UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

DIPARTIMENTO JONICO IN SISTEMI GIURIDICI ED ECONOMICI DEL MEDITERRANEO SOCIETÀ, AMBIENTE, CULTURE
IONIAN DEPARTMENT OF LAW, ECONOMICS AND ENVIRONMENT

ANNO IX

ANNALI 2021 DEL DIPARTIMENTO JONICO

ESTRATTO

LORENZO PULITO

Il sequestro dei nuovi beni immateriali: dalla piattaforma al token

http://edizionidjsge.uniba.it/ • ISBN - 9788894503074

EDIZIONI JSGE

Contatti:
Dipartimento Jonico in Sistemi Giuridici ed Economici del Mediterraneo: Società, Ambiente, Culture
Convento San Francesco - Via Duomo, 259 - 74123 Taranto, Italy
e-mail: annali.dipartimentojonico@uniba.it
telefono: + 39 099 372382 • fax: + 39 099
7340595
https://www.uniba.it/ricerca/dipartimenti/sistemi-giuridici-ed-economici/edizioni-digitali

ANNO IX

ANNALI 2021
DEL DIPARTIMENTO JONICO

EDIZIONI SGE

Lorenzo Pulito

IL SEQUESTRO DEI NUOVI BENI IMMATERIALI: DALLA PIATTAFORMA AL TOKEN*

ABSTRACT

Nel dischiudere prospettive inedite alle forme del crimine, la rivoluzione digitale – prolifica di piattaforme e token - pone nuove sfide anche sul versante dei sequestri. L'impatto delle ICT su strategie e strumenti di indagine penale è stato solo in parte oggetto di attenzione legislativa. Gli strumenti ablatori partoriti dal progresso tecnologico sono rimasti, per lo più, affidati a prassi e protocolli più o meno attendibili o ad utilizzi "atipici" dell'istituto normato. I silenzi legislativi e le pratiche giudiziarie indicano una tendenza a valorizzare la libertà investigativa attraverso metodi di cui non sempre sono verificabili idoneità tecnica e margini di affidabilità e che incidono sui diritti fondamentali della persona, che devono essere il punto di partenza per l'avanzamento della conoscenza del settore e soprattutto lo stimolo per iniziative legislative di rivisitazione complessiva della materia.

In disclosing unprecedented perspectives on the forms of crime, the digital revolution – prolific of platforms and tokens – poses new challenges also in terms of seizures. The impact of ICT on criminal investigation strategies and tools has been only partially subject of legislative attention. Nevertheless, the ablator instruments derived from the technological progress are mainly consigned to more or less reliable practices and protocols or to "atypical" uses of the regulated institute. Legislative silence and judicial practices indicate the tendency to boost the freedom of investigation using methods for which it is not always possible to verify the technical suitability and the margins of reliability, and which affect the fundamental rights of the person. The fundamental rights of the person shall be the starting point for any advancement of knowledge in the field and foremost the stimulus to legislative initiatives revisiting the subject overall.

PAROLE CHIAVE

Sequestro – piattaforme – token

Seizure – platforms – tokens

1. Accostare sequestri penali e beni immateriali tempo fa rappresentava un ossimoro.

* Saggio sottoposto a revisione secondo il sistema per *peer review*

In un decreto della Corte di Appello di Genova risalente all'anno 1962, premettendosi come il sequestro penale potesse essere adottato su beni dotati di «corporalità» ovvero su «oggetti o entità corporali aventi un'esistenza nel mondo fisico», veniva dichiarata l'inesistenza di un sequestro disposto *ex* art. 337 dell'allora vigente codice di rito sulle quote di una s.r.l., in base al rilievo che queste ultime fossero beni immateriali[1].

Parole che oggi ci inducono a sorridere.

Certo, anche gli istituti del "Codice Vassalli" diretti all'acquisizione probatoria sono stati pensati per un mondo in cui non esistevano "oggetti" immateriali, separabili e replicabili dal loro *corpus mechanicum*[2].

Ma, come ha recentemente ricordato la Corte di cassazione, attualmente «... ogni dubbio è ormai superato perché la legge 48/2008 […] ha reso esplicito nell'ordinamento penale che il concetto di "cosa" copre anche il dato informatico in quanto tale»[3].

La l. 18 marzo 2008, n. 48[4], come noto, ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2001, e ha introdotto per la prima volta in Italia una disciplina specifica in tema di acquisizione degli elementi di prova digitali grazie alla modifica degli articoli in materia di perquisizione, sequestro, acquisizione e conservazione dei dati presenti su supporti informatici.

In linea con la suddetta Convenzione[5], gran parte delle modifiche apportate al codice di rito hanno assimilato il dato informatico alle "cose".

---

[1] Il provvedimento viene richiamato da R. Nitti, *Quando il giudice penale sequestra la partecipazione societaria,* in *www.questionegiustizia.it,* 16 dicembre 2015.

[2] A. Monti, *Casi e problemi sul sequestro informatico anche a distanza,* in G. Cassano, S. Previti (a cura di), *Il diritto di internet nell'era internet,* Giuffrè, Milano 2020, p. 983 s.

[3] Cass. pen., Sez. VI, 24 febbraio 2015, n. 24617, in *www.penalecontemporaneo.it*, 23 luglio 2015, con nota di F. Cerqua, *Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica*.

[4] Per un inquadramento generale sulla l. n. 48/2008 si rimanda ai numerosi commenti, tra i quali S. Aterno, *Sub* art. 8, in G. Corasaniti, G. Corrias Lucente (a cura di), *Cybercrime, responsabilità degli enti, prova digitale*, Cedam, Padova 2009, p. 194 ss.; S. Aterno, M. Cuniberti, G.B. Gallus, F.P. Micozzi, *Commento alla legge di ratifica della convenzione di Budapest del 23 novembre 2001*, in *www.procura.milano.giustizia.it/files/commento-budapest.pdf*; M.L. Di Bitonto, A. Vitale, A. Macrillò, A. Barbieri, E. Forlani, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime: profili processuali*, in *Dir. Internet*, 5, 2008, p. 503 ss.; L. Luparia, *La ratifica della convenzione sul cyber crime del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 6, 2008, p. 717 ss.; L. Picotti, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*. *Profili di diritto penale sostanziale*, ivi, p. 700 ss.; G. Resta, *La disciplina acquista maggiore organicità per rispondere alle esigenze applicative*, in *Guida dir.,* 16, 2008, p. 52; E. Selvaggi, *Cooperazione giudiziaria veloce ed efficace*, in *Guida dir*., 16, 2018, p. 72. Per riferimenti tecnici, oltre che giuridici, si veda S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco, *Manuale di Computer Forensics*, Experta, Forlì 2011, *passim*.

[5] La Convenzione sui crimini informatici ha inteso disciplinare i "dati" di per sé come "cosa", considerandoli oggetto di sequestro, come si ricava dal punto 197 della relazione esplicativa in cui è chiarito che «"sequestrare" significa prendere il mezzo fisico sul quale i dati o le informazioni sono registrati oppure fare e trattenere una copia di tali dati o informazioni. "Sequestrare" include l'uso o il sequestro di programmi necessari ad accedere ai dati che si stanno sequestrando. Allo stesso modo in

2. L'evoluzione tecnologica ha collocato i sequestri penali (probatorio e preventivo particolarmente) in una nuova dimensione, non più unicamente commisurata sulla realtà fisica. La scienza ha impresso al processo un'accelerazione eccezionale, determinando l'inversione dell'ordine tradizionale delle attività di indagine[6] e il mutamento delle coordinate concettuali di alcuni istituti, adattati a recepire nuovi contenuti per intervento del legislatore.

Venendo alle "integrazioni" normative riguardanti il codice di procedura penale registrate in materia di ispezioni, perquisizioni e sequestri[7] (anche ad opera del personale di polizia giudiziaria), come apportate dalla suindicata legge, le stesse possono sintetizzarsi come appresso[8].

Con riferimento all'ispezione l'intervento normativo ha ampliato la tradizionale tipologia codicistica, da sempre fondata sull'entità materiale oggetto di ricerca (luoghi, cose o persone), inserendo all'art. 244, comma 2, c.p.p. un riferimento esplicito ai sistemi informatici o telematici, in relazione ai quali l'autorità giudiziaria può disporre rilievi ed altre operazioni tecniche; con riferimento alla perquisizione, l'art. 247, comma 1-*bis* c.p.p. prevede analoghi accorgimenti nel consentire la perquisizione di un sistema informatico o telematico, anche se protetto da misure di sicurezza, quando vi è fondato motivo di ritenere che in essi si trovino dati, informazioni, programmi informatici o tracce comunque pertinenti al reato (allo stesso modo può procedervi la polizia giudiziaria ai sensi dell'art. 352, comma 1-*bis*, c.p.p.). L'art. 254-*bis* c.p.p., nel disciplinare il sequestro di dati informatici presso fornitori di servizi, consente all'autorità giudiziaria di stabilire, per esigenze legate alla loro regolare fornitura, che l'acquisizione avvenga mediante copia dei dati su adeguato supporto, con una procedura che assicuri la conformità di quelli acquisiti a quelli originali e la loro immodificabilità[9], ordinandosi, in tale ipotesi, allo stesso fornitore, l'adozione delle

---

cui si usa il termine tradizionale "sequestrare", il termine "assicurare in modo simile" è incluso per indicare gli altri modi nei quali i dati intangibili possono essere portati via, resi inaccessibili o il suo controllo è in altro modo escluso per il sistema informatico».

[6] Nelle indagini informatiche il sequestro del dispositivo informatico o elettronico ben può anticipare la perquisizione, che, invece, nelle indagini tradizionali precede, cronologicamente e logicamente, il sequestro. Sull'impossibilità di individuare un preciso *iter* delle indagini informatiche, improntate su un criterio di utilità relativo al reato da accertare e all'elemento di prova digitale da ricercare v. M. Pittiruti, *Digital evidence e procedimento penale*, Giappichelli, Torino 2017, p. 6.

[7] Il tema del "sequestro informatico" è stato recentemente trattato da D. Curtotti, *Il sequestro*, in Aa.Vv., Cyber forensic *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Giappichelli, Torino 2021, p. 457 ss.

[8] Per un inquadramento generale su ispezioni, perquisizioni e sequestri v. A. Bernasconi, *Mezzi di ricerca della prova*, in A. Bernasconi, A. De Caro, A. Furgiele, M. Menna, C. Pansini, A. Scalfati, N. Triggiani, C. Valentini, *Manuale di diritto processuale penale*, III ed., Giappichelli, Torino 2018, p. 299 ss.

[9] Secondo M. Senor, *Informatica forense*, in M. Durante, U. Pagallo (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet, Torino 2012, p. 251, la positivizzazione delle prassi (non standardizzate) di *computer forensics* ha rappresentato «una felice evoluzione culturale dell'informatica forense» in grado di assicurare un maggior rispetto dei diritti di difesa.

cautele necessarie a conservarli e proteggerli in maniera adeguata; l'art. 260, comma 2, c.p.p. prescrive che, quando si tratti di dati, informazioni o programmi informatici, la copia debba essere realizzata su adeguati supporti, mediante una procedura che assicuri la conformità della stessa all'originale e la sua immodificabilità[10]; infine, l'art. 354, comma 2, c.p.p., disciplinando gli accertamenti urgenti dal parte della polizia giudiziaria, richiede l'adozione di misure tecniche ovvero l'imposizione delle prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso, prevedendo altresì che, ove possibile, la stessa si occupi di provvedere alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità[11].

I canoni così introdotti – variamente enunciati in diverse disposizioni del codice – sono «in ultimo riassumibili nell'endiadi genuinità e immodificabilità»[12].

La "scissione" del *corpus mysticum* dal *corpus mechanicum*, con la connessa replicabilità in infinite copie del contenuto rappresentativo originario e la volatilità del processo di duplicazione, hanno fatto avvertire la necessità di rispettare una corretta "catena di custodia" e di interrogarsi sulle conseguenze processuali della mancata osservanza della stessa nella gestione dei reperti informatici, dando vita a un dibattito che vede contrapposti i sostenitori dell'inutilizzabilità di dati e informazioni assicurate al processo in assenza del rispetto di *best practices* nell'esecuzione del sequestro informatico e delle successive analisi a quelli che, invece, propendono per la inattendibilità dei risultati[13].

La tecnica adoperata dalla l. n. 48 del 2008 è stata quella di eseguire una sorta di *upgrade* degli istituti tradizionali, circostanza che ha comportato l'insorgenza di numerose questioni interpretative, la cui risoluzione diventa più complicata per effetto

[10] Si tratta della c.d. "copia-clone", che consente la restituzione del materiale informatico in sequestro (o meglio di una copia di esso). In dottrina si sottolinea come la clonazione delle tracce informatiche non sia soltanto una semplice conservazione di tracce, ma un vero sequestro di materiale conoscitivo che, pertanto, va assoggettato alle regole del sequestro e del riesame, indipendentemente dalla sua capacità di essere restituito. Si v. A. Aterno, Digital forensics *e* scena criminis. *Norme, tecniche, scienze, logica*, in D. Curtotti, L. Saravo (a cura di), *Manuale delle investigazioni sulla scena del crimine*, Giappichelli, Torino 2019, p. 775 ss.

[11] Il sequestro di dati, informazioni, programmi, sistemi informatici o telematici, su cui la polizia giudiziaria può compiere rilievi ed accertamenti urgenti, risente all'evidenza della procedura operativa prevista per la duplicazione dei dati indicata nello stesso art. 354, comma 2, c.p.p. e anche nell'art. 254-*bis* c.p.p., a riguardo del sequestro di dati informatici presso un *service provider*. Sul punto, v. S. Venturini, *Sequestro probatorio e fornitori di servizi telematici*, in L. Luparia (a cura di), Internet provider *e giustizia penale*, Giuffrè, Milano 2012, p. 107 ss. Si interroga sulla utilizzabilità del sequestro che faccia seguito ad un accertamento su materiale informatico eseguito senza il rispetto delle procedure indicate nel comma 2 dell'art. 354 c.p.p. D. Curtotti, *Il sequestro*, cit., p. 464 ss.

[12] M. Pittiruti, *Dalla Corte di Cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in *Sist. pen.*, 14 gennaio 2021.

[13] A. Monti, *Casi e problemi sul sequestro informatico anche a distanza*, cit., p. 984. In argomento, C. Conti, *La prova informatica e il mancato rispetto della best practice: lineamenti sistematici sulle conseguenze processuali*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), Cybercrime. *Trattato di diritto penale*, Utet, Torino 2019, p. 1329 ss.

delle criticità operative che discendono dal dato tecnico e – più in generale – per effetto di una certa difficoltà di interazione tra sapere scientifico e sapere giuridico.

Tuttavia, definire l'intervento di mero *restyling* appare ingeneroso, considerata l'indiscutibile incidenza che ne è conseguita sul piano dei principi e delle garanzie difensive.

Se, per il sequestro probatorio, l'obiettivo del legislatore è stato quello di codificare l'esigenza di un'acquisizione conforme alle *best practices* sul confezionamento della *digital evidence*, nessun aggiornamento normativo ha riguardato il sequestro preventivo, le cui finalità cautelari vengono nondimeno raggiunte in "ambito digitale" grazie all'operazione di "riadattamento" dell'istituto forgiata per via giurisprudenziale.

3. L'evoluzione tecnico-scientifica impone all'interprete una riflessione sul bilanciamento tra le esigenze di sicurezza pubblica e di efficienza delle indagini con la tutela dei diritti individuali e delle garanzie processuali.

Diverse le tematiche in gioco e meritevoli di attenzione.

In primo luogo, quella della territorialità: la tecnologia oggi consente di compiere indagini informatiche a distanza dal proprio territorio, senza la necessità di un'attività materiale da parte di un'autorità straniera. In disparte i vantaggi in termini di velocità operativa, tali modalità investigative «mettono in crisi il principio di territorialità che da sempre contraddistingue la cooperazione giudiziaria internazionale, con l'evidente pericolo che vengano eluse le garanzie previste dalla lex loci»[14]. Laddove le indagini a distanza riguardano prove digitali reperibili nel c.d. *cloud* è ancora più evidente il pericolo che si determini la violazione delle garanzie processuali previste dalla *lex loci* e, mancando un preciso sistema nazionale a cui riferirsi, è più marcato il rischio che alla logica della territorialità si sostituisca quella della mera disponibilità[15].

[14] M. Daniele, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), Cybercrime. *Trattato di diritto penale*, cit., p. 1632.

[15] M. Daniele, *La collaborazione internazionale tra autorità investigative*, cit., p. 1635, che riporta: «In evenienze di questo tipo spesso gli organi inquirenti domandano al gestore di indicare il luogo in cui si trovano i dati, con la conseguenza di conferire a quest'ultimo l'abnorme potere di individuare il diritto nazionale da applicare al fine della raccolta delle prove. Sarebbe preferibile, piuttosto, determinare la lex loci da osservare sulla base del luogo in cui il gestore ha la propria sede legale, oppure di quello in cui si fruisce del servizio». Su tali profili problematici v. altresì S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino 2019, p. 199; F. Siracusano, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. pen. giust*., 1, 2017, p. 180. Circa le attività tipiche di indagine condotte sul *cloud* cfr. S. Aterno, Cloud forensics: *aspetti giuridici e tecnici*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), Cybercrime. *Trattato di diritto penale*, cit., p. 1689 ss. Più in generale, circa i problemi dell'acquisizione di dati custoditi in ambiente *cloud* comuni e specifici rispetto all'acquisizione della prova digitale, si rinvia a M. Bontempelli, *Acquisizione di dati custoditi in ambiente* cloud, in A. Scalfati (a cura di), *Le indagini atipiche*, II ed., Giappichelli, Torino 2019, p. 589 ss.

Non va trascurata in materia l'importanza del principio di proporzionalità, che, seppur previsto per le sole misure cautelari[16], ha manifestato portata espansiva lungo tutto il crinale del sistema processuale e capacità di costituire «un utile termine di paragone per lo sviluppo di nuove soluzioni ermeneutiche e, ancor prima, di nuovi modelli di ragionamento giuridico»[17]. Il c.d. *test* di proporzionalità è necessario per ogni tipo di sequestro ma, naturalmente, i termini rispetto ai quali deve essere svolto il relativo scrutinio variano a seconda della natura e della funzione del tipo di sequestro in questione. Rispetto a quello probatorio, il principio di proporzionalità esige la ponderazione tra il contenuto del provvedimento ablatorio e le esigenze di accertamento dei fatti oggetto delle indagini. Se, in astratto, un sequestro *omnibus* disposto dal pubblico ministero potrebbe reputarsi legittimo in casi peculiari, legati alla natura del bene o alla difficoltà di individuazione della *res*, il rischio di acquisizione "casuale" di informazioni "supersensibili" deve trovare adeguata compensazione, in punto di garanzie, grazie a una rigorosa motivazione del provvedimento di sequestro sotto i profili quantitativo (in ordine al nesso di pertinenza tra bene appreso e ipotesi investigativa), qualitativo (in relazione alla tipologia di operazioni tecniche da svolgere sul dato) e temporale (con riguardo alla durata temporale del vincolo)[18]. Ove così non fosse, infatti, l'apposizione del vincolo rischierebbe di trasformarsi in un'operazione esplorativa di ricerca del materiale utile alle indagini del tutto avulsa dai tradizionali schemi codicistici. Nel caso del sequestro preventivo c.d. impeditivo[19], invece, «il giudice deve motivare adeguatamente sulla impossibilità di conseguire il medesimo risultato ricorrendo ad altri e meno invasivi strumenti cautelari ovvero modulando quello disposto - qualora ciò sia possibile - in maniera tale da non compromettere la funzionalità del bene sottoposto a vincolo anche oltre le effettive necessità dettate dall'esigenza cautelare che si intende arginare»[20]. Il principio è stato recentemente riaffermato in un noto caso in cui il ricorrente si doleva dell'indiscriminata estensione del sequestro preventivo, che aveva investivo porzioni dei servizi televisivi rispetto ai quali non ne era stata prospettata la natura diffamatoria[21].

---

[16] Ed applicabili - sebbene i principi di proporzionalità, adeguatezza e gradualità siano dettati dall'art. 275 c.p.p. per le misure cautelari personali - anche alle misure cautelari reali, dovendo il giudice motivare adeguatamente sulla impossibilità di conseguire il medesimo risultato attraverso altri e meno invasivi strumenti cautelari. Sul punto v. Cass. pen., Sez. III, 7 maggio 2014, n. 21271, in *CED Cass*. n. 261509; Cass. pen., Sez. V, 16 gennaio 2013, n. 8382, in *CED Cass*. n. 254712; Cass. pen., Sez. V, 21 gennaio 2010, n. 8152, in *CED Cass*. n. 246103.

[17] M. Caianiello, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. contemp., Riv. Trim.*, 3-4, 2014, p. 145.

[18] M. Pittiruti, *Dalla Corte di Cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, cit.

[19] Su cui vedi *infra*, § 4.

[20] Cass. pen., Sez. V, 16 gennaio 2013, n. 8382, in *CED Cass.* n. 254712

[21] Cass. pen., Sez. V, 23 aprile 2021, n. 20644, in *CED Cass*. n. 281310, che ha respinto il ricorso di Mediaset con cui intendeva far annullare il sequestro preventivo del sito internet *www.iene.mediaset.it*, disposto limitatamente alle pagine in cui erano presenti i servizi televisivi andati in onda in due occasioni e riguardanti il divulgatore scientifico Roberto Burioni, riconosciuti lesivi della sua reputazione. La

Effettivamente delicata risulta la tutela dell'art. 21 Cost.

Uno dei problemi di cui si è discusso ha riguardato la possibilità di adottare il sequestro preventivo di testate giornalistiche regolarmente registrate *online*, tenuto conto dei maggiori limiti imposti dal dettato costituzionale e dalla legge sulla stampa[22].

Ampia considerazione merita il tema della "riservatezza informatica", inteso nella sua nuova dimensione, non più legata alla proprietà e alla rilevanza dei luoghi in cui si svolge, bensì alla dignità della persona[23], che trova tutela costituzionale e

---

Corte di cassazione ha ritenuto che, in base al principio di proporzionalità, siano sequestrabili non solo le frasi diffamatorie ma anche le parti del servizio, che - pur non afferendo direttamente al nucleo essenziale della comunicazione diffamatoria – finivano per rafforzarla ed amplificarla. Critico sulla sentenza F. Sarzana di S. Ippolito, *Burioni vince su Mediaset, la Cassazione apre a sequestri di siti giornalistici*, in *www.agendadigitale.eu*, 25 maggio 2021, secondo cui la decisione «sembra aprire la strada a sequestri integrali sul web di servizi giornalistici radio-televisivi molto ampi che sembrano cozzare con il principio di libertà d'espressione previsto dalla Costituzione, interpretando in maniera molto estesa il concetto di proporzionalità».

[22] Cass. pen., Sez. Un., 17 luglio 2015, n. 31022, in *Cass. pen.*, 10, 2015, p. 3437 ss., con nota di L. Paoloni, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa:* ubi commoda, ibi et incommoda?, ha chiarito, in punto di diritto, che «ove ricorrano i presupposti del fumus commissi delicti e del periculum in mora, è ammissibile, nel rispetto del principio di proporzionalità, il sequestro preventivo ex art. 321 c.p.p. di un sito web o di una singola pagina telematica, anche imponendo al fornitore dei relativi servizi di attivarsi per rendere inaccessibile il sito o la specifica risorsa telematica incriminata». La decisione è stata commentata inoltre da E. Avella, *Osservazioni a prima lettura a Cass., S.U. 17 luglio 2015 (c.c. 29 gennaio 2015), Fazzo*, in *Arch. pen. (web)*, 3, 2015, p. 1 ss.; S. Lorusso, *Un'innovativa pronuncia in tema di sequestro preventivo di testata giornalistica on line*, in *Giur. it*., 8-9, 2015, p. 2003 ss.; C. Melzi D'Eril, *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate on line registrate*, in *www.penalecontemporaneo.it*, 9 marzo 2016, p. 1 ss.; C. Melzi D'Eril, G.E. Vigevani, *Il sequestro di una pagina web può essere disposto imponendo al service provider di renderla inaccessibile*, in *Guida dir*., 38, 2015, p. 82 ss.; B. Piattoli, *Il sequestro preventivo di una pagina web: il funzionalismo della rete e le sue intersezioni nelle dinamiche processuali*, in *Dir. pen. proc*., 2, 2016, p. 212 ss.; A. Pulvirenti, *Sequestro e Internet: dalle Sezioni Unite una soluzione equilibrata, ma "creativa",* in *Proc. pen. giust.*, 6, 2015, p. 78 ss.; V. Vartolo, *In tema di sequestro preventivo della pagina web di testata giornalistica on line*, in *Riv. pen*., 10, 2015, p. 843 ss. La questione è stata rimessa alle Sezioni Unite da Cass. pen., Sez. I, ord. 3 ottobre 2014, n. 45053, in *www.penalecontemporaneo.it*, 21 gennaio 2015, p. 1 ss., con nota di M. Mariotti, *Rimessa alle sezioni Unite la questione dell'ammissibilità del sequestro preventivo, mediante oscuramento, di un sito web di una testata giornalistica*; l'ordinanza è stata commentata anche da E. Sturba, *Osservazioni a prima lettura a Cass., sez. I (ord.) 30 ottobre 2014 (ud. 3 ottobre 2014), Fazzo*, in *Arch. pen. (web)*, 3, 2014, p. 1 ss. Precedentemente, sul tema, cfr. C. Campanaro, *Legittimo il sequestro preventivo del sito internet se i contenuti sono diffamatori*, in *www.penalecontemporaneo.it*, 13 febbraio 2012; S. Di Paola, *Sequestro preventivo di sito web e inibitoria del giudice penale dell'attività del provider*, in *Foro it*., 2010, II, c. 144 ss.; C. Melzi D'Eril, *La Cassazione esclude l'estensione ai siti internet delle garanzie costituzionali previste per il sequestro di stampati*, in *www.penalecontemporaneo.it*, 25 marzo 2014, p. 1 ss.; Id., *Il sequestro di siti on-line: una proposta di applicazione analogica dell'art. 21 Cost. "a dispetto" della giurisprudenza*, in *Dir. inf. e inform.*, 2, 2014, p. 153 ss.; G. Sambuco, *Il sequestro dei contenuti on line: risposte giurisprudenziali e prospettive*, in *Proc. pen. giust*., 3, 2011, p. 58 ss.

[23] Sottolineatura in tal senso proviene da R. Orlandi, *Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, in *Arch. pen. (web)*, 25 luglio 2016. Condivisibile l'opinione per la quale l'interesse dell'utente di sistemi informatici e telematici è quello alla tutela dei propri dati, a prescindere dal luogo in cui si trovi e dallo strumento di comunicazione

convenzionale secondo un modello di garanzie paragonabile ai diritti di libertà classici[24].

Vi è poi la tematica della tutela del contraddittorio: il rischio che qualsiasi operazione compiuta sul dato informatico si potrebbe tradurre in un'irreparabile modifica dello stesso, anche qualora si utilizzino i più moderni strumenti di *digital forensics*, imporrebbe che fosse compiuta nel contraddittorio tra le parti[25]. In ogni caso, quest'ultimo viene indicato quale correttivo del paradosso della prova scientifica, nonché come baluardo contro l'ingresso nel processo della scienza-spazzatura[26], in quanto funzionale al controllo effettivo del giudice sulla scientificità della prova e sull'attendibilità del metodo scientifico impiegato nel caso concreto[27].

Infine, va ricordata la questione del controllo giurisdizionale (impugnazioni): non va infatti dimenticato che, per la giurisprudenza della Corte europea dei diritti dell'uomo, la sottoposizione delle operazioni istruttorie invasive della *privacy* ad un vaglio – almeno successivo – da parte di un organo indipendente rappresenta un requisito imprescindibile di compatibilità convenzionale[28].

---

scelto, espressa da F. Iovene, *Le c.d. perquisizioni on line tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. contemp., Riv. Trim*., 3-4, 2014, p. 335.

[24] In questi termini P. Felicioni, *Le ispezioni e perquisizioni di dati e sistemi*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), Cybercrime. *Trattato di diritto penale*, cit., p. 1404, che ricorda, da un lato, come la Corte costituzionale - con la nota sentenza n. 173/2009 - ha qualificato come fondamentale il diritto alla riservatezza riconoscendo ad esso la medesima caratura del diritto alla libertà e alla segretezza delle comunicazioni; dall'altro, come l'art. 8 CEDU è interpretato nel senso che la nozione di vita privata è riferibile alla sfera in cui l'individuo può liberamente perseguire lo sviluppo e la realizzazione della propria personalità.

[25] Nei casi di urgenza la tutela del contraddittorio esige quanto meno «che sia preservata la possibilità di controllare l'affidabilità della fonte e dell'elemento di prova», come ricorda P. Tonini, *L'evoluzione delle categorie tradizionali: il documento informatico*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), Cybercrime. *Trattato di diritto penale*, cit., p. 1327.

[26] G. Ubertis, *Il giudice, la scienza e la prova*, in *Cass. pen*., 11, 2011, p. 4118.

[27] P. Felicioni, *Le ispezioni e perquisizioni di dati e sistemi*, cit., p. 1406.

[28] Corte eur. dir. uomo, 27 settembre 2018, Brazzi c. Italia, in *www.questionegiustizia.it*, 15 gennaio 2019, con nota di D. Cardamone, *La sentenza della Cedu Brazzi c. Italia: sono arbitrarie le perquisizioni disposte dall'Autorità giudiziaria?* In tale procedimento, in cui è stata affrontata la questione della mancanza nel sistema processuale italiano di un controllo giurisdizionale *ex ante* e di un rimedio *ex post* con riferimento all'inviolabilità del domicilio, in caso di provvedimento di perquisizione domiciliare non seguito da sequestro (rispetto al quale, dunque, l'interessato non aveva potuto esperire il riesame ai sensi dell'art. 257 c.p.p. in modo da attivare un vaglio giurisdizionale perlomeno posticipato), i giudici hanno stabilito che «in assenza di un controllo giurisdizionale preventivo o di un controllo effettivo a posteriori della misura adottata, le garanzie della legislazione italiana non sono state sufficienti per evitare abusi da parte delle autorità incaricate dell'indagine penale» (§ 50) e che, seppur la misura ha una base legale nelle norme del codice di procedura penale, «il diritto interno non ha offerto al ricorrente sufficienti garanzie contro gli abusi o l'arbitrarietà prima o dopo la perquisizione» (§ 51), traendone nel caso di specie la conseguenza che l'interessato non ha beneficiato di un «controllo effettivo» come richiede «uno Stato di diritto in una società democratica» e concludendo che l'ingerenza nel diritto al rispetto del domicilio del ricorrente non è «prevista dalla legge» nel senso richiesto dall'articolo 8 § 2 della Convenzione (§ 51).

4. Se è vero che il sequestro probatorio è quello che è stato interessato normativamente dal fenomeno dell'immaterialità, di fatto è con il sequestro preventivo[29] che, assai più spesso, si interviene sulle piattaforme.

Operazioni riguardanti la diffusione illegale di materiale coperto da diritto d'autore, il fenomeno della pirateria audiovisiva attraverso la trasmissione non autorizzata su rete internet, la c.d. "IPTV" - Internet Protocol Television[30], o la

[29] Tra i principali studi monografici e le opere di carattere generale cfr.: E. Aprile, F. D'Arcangelo, *Le misure cautelari nel processo penale*, III ed., Giuffrè, Milano 2017, p. 737 ss.; P. Balducci, *Il sequestro preventivo nel processo penale*, II ed., Giuffrè, Milano 1991; L. Barone, *Le misure cautelari reali. Il sequestro preventivo*, in A. Bassi (a cura di), *La cautela nel sistema penale. Misure e mezzi di impugnazione*, Cedam, Padova 2016, p. 320 ss.; R. Bausardo, *Misure cautelari reali*, in M. Chiavario, E. Marzaduri (diretto da), *Giurisprudenza sistematica di diritto processuale* penale, *Libertà e cautele nel processo penale*, Utet, Torino 1996, p. 287 ss.; A. Bevere, *Coercizione reale. Limiti e garanzie*, Giuffrè, Milano 1999; M. Cassano, *Sub* art. 321, in A. Gaito (a cura di), *Codice di procedura penale commentato*, IV ed., vol. I, Utet, Torino 2012, p. 2042 ss.; M. Castellano, M. Montagna, *Misure cautelari reali*, in *Dig. disc. pen*., vol. VIII, Utet, Torino 1994, p. 100 ss.; A. Cisterna, *Sub* art. 321, in P. Corso (a cura di), *Commento al codice di procedura penale*, II ed., La Tribuna, Piacenza 2008, p. 1453 ss.; E. Conforti, A. Montesano Cancellara, *Il sequestro preventivo impeditivo*, in E. Conforti, A. Montesano Cancellara, G.L. Soana, *Il sequestro penale. Presupposti applicativi, gestione dei beni e strumenti di impugnazione*, Giuffrè, Milano 2016, p. 73 ss.; V. De Crescienzo, *Il sequestro penale e civile*, Utet, Torino 1997; A.M. De Santis, *Sequestro preventivo*, in *Dig. disc. pen*., vol. XIII, Utet, Torino 1997, p. 264 ss.; M. D'Onofrio, *Il sequestro preventivo*, Cedam, Padova 1998; N. Galantini, *Sub* art. 321, in E. Amodio, O. Dominoni (diretto da), *Commentario del nuovo codice di procedura penale*, vol. III, tomo II, Giuffrè, Milano 1990, p. 265; M. Garavelli, *Il sequestro nel processo penale*, Utet, Torino 2002; P. Gualtieri, *Sequestro preventivo*, in G. Spangher (diretto da), *Trattato di procedura penale*, vol. II, *Prove e misure cautelari*, tomo II, *Le misure cautelari*, a cura di A. Scalfati, Utet, Torino 2008, p. 365 ss.; Id., *Sub* art. 321, in A. Giarda, G. Spangher (a cura di), *Codice di procedura penale commentato*, IV ed., Ipsoa, Milano 2010, p. 3939 ss.; P. Gualtieri, G. Spangher, *Le misure cautelari reali*, in G. Spangher, A. Marandola, G. Garuti, L. Kalb (diretto da), *Procedura penale. Teoria e pratica del processo*, vol. II, *Misure cautelari. Indagini preliminari. Giudizio*, a cura di A. Marandola, Ipsoa, Milano 2015, p. 231 ss.; L. Milani, *Sub* art. 321, in G. Conso, G. Illuminati (a cura di), *Commentario breve al codice di procedura penale*, II ed., Cedam, Padova 2015, p. 1405 ss.; M. Montagna, *I sequestri nel sistema delle cautele penali*, Cedam, Padova 2005, p. 97 ss.; S. Olivero, *Sequestro preventivo*, in M. Chiavario (coordinato da), *Commento al nuovo codice di procedura penale*, I Agg., Torino, Utet 1993, p. 589 ss.; C. Pansini, voce *Sequestro preventivo*, in A. Scalfati (diretto da), *Digesto del processo penale on line*, Giappichelli, Torino 2012; C. Santoriello, *Il sequestro preventivo*, in F. Fiorentin, C. Santoriello, *Le misure cautelari*, vol. II, *Le misure cautelari reali*, a cura di G. Spangher, C. Santoriello, Giappichelli, Torino 2009, p. 1 ss.; E. Selvaggi, *Sub* art. 321, in M. Chiavario (coordinato da), *Commento al nuovo codice di procedura penale*, vol. III, Utet, Torino 1990, p. 359 ss.; Id., *Sub* art. 321, in M. Chiavario (coordinato da), *Commento al codice di procedura penale*, I Agg., Utet, Torino, 1993, p. 223 ss.; G. Spangher, *La pratica del processo penale*, vol. III, *I soggetti. Gli atti. Le prove. Le misure cautelari. Il procedimento penale davanti al giudice di pace*, Cedam, Padova 2014, p. 1012 ss.; N. Triggiani, *La misura volta ad evitare il reiterarsi del reato o l'inasprimento dei suoi effetti*, in M. Montagna (a cura di), *Sequestro e confisca*, Giappichelli, Torino 2017, p. 141 ss.; E. Turco, *Sub* art. 321, in G. Canzio, G. Tranchina (a cura di), *Codice di procedura penale*, tomo I, Giuffrè, Milano 2012, p. 2778; N. Ventura, voce *Sequestro preventivo*, in *Dig. disc. pen*., II Agg., Utet, Torino 2004, p. 750 ss.

[30] La rete abbonda di notizie relative ad operazioni di contrasto a tali fenomeni. Tanto per citarne qualcuna v. F. Sarzana di S. Ippolito, *Pirateria tv, sotto sequestro la piattaforma online Xtream. Ecco i dettagli dell'operazione*, in *www.ilfattoquotidiano.it*, 18 settembre 2019; G. Terlizzi, *Mazzata alla pirateria online, sequestrati 58 siti web e 18 canali Telegram*, in *www.agi.it*, 23 settembre 2020.

diffusione abusiva di copie digitali dei principali quotidiani[31], hanno visto l'Autorità Giudiziaria fare ricorso a tale istituto per "oscurare" siti *web* localizzati anche al di fuori della giurisdizione italiana[32].

È principio ormai consolidato nella giurisprudenza di legittimità[33] che le finalità tipiche del sequestro preventivo possano essere raggiunte in materia mediante operazioni tecniche - imposte al fornitore dei relativi servizi - tese ad oscurare e rendere inaccessibile agli utenti la visione del sito o l'accesso alla piattaforma.

In tal modo la misura si risolve in una inibitoria atipica, che sposta l'ambito di incidenza del provvedimento da quello reale, proprio del sequestro preventivo, a quello obbligatorio, in quanto indirizzato a soggetti determinati (i c.d. *provider*), ai quali viene ordinato di conformare la propria condotta al fine di ottenere l'ulteriore e indiretto risultato di impedire connessioni a questa o quell'altra piattaforma.

Anche se l'interpretazione fa leva su quanto disposto dal decreto legislativo attuativo della direttiva europea sul commercio elettronico[34], nondimeno è stato rilevato, da un lato, come il carattere obbligatorio che tale sequestro preventivo viene ad assumere viòla il principio di legalità processuale[35], dall'altro, come l'inibitoria non possa essere riguardata alla stregua di una mera "modalità esecutiva" del sequestro preventivo[36].

---

[31] Il provvedimento con cui la Procura della Repubblica presso il Tribunale di Bari ha disposto in tempi recenti il sequestro preventivo d'urgenza, mediante inibizione immediata dell'accesso, di numerosi canali Telegram mediante i quali, secondo le indagini, venivano diffuse abusivamente copie digitali dei principali quotidiani è diffuso e riassunto da G. Stampanoni Bassi, *Il provvedimento di sequestro della Procura di Bari nell'indagine sulle copie di riviste e quotidiani diffuse abusivamente su Telegram*, in *www.giurisprudenzapenale.com*, 3 maggio 2020.

[32] Per una panoramica sui casi più noti di sequestro preventivo di siti *web* allocati all'estero e sulle relative problematiche tecniche e giuridiche si v. F. Cajani, *Giurisdizione e competenza nelle indagini informatiche*, in Aa.Vv., Cyber forensic *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, cit., p. 182 ss.

[33] Rilevante sul tema è la pronuncia Cass. pen., Sez. Un., 17 luglio 2015, n. 31022, cit. Già in precedenza, relativamente al noto caso PirateBay, Cass. pen., Sez. III, 23 dicembre 2009, n. 49437, in *Dir. inf. e inform.*, 3, 2010, p. 437 ss, con nota di F. Merla, *Diffusione abusiva di opere internet e sequestro preventivo del sito* web. *Il caso* The pirate bay, aveva attribuito ad un sito *web* la natura di *res*, pur non necessariamente materiale in senso stretto; inoltre, pur non negando l'esistenza di «un risvolto della misura cautelare che può essere riguardato come un'inibitoria», la stessa decisione aveva ritenuto che «si rimane nell'ambito del sequestro preventivo che investe direttamente la disponibilità del sito web e che, solo come conseguenza, ridonda anche in inibizione di attività. Sicché sussiste, sotto questo profilo, il carattere reale del sequestro preventivo che quindi non viola il principio di tipicità delle misure cautelari penali».

[34] Il d. lgs. 9 aprile 2003, n. 70 che, in attuazione della direttiva 2000/31/CE, ha regolamentato taluni aspetti giuridici dei servizi delle società dell'informazione nel mercato interno con particolare riguardo al commercio elettronico. Sui rapporti tra tale inibitoria e il sequestro preventivo si v. F. Cajani, *Giurisdizione e competenza nelle indagini informatiche*, cit., p. 194 s.

[35] A. Testaguzza, *Il sequestro di dati e sistemi*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), Cybercrime. *Trattato di diritto penale*, cit., p. 1452.

[36] A. Monti, *Casi e problemi sul sequestro informatico anche a distanza,* cit., p. 979.

Dal punto di vista più strettamente operativo, invece, il mutamento di "pelle" della misura cautelare reale ha fatto affiorare difficoltà nel garantire efficacia a questi provvedimenti. Il rischio che il dominio sia modificato, eludendo il decreto di sequestro di un sito specifico, è stato arginato adoperando formulazioni aperte, che estendono il sequestro «a tutti gli alias e i nomi di dominio, presenti e futuri». La sorveglianza sui nuovi siti suscettibili di oscuramento, generati a seguito della chiusura dei precedenti, in un recente caso è stata affidata alla stessa persona offesa (in tal caso si trattava del titolare del diritto d'autore), impegnandola ad indicarli volta per volta agli *internet service provider*[37].

5. Oggi il quadro sembra complicarsi ulteriormente con il proliferare delle cripto-attività; ci si riferisce ai *token* di moneta elettronica[38] e, in particolare, a quelli di "classe 1", come la criptovaluta *Bitcoin*[39].

In realtà, le difficoltà risultano più pratiche che teoriche, in quanto la possibilità di operare sequestri di questi beni viene generalmente ammessa. Fuori dal nostro continente è celebre il caso statunitense *Silk Road*[40], ma anche in Italia si è proceduto al sequestro di una ingente quantità di *bitcoin* nei confronti dell'*exchange* di criptovalute denominato "*BitGrail*"[41] e, seppure ciò sia avvenuto nell'ambito di una procedura civilistica, nondimeno la vicenda consente di trarre utili spunti anche per l'ambito penale.

Quello che è complesso, in ragione della crittografia – che caratterizza i sistemi *Distributed Ledger Techcnolog* (DLT), categoria cui appartiene la *blockchain* – è proprio l'apposizione di un vincolo di indisponibilità.

Occorre innanzi tutto risalire alle chiavi private (che dovrebbero essere il vero oggetto di sequestro, in quanto i *bitcoin* sono solo, sintetizzando all'estremo, delle trascrizioni sulla *blockchain*)[42].

Il ritrovamento di un *wallet*, tuttavia, non esclude che lo stesso sia nella disponibilità di altri soggetti (*exchange* o dei *wallet providers*).

Inoltre, è difficile poter affermare con certezza che un determinato soggetto è 'titolare' di un *address bitcoin* alla stregua di quanto avviene con un conto corrente bancario.

---

[37] Trib. Milano, G.i.p., 12 giugno 2017, inedita. La decisione è riportata da P.E. Liedholm, *Gli illeciti in materia di diffusione non autorizzata di opere dell'ingegno*, in *https://www.4clegal.com/hot-topic/sequestro-preventivo-forma-contrasto-pirateria-online*, 9 settembre 2019.

[38] Sulle tipologie di *tokens* C. Pernice, *I modelli di valuta virtuale: sistematica e definizione*, in *mediaLaws*, 3, 2020, p. 47.

[39] G. Scotti, *Blockchain, Criptovalute e Ico: analisi tecnica e giuridica della più recente innovazione fintech*, in *Riv. Cammino Diritto*, 8 febbraio 2020, p. 12.

[40] Si v. G. Costabile, *Le indagini digitali*, in Aa.Vv., Cyber forensic *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, cit., p. 111 ss.

[41] La vicenda è tratteggiata da S. Capaccioli, P. Soldavini, *Fallisce Bitgrail, la piattaforma italiana per le criptovalute*, in *www.ilsole24ore.com*, 26 gennaio 2019.

[42] A. Rosato, *Profili penali della criptovalute*, Pacini editore, Pisa 2021, p. 140.

Occorre evitare che chi è a conoscenza della chiave privata possa servirsi di strumenti di *mixing* che facciano "perdere le tracce" sulla *blockchain* dei *bitcoin* posseduti[43].

Nel caso di *wallet software* o *online*, il sequestro dell'*hard disk* o la modifica della *password* del *wallet* non appaiono misure sufficienti, in quanto l'utente può aver effettuato un *backup* dei dati o avere comunque la disponibilità della chiave privata. Bisognerebbe, pertanto, creare un nuovo indirizzo *bitcoin*, trasferire i *bitcoin* sequestrati presso il nuovo indirizzo e, per proteggerli da tentativi di sottrazione, cifrare anche la chiave privata o adottare sistemi di *multisignature*.

Altra soluzione ipotizzabile è quella di convertire i *bitcoin* in valuta avente corso legale, seppure si tratti di operazione delicata alla luce degli instabili apprezzamenti/deprezzamenti del sistema e si tratti di attività che vada ben oltre la semplice 'apprensione' del bene[44].

Una semplificazione delle operazioni potrebbe venire da una futura implementazione delle funzioni della *blockchain*, prevedendo delle modalità di *freezing* (blocco) dei *wallet* a fini forensi, sebbene al momento ciò non sembrerebbe possibile[45].

6. Le "linee evolutive" della materia sembrano indirizzarsi verso il superamento del sequestro stesso quale strumento per assicurare al processo i beni immateriali[46], attraverso metodi acquisitivi differenziati che forniscono esiti sostanzialmente identici, ma divergono profondamente sul piano delle garanzie.

Ne sono esempio gli strumenti delineati dalla proposta – pubblicata nel 2018 dalla Commissione europea - di regolamento in materia di *European Production Order* e *European Preservation Order*[47], che mirano a creare un canale di cooperazione diretta

[43] G. Costabile, *Le indagini digitali*, cit., p. 127.

[44] R. Lupo, *Quale sequestro per le criptovalute?*, in *il Centauro*, 232, 2020, p. 53.

[45] G. Costabile, *Come funzionano le investigazioni e i sequestri su bitcoin*, in *https://www.agendadigitale.eu/sicurezza/come-funzionano-le-investigazioni-e-i-sequestri-su-bitcoin/*, 5 aprile 2018.

[46] Mette in evidenza come rispetto al sequestro probatorio si privilegino altre vie attraverso cui far entrare l'evidenza elettronica a far parte del compendio probatorio potenzialmente spendibile ai fini di una decisione giudiziale, sia a livello nazionale che internazionale, A. Paoletti, *Il sequestro probatorio di dati digitali, le perquisizioni informatiche e la valenza che assume la copia-clone del supporto di memoria oggetto d'investig*azione, in *www.iusinitinere.it*, 15 febbraio 2021.

[47] Proposta della Commissione europea di regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, del 17 aprile 2018, COM(2018)225, consultabile all'indirizzo internet *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018PC0225*. Tra i primi commenti L. Buono, *The Genesis of the European Union's New Proposed Legal Insturment(s) on e-Evidence*, in *ERA Forum*, 19, 2019, p. 307 ss.; E. Colombo, *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*., 7, 2019, p. 2722 ss.; V. Frassen, *The European Commission's e-Evidence Proposal: toward an EU-wide obligation for service providers to cooperate with law enforcement?*, in *www.europeanlawblog.eu*, 12 ottobre 2018; R.M. Geraci, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di*

(fuori dai confini nazionali) fra i *provider* e le autorità giudiziarie interessate all'acquisizione delle prove elettroniche in materia penale[48].

La proposta fonda sulla assenza di un controllo preventivo da parte dell'autorità dello Stato di esecuzione - che può essere chiamata in causa dallo stesso *provider* solo *ex post* e in determinati casi in cui pare esservi una palese violazione dei diritti fondamentali - e risponde alla forte esigenza di fornire alle autorità giudiziarie strumenti all'avanguardia per ottenere l'accesso transfrontaliero ai dati[49].

---

regolamento e-evidence, in *Cass. pen*., 3, 2019, p. 1340 ss.; M. Gialuz, J. Della Torre, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. contemp*., 5, 2018, p. 277 ss.; L. Gómez Amigo, *Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima*, in *Revista Española de Derecho Europeo*, 71, 2019, p. 1 ss.; J.H. Jeppesen-G. Nojeim, *Initial Observations on the European Commission's e-Evidence Proposals*, in *www.cdt.org*, 18 aprile 2018; Id., *Assessing the European Commission's E-Evidence Proposals on Ten Human Rights Criteria*, in *www.cdt.org*, 18 aprile 2018; F. La Chioma, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, in *www.magistraturaindipendente.it*, 6 giugno 2019; V. Mitsilegas, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Criminal Law*, 25, 2018, p. 263 ss.; L. Moxley, *EU Releases e-Evidence Proposal for Cross-Border Data Access*, in *www.insideprivacy.com*, 8 maggio 2018; O. Pollicino, M. Bassini, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, in *www.medialaws.eu*, 26 ottobre 2018; G. Robinson, *The European Commission's e-Evidence Proposal*, in *European Data Protection Law Review*, 3, 2018, p. 347 ss.; F. Ruggeri, *Novità. Il protocollo 16 alla Cedu in vigore dal 1° agosto 2018. La proposta per l'ordine europeo di conservazione o di produzione della prova digitale*, in *Cass. pen*., 7-8, 2018, p. 2660 ss.; V. Tondi, *L'accesso transfrontaliero all'electronic evidence, tra esigenze di effettività e tutela dei diritti*, in *Dir. pen. contemp., Riv. Trim.*, 2, 2019, p. 442 ss.; S. Tosza, *All evidence is equal, but electronic evidence is more equal than any other: the relationship between the European Investigation Order and the European Production Order*, in *New Journal of European Criminal Law*, 11, 2020, p. 161 ss.

[48] Nel Progetto di Relazione Sippel 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 del 24 ottobre 2019, COM(2018)0225 – C8-0155/2018 – 2018/0108(COD), consultabile al link *https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/PR/2021/03-22/1191404IT.pdf*, p. 147, si legge che si è di fronte a «un'interpretazione atipica del concetto di riconoscimento reciproco, che consente all'autorità di emissione di rivolgersi ai prestatori di servizi in un'altra giurisdizione senza coinvolgere automaticamente le autorità dell'altro e degli Stati interessati» e che vi è l'«introduzione dell'extraterritorialità o elusione di prerogative fondamentali dello Stato». Va ricordato che il Parlamento Europeo ha assegnato la discussione della proposta della Commissione alla commissione LIBE ("Committee on civil liberties, justice and home affairs") e alla deputata Birgit Sippel è stato affidato il compito di relatrice. Il summenzionato progetto di relazione contiene numerosi emendamenti che insistono su una più ampia tutela dei diritti fondamentali che, sebbene abbiano suscitato reazioni favorevoli in dottrina — T. Christakis, E-*evidence: the way forward (Summary of the Workshop held in Brussels on 25 Septembre 2019)*, in *www.europeanlawblog.eu*, 06 novembre 2019; Id., *Lost in notification? Protective logic as compared to efficiency in the European parliament's e-evidence draft report*, in *www.crossborderdataforum.org*, 07 gennaio 2020; Id., *E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report*, in *www.europeanlawblog.eu*, 21 gennaio 2020 — hanno anche comportato la reazione politica della Commissione, che ha avviato un confronto istituzionale inedito all'interno dell'Unione.

[49] Che, in casi urgenti, può avvenire entro sei ore. Ciò accelera notevolmente l'ottenimento di informazioni rispetto ai centoventi giorni per l'ordine europeo di indagine (EIO) e ai dieci mesi nel settore

A tal fine, la proposta prevede che l'autorità giudiziaria inquirente ordini direttamente al prestatore di servizi del sistema informatico o telematico localizzato in un altro Stato la conservazione o la produzione degli e-data in proprio possesso.
L'autorità giudiziaria può emettere un ordine di conservazione europeo (OCE) e ingiungere a un prestatore di servizi di conservare prove elettroniche in vista di una successiva richiesta di produzione. Quest'ultima rappresenta un ordine di produzione europeo (OPE), che consiste in una decisione vincolante di un'autorità di emissione di uno Stato membro che ingiunge a un prestatore di servizi di altro Stato membro di produrre prove elettroniche in suo possesso. Gli ordini emessi sono, in seguito, trasmessi per mezzo dei relativi certificati (denominati rispettivamente, per OCE e OPE, EPOC-CR ed EPOC), il cui scopo è quello di «fornire tutte le informazioni necessarie al destinatario in un formato standardizzato, escludendo dati sensibili contenuti negli ordini di produzione e di conservazione come quelli relativi alla necessità o alla proporzionalità di tali provvedimenti investigativi, per evitare di compromettere la segretezza e il buon esito delle indagini»[50].

Il punto critico — sebbene la proposta della Commissione sia stata oggetto di molteplici proposte emendative rispetto al progetto iniziale, che nel prossimo futuro saranno discusse a un tavolo trilaterale avviato tra Commissione, Consiglio e Parlamento[51] — è che spetterebbe ai *provider* anche verificare che le richieste istruttorie rispettino la Carta di Nizza[52].

---

dell'assistenza giudiziaria reciproca (convenzionale), come sottolinea A. Tinoco-Pastrana, *The Proposal on Electronic Evidence in the European Union*, in *Eucrim*, 1, 2020, p. 47.

[50] R. Pezzuto, *Accesso transazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione Europea al vaglio del Consiglio dell'Unione*, in *Dir. pen. contemp.*, 2, 2019, p. 80.

[51] Su cui O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in *www.lalegislazionepenale.eu*, 30 marzo 2021.

[52] Secondo A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea: le proposte della Commissione Europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, in *www.lalegislazionepenale.eu*, 16 ottobre 2020, p. 14, nella proposta in esame, vi è un'evidente «difficoltà derivante dal fatto di attribuire al prestatore di servizi il compito di valutare se l'ordine ricevuto si ponga in contrasto con gli obblighi derivanti dalla Carta dei diritti fondamentali dell'Unione europea e dall'articolo 6 del Trattato sull'Unione europea, dunque di richiedere a un privato di operare al fine della tutela dei diritti fondamentali come se fosse un'autorità giudiziaria». Critico anche M. Daniele, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Revista Brasileira de Direito Processual Penal*, 3, 2019, p. 1290, secondo cui «ci sono, tuttavia, forti dubbi che un tale complesso meccanismo possa sortire i suoi effetti, e ciò per una ragione connessa alla stessa essenza dei provider: i quali, a causa della loro natura privatistica e della conseguente – e legittima – esigenza di proteggere i loro interessi, non potrebbero mai agire come organi pubblici in posizione di imparzialità, di per sé del tutto indifferenti all'esito del vaglio. Per quanto possano avere a cuore la privacy dei loro utenti, la loro condotta sarebbe condizionata dalla comprensibile necessità di mantenere buoni rapporti con gli Stati in cui esercitano la loro attività economica. Il rischio, poi, che, rifiutandosi di eseguire gli ordini di conservazione o produzione dei dati, siano esposti a sanzioni, inevitabilmente falserebbe le loro valutazioni». In dottrina, di contro, O. Pollicino, M. Bassini, *La proposta di regolamento e-Evidence*, cit., p. 7, hanno considerato positivamente la clausola che rimette la tutela dei diritti e interessi

Ne deriverebbe, però, la privatizzazione di un'attività tradizionalmente riservata ad organi pubblici (le autorità giudiziarie): un preoccupante cambio di paradigma che rischia di porre in serio pericolo i diritti fondamentali[53], da garantire anche – e soprattutto – quando la sfera in cui vivono sia quella della immaterialità.

7. Le piattaforme sono sempre più nuove e sofisticate: di esse fruisce sia la criminalità per commettere reati, sia lo Stato per reprimere i reati.

L'immaterialità digitale produce nuove minacce criminali e modifica la fisionomia delle forme di manifestazione della delinquenza determinando una crescita esponenziale della frequenza con cui gli illeciti comuni sono compiuti attraverso tali strumenti informatici. In parallelo, si sviluppano indagini informatiche sempre più sofisticate e di formidabile efficacia investigativa.

Si profilano all'orizzonte diversi fattori in grado di destabilizzare l'accertamento giudiziario: abusi nelle indagini di mezzi tecnologici invasivi oltre i limiti della stretta necessità; impiego per le decisioni giudiziarie di elementi ottenuti attraverso metodi di cui non siano completamente verificabili idoneità tecnica, margini di affidabilità e rischio di errori; uso di strumenti che permettano di eludere presupposti e limiti che presidiano le forme acquisitive tipiche, di aggirare prerogative difensive o, addirittura, di manipolare la libera autodeterminazione (maggiormente esposta in un ambiente fluido quale il *cyberspace*).

Occorre tuttavia affrontare il tema evitando scorciatoie connesse alla mancanza di riferimenti normativi e alla necessità di efficaci mezzi idonei a contrastare l'accentuata pericolosità dei fenomeni criminali che sfruttano tali tecnologie.

I mezzi a disposizione degli organi investigativi non possono prescindere dalle garanzie proprie di un giusto processo, ma devono basarsi su un metodo rispettoso dei diritti fondamentali.

Solo in questo modo è possibile accrescere la conoscenza su metodi (in uso o in via di sviluppo) non sempre in linea con gli *standard* di un sistema di libertà, al fine di enucleare il complesso di garanzie da porre a fondamento di uno statuto processuale delle investigazioni ad alto contenuto tecnologico. Occorre muovere dalla considerazione di base per cui le investigazioni possono svolgersi senza vincoli solo se non intacchino prerogative che attengono al nucleo duro dei diritti della persona; tra le barriere poste dalle norme costituzionali e sovranazionali (in particolare, riserva di legge e di giurisdizione), non va trascurato il principio di proporzionalità, che consente sacrifici a diritti primari nei limiti di un equilibrio tra mezzi e fini.

---

fondamentali a soggettivi privati, in quanto «rispondente alla migliore tutela degli interessi in gioco», laddove un intervento preventivo dell'autorità giudiziaria dello Stato di esecuzione vanificherebbe i «benefici connessi alla disintermediazione» e sacrificherebbe la funzionalità della procedura in esame.

[53] M. Daniele, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1277.

Dalla capacità di coniugare il sapere tecnico con quello giuridico dipenderà la costruzione di metodi per “governare” i fenomeni criminali riguardanti le piattaforme digitali, efficaci e al contempo rispettosi dei diritti fondamentali.