che, tuttavia, non siano considerabili nel nostro ordinamento come cause di inutilizzabilità, l'eventuale violazione di tali condizioni sembra corretto ritenere che comporterà delle mere "irregolarità", che nella disciplina ante 2017 non erano configurabili.
Comparando tale conclusione con quella riguardante l'invalidità dell'acquisizione del dato digitale mediante i mezzi di ricerca della prova, è

[15] *Supra*, § 2.

possibile evidenziare l'omogeneità delle sanzioni previste nel nostro ordinamento: precisamente, in entrambi i casi l'acquisizione dovrà rispettare le *best practices* e la *chain of custody*, introdotte nel nostro ordinamento, come noto, con la l. 48/2008. Al contrario, con la disciplina precedente, vi era una sfasatura nelle sanzioni, a causa della mancata applicabilità delle cause di inutilizzabilità della prova digitale alle acquisizioni di essa all'estero mediante rogatoria internazionale.

5. La violazione delle best practices nelle operazioni compiute all'estero attraverso l'ordine europeo di indagine.

Quanto all'ordine europeo di indagine e alle invalidità conseguenti all'acquisizione della *digital evidence*, è necessario analizzare come tale materia sia stata disciplinata nel D. Lgs. 108/2017. La norma fondamentale è l'art. 33 del decreto attuativo, la quale al comma primo stabilisce che «l'autorità giudiziaria che ha emesso l'ordine europeo di indagine concorda con l'autorità di esecuzione le modalità di compimento dell'atto di indagine o di prova, specificamente indicando i diritti e le facoltà riconosciuti dalla legge alle parti e ai loro difensori». Si noti come venga lasciata ampia discrezionalità all'autorità giudiziaria con riguardo alle modalità istruttorie da inserire all'interno dell'OEI. Potranno, quindi, essere inserite precise modalità di esecuzione delle operazioni di acquisizione della *digital evidence*, richiedendo il rispetto delle procedure e dei protocolli adottati nell'ordinamento italiano. Si sostiene, inoltre, che, sulla base di un'interpretazione sistematica degli artt. 1 e 33 del D. Lgs. 108/2017, «l'autorità di emissione dovrebbe domandare all'autorità di esecuzione di adottare le modalità previste a pena di inutilizzabilità dalla *lex fori*»[16].

La dottrina, tentando di comprendere se, nello Stato di emissione, sia possibile, una volta che la prova sia stata raccolta e trasferita, eccepirne l'invalidità invocando gli errori occorsi durante la fase esecutiva, perviene a soluzioni simili all'orientamento precedentemente riportato: si propende per «una efficacia extraterritoriale della *lex fori*: è dunque da un certo punto di vista inevitabile che violazioni commesse nel momento della formazione del dato probatorio, che poi dovrà essere trasferito nello Stato di emissione, possano essere eccepite nel procedimento principale, e condurre, davanti alla autorità che ha adottato l'OEI, alla esclusione della prova illegittimamente formata»[17]. Vale a dire, quindi, che la prova digitale acquisita senza l'osservanza delle modalità e

[16] DANIELE, *L'ordine europeo di indagine penale entra a regime*, cit., 213.
[17] CAIANIELLO, *L'attuazione della direttiva sull'ordine europeo di indagine*, cit., 2203.

delle condizioni imposte dallo Stato italiano non potrà essere posta a base di un provvedimento giurisdizionale. A conforto di tale ipotesi interpretativa, infatti, può essere richiamato il parallelo art. 729, comma 2 c.p.p., giungendo così ad individuare l'inutilizzabilità come sanzione per l'invalidità dell'atto ottenuto tramite OEI.

A quanto detto sinora deve aggiungersi la nuova possibilità di eccepire di fronte al giudice italiano l'invalidità della prova digitale acquisita tramite OEI, che sembra ulteriormente confermata dall'art. 28 del D. Lgs. 108/2017, che attua l'art. 14 della direttiva 2014/41/UE, che al secondo comma prevede l'impugnazione delle ragioni di merito dell'emissione dell'OEI. L'art. 28 del decreto ha concretizzato questo istituto, stabilendo che «contro l'ordine di indagine avente ad oggetto il sequestro a fini di prova, la persona sottoposta alle indagini o l'imputato, il suo difensore, la persona alla quale la prova o il bene sono stati sequestrati e quella che avrebbe diritto alla loro restituzione, possono proporre richiesta di riesame ai sensi dell'articolo 324 del codice di procedura penale». È possibile, quindi, contestare di fronte al giudice «non solo le modalità di esecuzione, ma anche i presupposti di merito del sequestro»[18]: in concreto, quindi, le parti potranno eccepire i vizi di validità della *digital evidence* attraverso questo nuovo istituto previsto dal legislatore.

Infine, è necessario evidenziare il contenuto dell'art. 36 del D. Lgs. 108/2017 che prevede l'inserimento all'interno del fascicolo per il dibattimento, disciplinato dall'art. 431 c.p.p., delle prove acquisite con OEI ed in particolare i documenti ed i verbali degli atti non ripetibili, nonché i verbali degli atti ripetibili cui il difensore è stato posto in grado di assistere e di esercitare le facoltà a lui consentite dalla legge italiana. Ciò rende tali prove direttamente utilizzabili.

Concludendo sul punto, occorre evidenziare come il nuovo sistema istituito dall'OEI ha comportato dei mutamenti nell'equilibrio tra *lex fori* e *lex loci*, riguardo all'applicabilità delle due normative alle operazioni di acquisizione della *digital evidence*. Il meccanismo instaurato dalla direttiva 2014/41/UE permette di applicare anche in ambito extraterritoriale la *lex fori*, vale a dire la legge italiana; tuttavia, come evidenziato, vi sono dei limiti. Entrambi gli ordinamenti in gioco devono tendere a realizzare «un gioco di sintesi e semplificazione»[19] tra *lex loci* e *lex fori*. Da un lato, l'autorità di emissione deve indicare in modo dettagliato le forme e i protocolli da seguire, al fine di evitare che la prova digitale, una volta acquisita, sia inutilizzabile nell'ordinamento di

[18] DANIELE, *L'ordine europeo di indagine penale entra a regime*, cit., 213.
[19] CAIANIELLO, *L'attuazione della direttiva sull'ordine europeo di indagine penale*, cit., 2202.

destinazione. Dall'altro lato, l'autorità che esegue l'ordine di indagine penale è sollecitata ad adattare il proprio *modus operandi* alle forme processuali e operative indicate dallo Stato di emissione, a meno che la richiesta così effettuata contrasti con i principi fondamentali del proprio ordinamento. Autorevole dottrina[20] ha asserito che si tratta di una forma ibrida tra *lex loci* e *lex fori*, che ha l'intento «di contemperare le esigenze procedimentali dello Stato di emissione con il rispetto della sovranità dello Stato di esecuzione»[21].

6. Conclusioni.

Sembra potersi affermare, da una lettura complessiva della disciplina dell'acquisizione all'estero della *digital evidence* tramite i novellati strumenti di cooperazione internazionale, come le *best practices,* previste all'interno del codice di procedura penale italiano, siano rilevanti anche nella raccolta transfrontaliera della *digital evidence*. Inoltre, nel momento in cui si proceda all'acquisizione dei dati digitali conservati all'estero, tramite rogatoria ed OEI, violando le *best practices*, la sanzione processuale conseguente non potrà che essere quella dell'inutilizzabilità.

Infatti, la patologia dell'acquisizione della prova digitale all'estero, pur basata su parametri normativi eterogenei, non sembra dover mutare, sia essa avvenuta tramite la rogatoria all'estero o l'ordine europeo di indagine penale. Il rispetto delle *best practices* sembra, pertanto, ormai costituire canone ineludibile per una piena utilizzabilità processuale del dato digitale ovunque esso venga acquisito.

[20] MARAFIOTI, O*rizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, in *L'ordine europeo di indagine. Criticità e prospettive*, a cura di Bene, Marafioti, Luparia, Torino, 2016, 22.
[21] DANIELE, *L'impatto dell'ordine europeo di indagine penale*, cit., 70.