Issn: 2612-4491

Diritto di INTERNET

Digital Copyright e Data Protection

RIVISTA TRIMESTRALE

2021
4

Pacini Giuridica

SOMMARIO

SAGGI

GIURISPRUDENZA

EUROPEA

COMPARATA

CIVILE

PENALE

AMMINISTRATIVA

PRASSI

Catena di Custodia, Prova Digitale e Tecnologia Block-chain

di Giulio Soana

Le peculiari caratteristiche della prova digitale ed il suo pervasivo utilizzo per l'accertamento penale richiedono l'impiego di nuove tecniche che permettano di garantirne l'integrità e comprensibilità per gli attori processuali; in particolare, la catena di custodia, elemento cruciale per garantire la correttezza metodologica della prova scientifica, può giocare un ruolo centrale in questo sforzo. Tale aggiornamento delle tecniche forensi è oltretutto legislativamente demandato a seguito dell'introduzione della l. 48/2008. In quest'ottica, la tecnologia block-chain può essere implementata quale strumento di registrazione e conservazione della catena di custodia; l'attitudine di tale tecnologia a questo scopo è stata d'altro canto già dimostrata dalla sua prima adozione da parte dell'Hangzhou Internet Court in Cina. Il presente contributo analizza, da una prospettiva prettamente giuridica, le potenzialità di una tale implementazione nell'ordinamento italiano.

The characteristics of the digital evidence and its pervasive use as means to establish criminal responsibility call for new techniques to guarantee its integrity and comprehensibility for the parties; the chain of custody plays a crucial role in guaranteeing the methodological soundness of the scientific evidence, and can, therefore, be a fundamental piece in this effort. This update of the techniques is law-mandated following the introduction of the l. 48/2008. Within this framework, block-chain can be implemented as a means to register and store the chain of custody; the aptness of this technology is, furthermore, witnessed by its adoption by the Hangzhou Internet Court in China. The article analyses, from a legal perspective, the risk and opportunities of this implementation within the Italian legal system.

1. Introduzione

La tecnologia è divenuta un elemento pervasivo della nostra quotidianità. Ambiti che fino a pochi decenni fa erano considerati dominio esclusivo dell'interazione umana ed espressione del libero arbitrio individuale sono oggi svolti e regolati, apertamente o occultamente, da strumenti tecnologici; funzioni essenziali dello sviluppo e della vita umana quali l'orientamento, l'interazione familiare e la ricerca di un partner sono attualmente, in maniera quasi totalitaria, svolti mediante strumenti informatici in modo tale da comportare una vera e propria sovrapposizione, per non dire sostituzione, con le capacità analogiche dell'individuo.

Come è ovvio, questa transizione tecnologica non ha riguardato solo la fisiologia dell'agire bensì anche la sua patologia, sia in ambito strettamente informatico sia in quello tradizionale. Segnatamente, l'aumento esponenziale della criminalità informatica è stato accompagnato da un sempre maggiore utilizzo di strumenti tecnologici nell'*iter criminis* di reati essenzialmente analogici (1).

Tale fusione tra uomo e macchina ha comportato una crescente necessità per le autorità investigative di avvalersi di tali strumenti al fine di svolgere il proprio compito istituzionale, rendendo la prova digitale vitale per la ricostruzione dei fatti in ambito penale (2) ed approssimandola a scalzare il DNA dal suo ruolo di novella prova regina.

La prova digitale, come d'altro canto qualunque prova scientifica, impone all'interprete due valutazioni tra loro connesse e gerarchicamente ordinate; invero, il giudizio riguardo la rilevanza del contenuto probatorio addotto da tale prova alla ricostruzione giudiziale dei fatti è sottoposto ad una valutazione in merito alla validità e alla correttezza della metodologia utilizzata al fine di ottenere, analizzare e conservare l'apporto probatorio (3). Tale valutazione metodologica è un elemento coessen-

(1) Pittiruti, *Digital Evidence e procedimento penale*, Torino, 2017, 1; Antwi-Boasiako - Venter, *Implementing the harmonized model for digital evidence admissibility assessment* in *Advances in digital forensics XV*, a cura di Peterson - Shenoi, Cham, 2019; Siracusano, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. pen. e giust.*, 2017, 179; Europol, *Internet Organized Crime Threat Assessment*, 2020, 6.

(2) Mercer, *Computer Forensics: Characteristics and Preservation of Digital Evidence*, in *FBI Law Enforcement Bulletin*, 2004, 28; Lupária - Ziccardi, *Investigazione penale e tecnologia informatica*, Milano, 2007, 131-34; Bartoli - Maioli, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in *Informatica e diritto*, 2015, 140.

(3) Kasper - Lauritus, *Challenges in collecting digital evidence: a legal perspective*, in *The future of law and eTechnologies*, Cham, 2016, 228, "*Forensic*

ziale a qualunque risultato scientifico, date le peculiarità dell'epistemologia scientifica, nonché precondizione di un corretto apprezzamento fattuale dei dati apportati.
Il summenzionato giudizio metodologico assume una rilevanza primaria nel caso della prova digitale date le specificità ontologiche che la caratterizzano, le quali impongono un'attenzione speciale al fine di garantire la sua integrità e prevenire alterazioni (4); invero, questa prova si contraddistingue per la sua fragilità e volatilità che comporta un alto rischio di modificazioni dolose o colpose del suo contenuto (5). Inoltre, la natura transnazionale della prova digitale e la relativa mutabilità delle metodologie, implementate in ambito forense, impone un'accentuata tracciabilità degli apporti probatori, al fine di salvaguardare la funzione del giudice di garante della correttezza epistemologica del processo e permettere un'efficiente revisione *ex post* dei procedimenti forensi. Peraltro, tale tracciabilità è cruciale per preservare l'effettività del contraddittorio processuale, risultando altrimenti virtualmente impossibile per la difesa comprendere, e quindi tentare di confutare, la validità astratta e la correttezza concreta delle prove addotte.
Strumento chiave per la salvaguardia e la valutazione della correttezza metodologica della prova scientifica è la catena di custodia. Tale strumento funge da metadato della prova, registrando in modo consequenziale i vari momenti dell'indagine forense ed identificando per ognuno di essi il chi, il come, il quando e il perché (6). Invero, solo assicurando la completa e continuativa registrazione di ogni momento dell'indagine forense è possibile garantire l'ammissibilità della prova (7), preservando allo stesso tempo la funzione del giudice e della difesa in ambito di valutazione metodologica della stessa.
Lo sviluppo tecnologico può fornire una soluzione al problema da esso stesso creato. Segnatamente - nell'ambito di un più ampio movimento che nell'ultimo decennio ha portato all'emersione di un fiorente mercato per la realizzazione di strumenti informatici volti a facilitare la compliance normativa (il c.d. RegTech) - l'attitudine della prova informatica e dei processi di informatica forense a comunicare con sistemi digitali comporta un ampio spazio per la digitalizzazione del procedimento di creazione e conservazione della catena di custodia in modo tale da ridurre le asimmetrie informative e garantirne l'immodificabilità ed affidabilità.
In particolare, una tecnologia che sembra particolarmente adatta ad una tale implementazione è la block-chain (8). Invero, con il suo registro trasparente, decentralizzato, consequenziale ed immodificabile questa tecnologia ben rispecchia le necessità della catena di custodia e potrebbe aumentarne in maniera sostanziale l'affidabilità nonché l'accessibilità (9). Inoltre, la possibilità di codificare *smart contracts* contribuirebbe a ridurre il carico amministrativo della polizia scientifica e garantire al contempo l'implementazione automatica dei protocolli forensi, nonché a diminuire la contestabilità della catena stessa salvaguardando l'efficacia del lavoro degli esperti forensi. Infine, l'accessibilità della catena e la sua comunicabilità, data dalla decentralizzazione del registro, ridurrebbe i costi e velocizzerebbe le procedure assicurando l'accesso immediato alla catena di custodia per gli operatori autorizzati.
Una tale implementazione della block-chain è già stata, d'altro canto, testata ed è attualmente utilizzata in Cina, seppur in ambito civile: sin dal 2019 la Hangzhou Internet Court ha creato la Hangzhou Judicial Blockchain Platform proprio al fine di facilitare la produzione

evidence is only as valuable as the integrity of the method that the evidence was obtained".

(4) Peluso, *L'acquisizione e la conservazione della prova informatica*, in *La responsabilità nei nuovi reati informatici*, a cura di Peluso, Bologna, 2020, 264; Cuomo, *La prova digitale*, in *Prova Scientifica e Processo Penale* a cura di Canzio - Lupària, Milano, 2017, 675.

(5) Come indicato nella relazione esplicative della Convenzione di Budapest sulla criminalità informatica, Council of Europe, *Explanatory report to the Convention on Cybercrime*, 2001, 25, "*because of the volatility of computer data, the data is easily subject to manipulation or change. Thus, valuable evidence of a crime can be easily lost through careless handling and storage practices, intentional manipulation or deletion designed to destroy evidence or routine deletion of data that is no longer required to be retained*"; Aterno, *Digital Forensics e scena criminis*, in *Manuale delle investigazioni sulla scena del crimine*, a cura di Curtotti - Saravo, 2019, Torino, 804; Giova, *Improving chain of custody in forensic investigation of electronic digital systems*, in *International Journal of Computer Science and Network Security*, 2011, 2; Cuomo, *La prova digitale*, cit., 675; Lupària - Ziccardi, *Investigazione penale e tecnologia informatica*, cit., 143.

(6) Giova, *Improving chain of custody in forensic investigation of electronic digital systems*, cit., 1; Goodison - Davis - Jackson, *Digital evidence and the US criminal justice system*, cit., 12.

(7) Peluso, *L'acquisizione e la conservazione della prova informatica*, cit., 290; Mercer, *Computer Forensics: Characteristics and Preservation of Digital Evidence*, cit., 30; Rivello, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 2013, 1710.

(8) Burri - Casey - Bolle - Jaquet-Chiffelle, *Chronological independently verifiable electronic chain of custody ledger using blockchain technology*, in *Forensic Science International: Digital Investigation*, 2020, 2, "*Blockchain technology provides the ideal solution of this digital transformation of provenance information related to digital evidence (...) no alteration can be executed without being evident: once data are stored in the blockchain, they cannot be modified or removed*"; Billard, *Block-chain based digital inventory*, in *Journal of Advances in Information Technology*, 2019, 42, "*Blockchain, by its immutable nature, is the ideal candidate for supporting data provenance in a forensics environment. When a digital evidence is added to the blockchain, as a transaction, it is validated by the users of the blockchain by the commit of its block. Once committed, the digital evidence cannot be further altered or removed*".

(9) Billard, *Block-chain based digital inventory*, cit., 47; Lone - Roohie, *Forensic-chain: Ethereum blockchain based digital forensics chain of custody*, cit., 45.

di prove nei processi presso tale Corte, eliminando la necessità di certificazione notarile.

2. Volatilità, modificabilità e transnazionalità. Le chiavi di volta del rischio digitale

Come anticipato la prova digitale si caratterizza per delle peculiarità che acuiscono l'esigenza di salvaguardarne l'integrità e l'immodificabilità durante il procedimento forense; in particolare, questa si contraddistingue per la sua volatilità (10), modificabilità (11) e transnazionalità (12).

Partendo dalla volatilità, questa è una conseguenza della natura essenzialmente dinamica degli ambienti digitali che implica un'attitudine di questi ultimi a modificarsi con grande rapidità causando effetti distruttivi sull'esistenza ovvero sulla consistenza dei dati in questi contenuti. In particolare, questi continui passaggi di stato richiedono una speciale attenzione e tempestività nell'esecuzione del procedimento forense, al fine di evitare che l'attività ovvero l'inattività del tecnico comportino la perdita di dati volatili.

Tale volatilità si combina con la modificabilità della prova digitale. In particolare, per modificabilità si intende l'attitudine della prova digitale a mutare in maniera spesso irreparabile ed, ancora peggio, impercettibile a seguito di azioni colpose o dolose dell'utente. È proprio tale impercettibilità del cambiamento ad essere particolarmente problematica: invero, la prova digitale può essere irrimediabilmente compromessa apparendo al contempo *prima facie* integra.

La volatilità e modificabilità della prova digitale, se da una parte richiedono agli investigatori di prestare particolare attenzione nella preparazione ed esecuzione di indagini forensi al fine di evitare alterazioni o perdita di dati, d'altra parte, impongono la minuziosa registrazione della catena di custodia al fine di certificare l'identità tra prova acquisita e prova prodotta (13). Solo attraverso tale completa annotazione di ogni fase, dall'identificazione alla produzione, sarà possibile dimostrare e, conseguentemente, valutare la genuinità della prova addotta. Invero, tali caratteristiche della prova digitale implicano un elevato rischio che attività negligenti o dolose possano comprometterla e causare uno sviamento delle indagini e dell'accertamento processuale con esiti potenzialmente catastrofici (14).

Da ultimo, la prova digitale si contraddistingue per la sua transnazionalità: invero, l'ambiente informatico si caratterizza per la sua incorporeità ed a-territorialità (15). Tale assenza di collegamento territoriale tra utente e dato, ulteriormente accelerato dal progressivo sviluppo della tecnologia *cloud* (16), si scontra con la natura essenzialmente territoriale della giurisdizione penale, sia nella fase investigativa che processuale (17).

Questa discrasia comporta una continua necessità da parte delle autorità investigative di collaborare con le autorità straniere al fine di ottenere i necessari apporti probatori (18); tale collaborazione implica problemi in termini di comprensibilità e verificabilità per gli attori della giurisdizione ricevente della metodologia implementata in fase di assunzione della prova (19). Invero, la distanza fisica tra giudice, difesa e polizia forense straniera (20), combinata con la frequente impossibilità di sottoporre al contraddittorio processuale i tecnici che hanno materialmente proceduto all'acquisizione e conservazione della prova, affievolisce il potenziale del contraddittorio quale strumento per la formazione della verità processuale; a questo si aggiunge l'assenza di standard universalmente accettati in ambito di infor-

(10) Aterno, *Digital Forensics e scena criminis*, cit., 780; Bartoli - Maioli, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, cit., 139; Lone - Roohie, *Forensic-chain: Ethereum blockchain based digital forensics chain of custody*, cit., 47.

(11) Peluso, *L'acquisizione e la conservazione della prova informatica*, cit., 264, 284; Siracusano, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., 178; Cuomo, *La prova digitale*, cit., 675; Cole - Quintel, *Transborder Access to e-Evidence by Law Enforcement Agencies*, in *University of Luxembourg Law Working Paper*, 2018, 1.

(12) Brenner - Schwerha, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, in *J. Marshall J. Computer & Info. L.*, 2001, 366; Soana, *L'accesso transfrontaliero alla prova informatica. Oltre il principio di territorialità*, in *Rivista semestrale di diritto*, 257; Lupària . Ziccardi, *Investigazione penale e tecnologia informatica*, cit., 211.

(13) Aterno, *Digital Forensics e scena criminis*, cit., 776.

(14) Peluso, *L'acquisizione e la conservazione della prova informatica*, cit., 262; si veda il caso "Amero" citato da Vaciago, *Digital Evidence*, Torino 2022, in stampa, 14 ss.; Kasper - Lauritus, *Challenges in collecting digital evidence: a legal perspective*, cit., 199-200.

(15) Daskal, *Law enforcement access to data across borders: The evolving security and rights issues*, in *J. Nat'l Sec. L. & Pol'y*, 2015, 476; Marletta - Simonato, *Le sfide della cooperazione internazionale nell'era digitale*, in *Cassazione Penale*, 2016, 1235.

(16) Peluso, *L'acquisizione e la conservazione della prova informatica*, cit., 261; McDonald, *Authenticating Digital Evidence from the Cloud*, cit., 40-41; Woods, *Mutual Legal Assistance in the Digital Age*, in *The Cambridge Handbook of Surveillance Law*, a cura di Gray - Henderson, Cambridge, 2017, 660, "*digital criminal evidence – evidence that would historically have been physically located in the same jurisdiction as the crime – is now very often stored in the cloud, and often with a service provider that is foreign*".

(17) Siracusano, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., 179; Soana, *L'accesso transfrontaliero alla prova informatica. Oltre il principio di territorialità*, cit., 257-258.

(18) Kasper-Lauritus, *Challenges in collecting digital evidence: a legal perspective*, cit., 197.

(19) Kasper-Lauritus, *Challenges in collecting digital evidence: a legal perspective*, cit.

(20) Gless, *Transnational Access to Evidence, Witnesses, and Suspects*, in *The Oxford Handbook of Criminal Process*, 2019, 8.

matica forense (21), il che diminuisce ulteriormente la comprensibilità della metodologia implementata. Tutto ciò implica la necessità di garantire un alto livello di trasparenza e tracciabilità della metodologia utilizzata, e pertanto della corrispondente catena di custodia, al fine di garantire la pienezza del contraddittorio nella giurisdizione ricevente, nonché l'effettività della funzione del giudice di guardiano della correttezza epistemologica del processo (22).

3. Catena di custodia e prova digitale. Un binomio necessario

La volatilità, fragilità e transnazionalità della prova digitale pongono l'accento sulla centralità della catena di custodia quale elemento chiave per evitare una completa abdicazione del controllo metodologico, nonché la verificabilità processuale ed extraprocessuale dei procedimenti forensi.

Pertanto è ora necessario analizzare questo istituto, al fine di delinearne gli elementi chiave e le funzioni. Secondo quanto statuito dall'Istituto Nazionale di Giustizia statunitense (NIJ), la catena di custodia è:

a process used to maintain and document the chronological history of the evidence. (Documents should include name or initials of the individual collecting the evidence, each person or entity subsequently having custody of it, dates the items were collected or transferred, agency and case number, victim's or suspect's name, and a brief description of the item) (23).

Partendo da questa definizione, la catena di custodia può, quindi, essere descritta come lo strumento utilizzato per tracciare la storia della prova ed, in particolare, per registrare il come, il quando, il chi di ogni fase probatoria in modo cronologico e continuativo, al fine di garantire la continua tracciabilità e verificabilità di qualunque interazione con la prova stessa, nonché delle sue condizioni di conservazione (24).

Da un punto di vista teleologico, la catena di custodia svolge due funzioni principali: in primo luogo, certificare che la prova prodotta in processo sia effettivamente la prova assunta in fase investigativa; in questo senso, la catena di custodia ha la funzione di evitare che possano verificarsi scambi di prove, o situazioni similari, e di certificare, quindi, l'identità della prova prodotta in processo (25). In secondo luogo, assicurare che non si verifichino modificazioni nel contenuto della prova stessa dall'assunzione fino alla produzione (26); questa seconda finalità evidenzia la funzione di garanzia giocata dalla catena di custodia rispetto all'integrità della prova (27): invero, mediante il tracciamento di ogni fase dell'indagine forense è possibile assicurare, nonché verificare *ex post*, l'integrità della prova e, conseguentemente, la sua utilizzabilità ai fini della ricostruzione processuale (28).

A tale fine è cruciale che la compilazione dei blocchi della catena di custodia non si esaurisca in un mero esercizio stilistico, bensì si sostanzi in una precisa e dettagliata indicazione di ogni azione eseguita dall'operatore e delle condizioni in cui la prova si trova in ogni momento; infatti, solo attraverso questa continuativa descrizione sarà possibile, per il giudice e le parti processuali, verificare l'integrità della prova e, conseguentemente, giudicarne l'ammissibilità (29).

In ambito di informatica forense la catena di custodia gioca anche un secondo ruolo parallelo a quello di garantire l'integrità della prova: permettere la revisionabilità delle metodologie utilizzate in un dato processo (30). Invero, la spasmodica evoluzione che caratterizza il settore informatico (31) e la relativa giovinezza di alcuni dei

(21) Aterno, *Digital Forensics e scena criminis*, cit., 790; Cass., 6 settembre 2012, n. 44851; Cass., 16 giugno 2015, n. 24998; Bartoli - Maioli, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, cit., 150; Cuomo, *La prova digitale*, cit., 674; Lupària - Ziccardi, *Investigazione penale e tecnologia informatica*, cit., 143.

(22) Biasiotti - Epifani - Turchi, *The evidence project: Bridging the gap in the exchange of digital evidence across Europe*, cit., 26, "*detecting of the existence of criteria and standards for guaranteeing reliability, integrity and chain of custody requirement of electronic evidence in the EU Member States and eventually in the exchange of it*".

(23) National Institute of Justice, *Glossary for Crime Scene Investigations: Guides for Law Enforcement*, 2009, all'indirizzo <https://nij.ojp.gov/topics/articles/glossary-crime-scene-investigation-guides-law-enforcement>. Altra possibile definizione è quella fornita dallo Scientific Working Group on Digital Evidence, *SWGDE Digital & Multimedia Evidence Glossary. Version 3.0*, cit., 5 che definisce la catena di custodia "*The chronological documentation of the movement, location and possession of evidence*".

(24) Siracusano, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., 179.

(25) Giannelli, *Chain of custody and the handling of real evidence*, in *American Criminal Law Review*, 1983, 531.

(26) Giannelli, *Chain of custody and the handling of real evidence*, cit., 533, "*in addition to showing that the object introduced in evidence is the same object as the one involved in the crime, the proponent of evidence must show that the object has retained its relevant evidentiary characteristics. Substantial alteration of the item reduces or negates its probative value and may mislead the jury*"; Burri - Casey - Bolle - Jaquet-Chiffelle, *Chronological independently verifiable electronic chain of custody ledger using blockchain technology*, cit., 1.

(27) Vaciago, *Digital Evidence*, cit., 70.

(28) Giova, *Improving chain of custody in forensic investigation of electronic digital systems*, in *International Journal of Computer Science and Network Security*, 2011, 1.

(29) Aterno, *Digital Forensics e scena criminis*, cit., 776.

(30) Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, cit., 709.

(31) Goodison – Davis - Jackson, *Digital evidence and the US criminal justice system*, cit., 13-14.

suoi ambiti comporta che le tecniche forensi a questa associate siano oggetto di frequenti, quanto fisiologiche, evoluzioni che possono portare all'identificazione di fragilità o perfino all'invalidazione della tecnica stessa.
Ora, mentre tale evoluzione è fisiologica (32), dato l'andamento per falsificazioni del processo scientifico, quando rapportata agli effetti definitivi e gravemente limitativi della libertà personale del procedimento penale richiede un'attenta valutazione. Tale valutazione è effettuata in sede processuale mediante il giudizio sulla validità della metodologia e soprattutto della nuova prova scientifica; d'altro canto, tale giudizio non può essere ritenuto una soluzione universale, data la necessaria temporaneità di qualunque giudizio in merito ad una metodologia scientifica, ancor più in ambito informatico.
È, pertanto, necessario garantire che in caso di avanzamenti tecnologici che falsifichino in maniera rilevante una tecnologia o metodologia utilizzata in un dato processo, quest'ultimo sia revisionabile per verificare la presenza di eventuali errori giudiziali. Tale revisionabilità è ovviamente sottoposta alla presenza di una chiara e dettagliata catena di custodia la quale permetta, *ex post*, di verificare le metodologie utilizzate nella data analisi forense e pertanto di giudicarne la fallacia e l'impatto di quest'ultima sul convincimento del giudice.
In quest'ottica la catena di custodia si pone quale traccia fondamentale per permettere l'audit dell'indagine forense e correggere eventuali errori giudiziari.

4. La legge 48/2008 di attuazione della Convenzione di Budapest

La particolare fragilità della prova digitale e le conseguenti maggiori necessità in ambito processuale sono state legislativamente cristallizzate mediante la l. 48 del 2008, con la quale si è data attuazione nell'ordinamento nazionale alla Convenzione di Budapest sulla criminalità informatica del 2001, apportando una serie di modifiche all'ordinamento penale, sia in ambito sostanziale, che processuale.
Con particolare riguardo all'ambito che qui interessa, la legge ha introdotto una serie di modifiche che vanno ben al di la di quanto previsto dalla Convenzione: in particolare, questa nulla prevede in ambito di integrità della prova digitale, salvo quanto statuito dall'articolo 19 della stessa su perquisizioni e sequestri informatici, dove si statuisce genericamente, al comma 3 lett. c, il dovere del legislatore di prevedere il potere delle autorità competenti di garantire l'integrità del materiale rilevante salvato su supporti informatici.
D'altra parte, se il testo normativo della Convenzione non prevede salvaguardie specifiche volte a garantire l'integrità e genuinità della prova digitale, le peculiarità di tale strumento probatorio non erano sfuggite al legislatore storico, il quale nella relazione esplicativa della Convenzione aveva chiaramente statuito che:

because of the volatility of computer data, the data is easily subject to manipulation or change. Thus, valuable evidence of a crime can be easily lost through careless handling and storage practices, intentional manipulation or deletion designed to destroy evidence or routine deletion of data that is no longer required to be retained.

Tale affermazione, seppur non direttamente vincolante, ben sottolinea la consapevolezza del legislatore storico in merito alle peculiarità della prova digitale ed ai maggiori rischi che questa soffre in ambito di possibili modificazioni volontarie o colpose, che possano compromettere il suo valore probatorio.
Il legislatore nazionale ha colto queste peculiarità, nel trasporre appunto la Convenzione ha previsto una serie di modifiche che vanno al di là di quanto espressamente previsto dalla Convenzione medesima. In particolare, la legge 48 del 2008, invece di introdurre disposizioni specifiche in ambito di prova informatica, ha apportato una serie di modifiche ai preesistenti articoli che disciplinano le varie fasi del procedimento investigativo. Tali modifiche hanno quale comune denominatore la previsione di un generico obbligo in capo agli investigatori di adottare, in ambito di prova digitale, misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione (33).
La previsione di tale obbligo generico ha suscitato perplessità in dottrina (34), dove si è sottolineata la peculiarità della tecnica legislativa adottata. D'altro canto, la previsione di una clausola generale ha quale vantaggio la sua adattabilità al mutevole panorama digitale, evitando l'obsolescenza della norma (35); invero, in questo modo

(32) Como sottolineato da Kuhn il progresso scientifico si caratterizza per un andamento rivoluzionario e non lineare, il che implica che la scoperta di nuove leggi scientifica non comporta solo un miglioramento delle teorie antecedenti ma una falsificazione dei postulati e della validità delle tesi precedenti; si veda Kuhn, *La struttura delle rivoluzioni scientifiche*, Torino, 2009.

(33) Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, 716; Cass., 6 settembre 2012, n. 44851; Bartoli - Maioli, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, cit., 145 ss.

(34) Si veda Bartoli-Maioli, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, cit.; Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, 760.

(35) Siracusano, La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione, cit., 189; Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, cit., 716, "*lo strumento della legge è sicuramente inidoneo a incorporare protocolli operativi che necessiterebbero di continui aggiornamenti*".

il legislatore imparte a tutti gli attori della fase investigativa e processuale una linea di condotta, segnalando le caratteristiche di questo specifico mezzo di prova ed imponendo una maggiore attenzione alle tecniche utilizzate nel procedimento forense per estrarre, analizzare e conservare la prova digitale. Inoltre, questa normativa rafforza il ruolo dell'organo giudicante di garante della correttezza epistemologica del processo, fornendogli una precisa direttiva interpretativa in ambito di valutazione metodologica della prova digitale.
La natura dinamica di questa modifica normativa permette inoltre un continuo adattamento dello standard giudizialmente richiesto alle migliori pratiche offerte dalla scienza forense del tempo imponendo, quindi, un'opera di continuo adeguamento degli investigatori agli stimoli provenienti dal progresso tecnologico.
Purtroppo, la giurisprudenza non ha completamente colto l'innovazione e l'opportunità offerta dalla modifica normativa ed ha anzi operato un rilevante ridimensionamento della portata innovativa di quest'ultima.
In particolare, la giurisprudenza della Cassazione, se ha da una parte riconosciuto che "è essenziale il mantenimento della integrità e non alterazione delle tracce "digitali" dei dati informatici, i quali devono essere acquisiti al processo, ed analizzati, attraverso l'estrazione di copia degli stessi ottenuta tramite una procedura che ne assicuri la conformità (36)", ha ridimensionato l'impatto pratico di tale modifica escludendo che, data l'assenza di sanzioni espresse in caso di violazione di queste disposizioni, da questa possa derivare un inutilizzabilità, bensì meramente una "valutazione in concreto della prova e quindi, nella specie, dell'eventuale avvenuta o meno alterazione dei dati originali e della corrispondenza o meno di quelli estratti a quelli originali (37)" rimettendo al libero convincimento del giudice la valutazione in merito all'effettiva modificazione della prova digitale e riconducendo all'alveo dell'attendibilità della prova eventuali violazioni.
Tale orientamento sottovaluta la necessaria autonomia del giudizio sulla metodologica rispetto a quella sostanziale sia per ragioni di ordine metodologico, in termini di necessaria scansione temporale e separazione del giudizio sulla metodologia rispetto a quello sulla sostanza, che per ragioni logiche ed in particolare di contaminazione del processo decisionale che tale commistione comporta.

5. Block-chain e RegTech. Un'introduzione

Introdotta nel 2008 dal fantomatico Satoshi Nakamoto quale tecnologia sottostante all'ormai celebre bitcoin (38), la block-chain ha conosciuto un intenso sviluppo nell'ultimo decennio, che ha portato ad una diversificazione non solo delle implementazioni, ma anche della struttura della block-chain stessa, la quale ha assunto in alcuni casi caratteristiche molto lontane dal modello tradizionale del bitcoin.
Nata come uno strumento di decentralizzazione del potere e della governance monetaria, quale reazione ai fallimenti del sistema bancario e finanziario resi evidenti dalla crisi del 2008 (39), la block-chain è stata via via adeguata agli interessi del mercato, cedendo alcuni caratteri di decentralizzazione in favore di un maggiore controllo centrale.
Il predetto sviluppo della block-chain impedisce una descrizione unitaria di questa tecnologia la quale è, invece, attualmente meglio descrivibile come una classe di tecnologie accomunate da una logica comune, le quali si pongono in uno spettro continuo da totalmente decentralizzate a totalmente centralizzate (40).
Proprio questo sviluppo è essenziale per il tema qui trattato, in quanto la struttura economica e normativa che caratterizza l'esercizio di funzioni pubbliche o para-pubbliche rende difficilmente praticabile l'implementazione di soluzioni basate sul modello tradizionale della block-chain pubblica e *permissionless*; invero, la necessità di mantenere un certo grado di controllo sulla governance e sui dati condivisi sulla block-chain da parte del decisore pubblico che voglia implementare tali soluzioni impone una mitigazione della decentralizzazione carat-

(36) Cass. 23 giugno 2015, n. 38148; nello stesso senso Cass. 21 settembre 2015, n. 38148, "*a seguito delle modifiche apportate con la L. del 18 marzo 2008, n. 48 (che ha ratificato la Convenzione Cybercrime del Consiglio d'Europa del 2001) le norme del codice di procedura penale disciplinano ora la "cristallizzazione della digital evidence" e tendono a garantire l'integrità dei dati, proprio nella consapevolezza della fragilità del dato informatico per la sua facile modificabilità, la possibilità della sua distruzione e la falsificabilità, con ciò confermando la assoluta peculiarità del dato informatico rispetto ad altri dati*".

(37) Cass. 12 febbraio 2014, n. 10618; si veda anche "*la disciplina in discorso non ha introdotto alcuna inutilizzabilità probatoria del dato acquisito (costituito, peraltro, nel caso di specie, da una mera stampa di una videata, frutto di un'operazione informaticamente elementare) senza il rispetto delle suddette procedure, che il giudice potrà valutare, secondo il principio del libero convincimento, al pari di qualsiasi altro documento*"; in Cass. 19 luglio 2016, n.9684 ed ancora "*L. 18 marzo 2008, n. 48, che ha introdotto unicamente l'obbligo per la polizia giudiziaria di rispettare determinati protocolli di comportamento, senza prevedere alcuna sanzione processuale in caso di mancata loro adozione, potendone derivare, invece, eventualmente, effetti sull'attendibilità della prova rappresentata dall'accertamento eseguito*"; in Cass. 19 luglio 2016, n.9684; Cass. 04 giugno 2015, n. 24998; si veda l'analisi di Lucattoni, *Per la Cassazione le regole di acquisizione del dato informatico introdotte dalla l. n. 48/2008 hanno natura solo programmatica*, in questa ***Rivista***, 2021, 355.

(38) Si veda Nakamoto, *Bitcoin: a peer-to-peer electronic cash system*, 2008.

(39) Forgang, *Money Laundering through Cryptocurrencies* in *Economic Crime Forensics Capstones*, 2019, all'indirizzo <https://digitalcommons.lasalle.edu/ecf_capstones/40>; Soana, *Criptovalute e Riciclaggio. Modus operandi e tentativi regolatori*, in questa ***Rivista***, 2019, 671.

(40) Shahaab et al., *Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review*, in *IEEE Access*, 2019, 2.

terizzante la block-chain disegnata da Nakamoto (41). Tale necessità è stata colta dalla dottrina e dal mercato i quali hanno proposto nel settore dell'integrità finanziaria e dell'efficientamento dei servizi pubblici soluzioni basate su block-chain private o consortili (42), a seconda del livello di centralizzazione desiderato (43).

Partendo dal modello primigenio, la block-chain del bitcoin permette di scambiare valore online in modo sicuro, senza la necessità di un terzo intermediario (44); il commercio su internet si basa quasi integralmente sull'intermediazione delle istituzioni finanziarie o di altri terzi garanti, quali soggetti che permettono scambi a distanza anche in assenza di fiducia reciproca tra le parti della transazione (45); il bitcoin inverte questo trend ,permettendo ai possessori di tale bene di scambiarlo direttamente senza alcun intermediario: da pari a pari (p2p). Ciò è reso possibile mediante la polverizzazione del ruolo del garante, che viene traslato dall'intermediario centralizzato – ovvero la banca, oppure il notaio – alla rete,affidando ad ogni utente (46) – c.d. nodo – della rete block-chain l'intero libro mastro delle transazioni e coinvolgendolo nel processo di attualizzazione di quest'ultimo; in questo modo, la block-chain scavalca l'intermediario creando un sistema di verificazione decentralizzata e competitiva, basato su centri di informazione distribuiti, invece che centralizzati. Tale sistema comporta una drastica riduzione dei costi di transazione, soprattutto in ambito transnazionale, ed una decisa diminuzione dei tempi necessari per trasferire valore a livello globale; inoltre, la decentralizzazione della block-chain la rende particolarmente resiliente ad attacchi informatici, in quanto non vi è un singolo punto di vulnerabilità – i.e. *single point of failure*.

Passando a descrivere gli elementi differenziali di tale modello primigenio, il bitcoin implementa una block-chain pubblica e *permissionless*, basata sulla logica di attualizzazione della *proof of work* (PoW) (47). Per pubblica e permissionless si intende che chiunque può divenire un nodo della rete block-chain e può leggere e scrivere nella block-chain stessa; non vi è pertanto alcun organo di controllo e/o di governo centralizzato, né alcuna forma di filtro all'ingresso per nodi ed utenti. Per quanto riguarda la *proof of work (48)*, tale modello di attualizzazione si basa su un sistema competitivo, il quale riconosce il diritto a creare un nuovo blocco ed aggiungerlo alla block-chain al soggetto – il c.d. *miner* – che impieghi una sempre maggiore potenza computazionale al fine di trovare l'*hash* corrispondente al nuovo blocco da creare. Questo tipo di block-chain è stata implementata dalla maggior parte delle cripto-valute, nonché da grandi piattaforme che forniscono servizi medianti block-chain, quali Ethereum (49), seppur con alcune deviazioni in termini di protocollo di consenso; d'altro canto questo tipo di tecnologia è di difficile implementazione quale strumento di gestione, condivisione ed archiviazione dei dati da parte di soggetti pubblici. Invero, come anzidetto, la natura pubblica del registro e l'assenza di alcuna forma di controllo in termini di gestione ed accesso ai dati è in conflitto con le necessità economiche e con gli obblighi giuridici – e.g. GDPR – ricadenti su tali soggetti (50); inoltre, l'utilizzo del *proof of work*, quale strumento di attualizzazione della block-chain, è estremamente dispendioso dal punto di vista energetico, con un rilevante impatto dal punto di vista economico ed ambientale (51).

Al fine di rispondere a questa diversa esigenza si è via via andato affermando un secondo tipo di block-chain, che

(41) Shahaab et al., *Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review*, cit., 10; Sim-De Caro, *Blockchain-based distributed compliance in multinational corporations' cross-border intercompany transactions*, cit., 511. Sui rischi della blockchain pubblica per privacy e copyright si veda Gabison, *Policy considerations for the blockchain technology public and private applications*, in *SMU Science and Technology Law Review*, 2016, 19, 330 e ss

(42) MacLeod Heminway-Sulkowski, *Blockchain, Corporate Governance and the Lawyer's role*, cit., 20. Tra tali proposte si veda tra i tanti Parra Moyano - Ross, *KYC optimization using distributed ledger technology*, in *Bus. Inf. Syst. Eng*, 2017; Hyva ̈rinen - Risius-Friis, *A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services*, in *Bus. Inf. Syst. Eng.*, 2017.

(43) Per una breve ed efficace descrizione della distinzione tra private e public blockchain si veda Jayachandran, *The Difference between private and public blockchain*, 31 Maggio 2017, all'indirizzo <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/>.

(44) Soana, *Criptovalute e Riciclaggio. Modus operandi e tentativi regolatori*, cit., 671.

(45) Nakamoto, *Bitcoin: a peer-to-peer electronic cash system*, 2008, 1.

(46) Merkx, *VAT and Blockchain: Challenges and Opportunities ahead*, in *EC Tax Review*, 2019, 83.

(47) Sebbene la proof of work sia il modello primigenio introdotto da Nakamoto, altri sistemi di attualizzazione sono stati proposti ed implementati nel tempo quali, ad esempio, la proof of stake (PoS); per una disamina di questi sistemi si veda Seibold - Samman, *Consensus – Immutable agreement for the internet Value*, 2016, KPMG, 3-7.

(48) Nakamoto, *Bitcoin: a peer-to-peer electronic cash system*, cit., 3.

(49) Su Ethereum si veda <https://ethereum.org/it/>.

(50) Campbell - Thompson - Ferry - Rudman, *Distributed Ledger Technologies in the Public Sector: Learnings on the application of Distributed Ledger Technologies across international public services and their role in realising Scotland's full potential in a digital world*, 2018, 22; Mohan, *State of public and private blockchains: Myths and reality*, in *Proceedings of the 2019 International Conference on Management of Data*, 2019, 1.

(51) Secondo le misurazioni effettuate dal Cambridge Centre for Alternative Finance dell'Università di Cambridge, la blockchain del Bitcoin consuma annualmente più energia della Svezia, e questa cifra è in continua crescita, per statistiche aggiornate si veda il Cambridge Bitcoin Electricity Consumption Index all'indirizzo <https://cbeci.org/>.

permette di mitigare la decentralizzazione del modello tradizionale adattandolo alle necessità dell'utente (52): la block-chain privata e *permissioned*, basata sulla logica di attualizzazione della *proof of authority* (PoA).
Per privata e *permissioned* si intende che l'accesso alla rete block-chain, sia in qualità di nodo, che in termini di diritto a leggere e scrivere, è sottoposta ad un'autorizzazione, che può essere rilasciata da un gestore, da un panel di gestori – in questo caso la rete viene denominata consortile – ovvero, nelle reti maggiormente decentralizzate, automaticamente dalla rete, sulla base di uno *smart contract*, all'avverarsi dei presupposti da questo prescritti; inoltre, in tali reti è possibile differenziare tra classi di utenti garantendo diritti di lettura e/o di scrittura limitati.
Per quanto riguarda la *proof of authority* questa, più che essere una caratteristica inerente a questo tipo di block-chain, che può comunque utilizzare altri protocolli di validazione quali la *proof of work* o la *proof of stake*, è una conseguenza del differente rapporto fiduciario esistente tra i partecipanti di una block-chain privata e *permissioned*; invero, a differenza della block-chain pubblica e *permissionless,* nata per permettere transazioni tra parti ignote e in assenza di vincoli di fiducia reciproca, in questo tipo di block-chain i partecipanti sono solo soggetti conosciuti ed approvati dal gestore della rete; da tale minore decentralizzazione degli utenti deriva anche una minore decentralizzazione dell'attività di *mining* che può essere affidata a soggetti predeterminati i quali svolgono la funzione di certificatori della validità dei nuovi blocchi sulla base, appunto, dell'autorità a questi conferita dall'organo di governance della rete.
Il differente rapporto di fiducia esistente tra i partecipanti alla rete cambia anche la funzione che in queste reti gioca la decentralizzazione; segnatamente, mentre nella block-chain tradizionale la decentralizzazione di controllo, accesso e *mining* sono strumenti per prevenire il comportamento opportunistico o fraudolento dei partecipanti e garantire transazioni sicure senza l'intervento di alcun terzo intermediario, nelle reti private e *permissioned* la decentralizzazione ha la funzione di consolidare la fiducia tra parti di un rapporto preesistente distribuendo controllo ed accesso alle informazioni, migliorando la qualità e la rapidità degli scambi di informazioni, eliminando asimmetrie informative, creando un registro unico ed immutabile degli scambi avvenuti tra tali parti e permettendo, infine, mediante gli *smart contracts*, di stabilire regole comuni la cui applicazione è automatica ed indipendente dalla volontà delle stesse (53). In questo senso, la block-chain privata ha un ruolo di consolidamento della fiducia, più che di sostituzione della stessa come avviene nelle block-chain pubbliche.
Nonostante gli indubbi vantaggi, perlomeno in determinati settori, assicurati dalla flessibile centralizzazione della governance garantita dalla block-chain privata e *permissioned*, la centralizzazione comporta alcuni rischi che devono essere attentamente valutati in sede di design di tali sistemi: in primo luogo, espone la rete alla possibile corruzione dell'organo di controllo nonché dei nodi di sua fiducia – in tal senso è fondamentale garantire che la rete sia formata da nodi i quali rappresentino interessi multipli e, possibilmente, concorrenti; in secondo luogo, il numero ridotto di nodi che tendenzialmente formano una block-chain privata diminuisce la resilienza della rete, soprattutto, se tali nodi sono tutti riconducibili ad una singola entità (54).

6. Il caso di studio: block-chain per la catena di custodia

Le criticità fin qui evidenziate sottolineano la necessità di individuare nuove soluzioni per migliorare l'attività di compilazione, conservazione e trasmissione della catena di custodia; svariati studi hanno evidenziato le potenzialità della block-chain, quale strumento per migliorarne la trasparenza e la tracciabilità (55): la scelta di questa tecnologia è ricollegabile alla sua attitudine a garantire la creazione di registri accessibili, trasparenti, immodificabili e tracciabili. Nonostante le varie proposte si differenzino tra loro è possibile estrapolare un modello di riferimento.
Partendo dalla configurazione della rete – data la necessaria centralità del decisore pubblico in ambito di indagini forensi e la natura riservata dei dati in oggetto – l'infrastruttura maggiormente adatta sembra essere quella della block-chain privata e *permissioned* (56). Inve-

(52) Mohan, *State of public and private blockchains: Myths and reality*, cit., 2.

(53) Finck, *Blockchain Regulation and governance in Europe*, Cambridge, 2018, 75-76; sull'utilizzabilità di smart contracts in ambito privacy si veda Ladia, *Blockchain: A Privacy Centered Standard for Corporate Compliance*, cit., 87-88.

(54) Finck, *Blockchain Regulation and governance in Europe*, cit., 196.

(55) Billard, *Block-chain based digital inventory*, cit.; Burri - Casey - Bolle - Jaquet - Chiffelle, *Chronological independently verifiable electronic chain of custody ledger using blockchain technology*, cit.; Lone-Roohie, *Forensic-chain: Ethereum blockchain based digital forensics chain of custody*, cit.; Li - Lal - Conti - Hu, *LEChain: A blockchain-based lawful evidence management scheme for digital forensics*, in *Future Generation Computer Systems*, 2021; Billard, *Weighted forensics evidence using blockchain*, in *Proceedings of the 2018 International Conference on computing and data engineering*, 2018.

(56) Burri - Casey - Bolle - Jaquet - Chiffelle, *Chronological independently verifiable electronic chain of custody ledger using blockchain technology*, cit., 2, "A *private blockchain only allows access to trusted parties, making it more suitable for use in criminal justice contexts and other situations involving*

ro, se da una parte questo sistema permette di garantire il controllo dell'infrastruttura al decisore pubblico e la segretezza dei dati, d'altra parte, ben si sposa con la finalità della tecnologia qui immaginata: creare una verità condivisa tra soggetti identificati e tra i quali già esiste un rapporto.
Nonostante quella della block-chain *permissioned* appaia come la scelta più adatta, è comunque necessario agire al fine di mitigare i summenzionati rischi derivanti dalla centralizzazione che contraddistingue questo secondo modello di block-chain. In tal senso, due misure di mitigazione possono essere prese congiuntamente o alternativamente: in primo luogo garantire la neutralità dell'organo di gestione della rete rispetto agli interessi espressi in ambito di catena di custodia; in quest'ottica il tribunale o una rete di tribunali, a seconda del design implementato, sembra la figura più adatta a svolgere questo compito, data la costituzionalmente demandata terzietà del giudice, nonché la sua funzione di garante della correttezza epistemologica del processo. Meno adatti sembrano gli organi investigativi, procura e polizia scientifica, per la loro posizione necessariamente partigiana in ambito investigativo, così come il Ministero della Giustizia dato il suo legame con il potere esecutivo.
In secondo luogo si potrebbe abbinare alla block-chain privata una block-chain pubblica, anche appoggiandosi a block-chain preesistenti, su cui salvare solamente gli *hash* dei singoli blocchi; in questo modo, se la riservatezza delle informazioni salvate sulla block-chain privata ed il suo controllo sarebbe pienamente preservata, lo stesso varrebbe per la sua immodificabilità, potendosi in ogni momento verificare la corrispondenza tra gli *hash* salvati sulla block-chain privata con quelli salvati sulla block-chain pubblica (57).
Passando ora ad analizzare la composizione della rete, al fine di garantire la necessaria accessibilità e il previsto effetto di miglioramento dell'efficienza informativa, è necessario che ad essa partecipino quantomeno il giudice, la procura, la difesa, la polizia e il laboratorio forense. La diretta partecipazione della difesa potrebbe porre problemi, soprattutto durante la fase investigativa, in termini di salvaguardia del segreto istruttorio, nonché di eccessiva trasparenza dell'attività investigativa; tale questione potrebbe essere risolta criptando i dati specificamente coperti da segreto e condividendo la password con la difesa solo quando le esigenze di secreto siano cessate. In questo modo si otterrebbe un duplice vantaggio: se gli investigatori vedrebbero preservate le esigenze di confidenzialità connaturate all'indagine penale, la difesa controllando gli *hash* dei blocchi potrebbe continuamente sincerarsi in merito all'immodificabilità di questi ultimi e, pertanto, della genuinità delle informazioni condivise.
Da un punto di vista dinamico il sistema si baserebbe, pertanto, sulla creazione da parte di ogni operatore che abbia contatto con la specifica prova di un blocco della catena contenente tutte le informazioni necessarie; questo creerebbe una catena di blocchi consequenzialmente e cronologicamente vincolati, immodificabili una volta creati e accessibili in maniera diretta da ogni nodo della rete.
La registrazione di queste fasi potrebbe essere ulteriormente velocizzata ed automatizzata data la natura digitale della prova e della correlata analisi forense. Invero, come nel caso cinese che sarà successivamente illustrato, il sistema potrebbe muoversi parallelamente al software di analisi forense, registrando automaticamente ogni azione del tecnico e trasponendola autonomamente sulla block-chain, in modo da garantire l'affidabilità del sistema nonché alleviando il carico burocratico collegato all'attività dell'esperto.
Un esempio può facilitare la comprensione del funzionamento di questo sistema; immaginiamo che la procura pianifichi una perquisizione nei confronti di un soggetto sospettato di detenere materiale pedopornografico. A questo punto il pubblico ministero creerebbe il primo blocco includendo la base giuridica, identificando l'oggetto della perquisizione etc. Il secondo blocco verrebbe creato dal tecnico della polizia scientifica, il quale descriverebbe la procedura di perquisizione (software utilizzato, oggetto etc.), data, ora, identificazione dell'operatore etc. Poi, se sul computer dovesse essere rinvenuto del materiale pedopornografico, il tecnico procederebbe all'acquisizione dello stesso creando un ulteriore blocco e così via per ogni fase della catena di custodia. Al momento della produzione giudice e difesa, ed i loro periti, potrebbero accedere alla catena di custodia direttamente e semplicemente, potendo in tal modo valutare ed, eventualmente, provare a falsificare il lato metodologico della prova addotta in processo fondandosi su una base informativa chiara, trasparente ed affidabile.

7. Ricadute processuali ed extraprocessuali

L'adozione del summenzionato sistema avrebbe ricadute dirette in termini di efficientamento della gestione della prova digitale e di certezza del diritto, le quali rendono questa soluzione un'opzione attrattiva per il legislatore nel quadro della digitalizzazione dell'apparato statale, nonché del progressivo adattamento del diritto sostanziale e processuale alle sempre più pressanti istanze della

sensitive information"; .; Li - Lal - Conti - Hu, *LEChain: A blockchain-based lawful evidence management scheme for digital forensics*, cit., utilizzano una blockchain consortile; Lone - Roohie, *Forensic-chain: Ethereum blockchain based digital forensics chain of custody*, cit.

(57) Come proposto da Burri - Casey - Bolle - Jaquet - Chiffelle, *Chronological independently verifiable electronic chain of custody ledger using blockchain technology*, cit.

rivoluzione digitale. Inoltre, tale implementazione tecnologica è in linea con la chiara indicazione legislativa di adottare misure tecniche volte ad "assicurare la conservazione dei dati originali e ad impedirne l'alterazione" e costituirebbe, pertanto, un'innovativa forma di attuazione della volontà legislativa. Invero, essendo la catena di custodia lo strumento internazionalmente riconosciuto per la preservazione della correttezza epistemologica della prova scientifica, l'implementazione di un sistema che ne garantisca l'immutabilità, accessibilità e tracciabilità costituirebbe la massima realizzazione dello standard legislativamente demandato.

Dal punto di vista strettamente endoprocessuale l'adozione di tale sistema avrebbe tre vantaggi molto evidenti. In primo luogo, la possibilità per il giudice di avere accesso diretto ad un registro affidabile e trasparente che descriva il procedimento forense seguito per una determinata prova rafforzerebbe il ruolo di quest'ultimo di guardiano della correttezza epistemologica del processo. Mediante il registro block-chain il giudice avrebbe una fonte informativa unica ed affidabile per svolgere la propria valutazione in merito alla validità metodologica della prova, nonché per valutare la correttezza e coerenza dei ragionamenti sviluppati dal perito e dai consulenti tecnici di parte. Inoltre, se l'accessibilità immediata da parte del giudice ridurrebbe i costi e i ritardi dovuti alla necessità per l'accusa di trasferire le informazioni al giudice ed alla difesa, la trasparenza e affidabilità del registro diminuirebbe la contestabilità della catena di custodia, creando una base conoscitiva condivisa sulla base della quale sviluppare le argomentazioni di parte.

In secondo luogo, la pienezza ed efficacia del contraddittorio processuale risulterebbe fortemente rafforzata con speciale riguardo al diritto della difesa di contraddire la validità e correttezza epistemologica delle prove digitali prodotte in processo. Invero, mediante il sistema block-chain la difesa, invece di dover dipendere dall'accusa per ottenere la catena di custodia, avrebbe accesso diretto alle informazioni beneficiandone sia in termini di affidabilità di queste ultime – data la loro controllabilità, seppur nei soli termini di immodificabilità, anche in fase di indagine – che di rapidità di accesso. Inoltre, la trasparenza e comprensibilità di tale sistema di formazione della catena di custodia permetterebbe di analizzare in maniera piena e completa la correttezza metodologica della prova prodotta, garantirebbe di preservare il principio della parità delle armi, nonché la pienezza del diritto di difesa. Mediante questo sistema si creerebbe, almeno in ambito di catena di custodia, una situazione di equilibrio informativo tra tutti gli attori processuali con dirette ricadute in termini di efficienza ed affidabilità. In questo modo, inoltre, lo standard giurisprudenziale per cui sta alla difesa addurre i motivi sulla base dei quali la prova risulta epistemologicamente fallace, e pertanto inutilizzabile, diverrebbe accessibile data l'effettiva controllabilità per parte della difesa di ogni fase del processo forense.

In terzo luogo, questo sistema contribuirebbe a risolvere il problema della restituzione del dato informatico sottoposto a sequestro. Questa è una tematica molto frequente in ambito di prova digitale, data l'ontologica duplicabilità (58) di quest'ultima nonché la frequente ampiezza dei sequestri di dati digitali; questi due elementi comportano che, da una parte, l'organo investigativo si trovi in possesso di una grande quantità di dati di cui una buona parte irrilevanti ai fini investigativi (59), d'altra parte che la restituzione dei dati non interrompa il vincolo sul bene (60), e pertanto l'interesse alla restituzione, nel caso in cui questo sia stato duplicato e la copia permanga nella disponibilità delle autorità investigative. Tale principio è stato chiaramente affermato dalla Suprema Corte la quale ha statuito che "è ammissibile il ricorso per cassazione avverso l›ordinanza del tribunale del riesame di conferma del sequestro probatorio di un computer o di un supporto informatico, nel caso in cui ne risulti la restituzione previa estrazione di copia dei dati ivi contenuti, sempre che sia dedotto l›interesse, concreto e attuale, alla esclusiva disponibilità dei dati" (61). Da ciò consegue che in caso di prova digitale

(58) Come affermato da Cass. 27 ottobre 2016, n.25527 "È *stato evidenziato che il concetto stesso di copia perde di significato nel caso del documento informatico: la riproducibilità globale, l'indistinguibilità della riproduzione, la sostanziale indifferenza del supporto, rispetto al "dato originale", rendono irrilevante la diversità concettuale tra dato riprodotto ed il suo originale, tanto che si è suggerito di sostituire per il documento informatico il concetto di "duplicato" a quello di "copia""*; Cuomo, *La prova digitale*, cit., 683, 696 "*la nozione di originale e di copia perdono significato per la natura intrinseca dei documenti elettronici che, dotati della corporalità propria del bit, non si distinguono in nulla rispetto alle informazioni orginarie*"; Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, 700.

(59) Cuomo, *La prova digitale*, cit., 682; Goodison - Davis - Jackson, *Digital evidence and the US criminal justice system*, cit., 9, "*courts have recognized that the initial seizure may, of necessity, be overly broad and include much information not covered by the search warrant. Therefore, there needs to be a second stage in which law enforcement agents examine the data seized and cull the information specifically covered under the search warrant*"; Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, cit., 713.

(60) Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, cit., 714.

(61) Si veda Cass. 27 ottobre 2016, n.25527, "*in tema di sequestro probatorio, la restituzione, previo trattenimento di copia dei dati informatici estratti, dei beni materiali (server, computer e "hard disk") coercitivamente acquisiti per effettuare le operazioni di trasferimento dei dati, non comporta il venir meno del vincolo, con la conseguenza che permane l'interesse a richiedere il controllo giurisdizionale sulla legittimità del sequestro al competente tribunale del riesame*"; ed ancora "*pertanto le disposizioni introdotte dalla L. n. 48 del 2008 riconoscono al "dato informatico", in quanto tale, la caratteristica di oggetto del sequestro, di modo che la restituzione, previo trattenimento di copia, del supporto fisico di memorizzazione, non comporta il venir meno del sequestro quando permane, sul piano del diritto sostanziale, una perdita autonomamente valutabile per il titolare del dato mentre, nel caso in esame, tale dimostrazione non è stata in alcun modo fornita non avendo i ricorrenti in alcun modo dimostrato che i dati informatici*

il soggetto passivo abbia un vero e proprio diritto esclusivo all'informazione, conseguibile solamente mediante la cancellazione del dato da parte delle autorità investigative; ora, verificare l'effettiva cancellazione risulta operazione complessa. L'utilizzo della block-chain permetterebbe al soggetto passivo ovvero al giudice di verificare direttamente l'avvenuta cancellazione del dato e, pertanto, l'effettiva cessazione del vincolo reale.
Passando al livello extraprocessuale, l'implementazione di questa tecnologia avrebbe due vantaggi evidenti. Da una parte, l'adozione del sistema block-chain migliorerebbe l'efficienza della circolazione transnazionale delle prove migliorando la comprensibilità e comunicabilità degli apporti probatori. Invero, come summenzionato, data l'ontologica transnazionalità della prova digitale, la sua circolazione internazionale è divenuta una modalità abituale per l'assunzione della stessa. Per evitare che tale circolazione comporti una sostanziale impossibilità per gli attori processuali di comprendere, e quindi valutare, la correttezza metodologica della prova addotta in processo è cruciale che questa sia corredata da una catena di custodia comprensibile e, soprattutto, affidabile. Mediante la block-chain compartire questa catena sarebbe estremamente semplice, data la possibilità di includere quale nodo con diritto di lettura per quella singola catena l'autorità investigativa o giudiziaria del paese ricevente ovvero semplicemente di condividere una copia della catena; permettendo, in questo modo, alla giurisdizione ricevente di avere rapidamente un quadro chiaro e comprensibile. Inoltre, con la progressiva adozione da parte di differenti giurisdizioni di sistemi block-chain per la registrazione della catena di custodia si potrebbero stabilire standard comuni al fine di permettere l'interoperabilità dei sistemi.
D'altra parte, l'utilizzazione di un registro block-chain immutabile per la conservazione delle catene di custodia semplificherebbe la revisione *ex post* della correttezza metodologica di una determinata prova e pertanto del processo in cui questa è stata utilizzata. Questo è un elemento di particolare interesse, in quanto il progresso tecnologico comporta un continuo aggiornamento delle tecnologie e delle metodologie utilizzate seguendo un percorso non lineare, bensì ciclico; ciò implica che il progresso spesso comporta la falsificazione di una determinata metodologia ovvero la scoperta di debolezze precedentemente sconosciute. Data l'indiscutibile funzione del progresso scientifico per l'efficiente funzionamento della repressione penale è, d'altro canto, necessario garantire che in caso di utilizzazione a fini processuali di metodologie, che poi si rivelino totalmente o parzialmente fallaci, sia possibile valutarne l'impatto sull'esito processuale e poter porre rimedio. La block-chain data la sua tracciabilità, immodificabilità e trasparenza fornisce una base unica per compiere attività di audit delle analisi forensi in un dato procedimento (62).

8. La *Hangzhou Judicial Block-chain Platform*

L'implementazione di cui si è finora discorso è già parzialmente realtà in Cina; invero, seppur non nell'ambito penale, la Hangzhou Internet Court ha implementato a partire del 2018 un sistema block-chain (63) per permettere alle parti di produrre prove in giudizio in maniera diretta e senza la necessità di fornire prova dell'autenticità della prova stessa (64).
Scopo precipuo di tale infrastruttura tecnologica è facilitare l'ammissibilità delle prove, semplificare la comprensibilità e l'accessibilità per i giudici nonché ridurre tempi e costi per le parti. Il sistema in argomento si basa su una block-chain consortile a cui partecipano i tribunali, le autorità di certificazione etc. (65)
Dal punto di vista dinamico (66), questo sistema si struttura mediante un'interfaccia per l'utente il quale per produrre una prova in giudizio può accedere a tale interfaccia e navigando mediante quest'ultima individuare la prova (si pensi ad esempio ad una pagina web che si alleghi in violazione del diritto d'autore). L'interfaccia registra ogni passaggio in maniera automatica sulla block-chain generando *hash* corrispondenti sulla block-chain e la creazione di blocchi successivi e consequenziali. La block-chain in questo sistema pertanto contiene esclusivamente gli *hash* di ogni fase del procedimento di acquisizione e non il contenuto della prova stessa; la prova verrà poi condivisa dalla parte con il tribunale che potrà verificarne la corrispondenza con quanto salvato sulla block-chain a cui ha accesso diretto (67).
Ai nostri fini tale sistema testimonia la utilizzabilità e adeguatezza della block-chain, quale tecnologia per la

contenuti negli apparecchi e nelle strutture hardware di cui si è disposta la copia avessero per gli stessi rilievo sotto il profilo dell'importanza della esclusiva disponibilità dell'informazione contenuta, tal da fare ritenere detta operazione di copia un vero e proprio sequestro di "informazione" autonomamente apprezzabile" in Cass. 09 settembre 2016, n. 40831.

(62) Lone - Roohie, *Forensic-chain: Ethereum blockchain based digital forensics chain of custody*, cit., 52.

(63) Wu - Zheng, *Electronic Evidence in the Blockchain Era: New rules on authenticity and integrity*, cit., 8.

(64) Liu, *The Implementation of Blockchain Technologies in Chinese Courts*, cit., 10.

(65) Liu, *The Implementation of Blockchain Technologies in Chinese Courts*, cit., 10; Wu - Zheng, *Electronic Evidence in the Blockchain Era: New rules on authenticity and integrity*, cit., 8.

(66) Si veda Liu, *The Implementation of Blockchain Technologies in Chinese Courts*, cit., 12-14.

(67) Liu, *The Implementation of Blockchain Technologies in Chinese Courts*, cit., 14.

creazione e custodia della catena di custodia di prove digitali al fine di migliorarne l'affidabilità ed accessibilità nonché per ridurre i costi ed automatizzare i processi burocratici.

9. Conclusione

In un mondo sempre più immerso e dipendente dagli strumenti tecnologici la prova digitale ha assunto un ruolo primario al fine di garantire l'accertamento dei fatti in ambito penale. Tale, necessità comporta di adattare i procedimenti forensi alle peculiarità di questa prova la quale si caratterizza per la sua fragilità, volatilità e transnazionalità.

Al fine di preservare il principio del contraddittorio nonché la comprensibilità degli apporti probatori per giudice e parti è necessario garantire la trasparenza ed accessibilità della catena di custodia. Invero, questo strumento costituisce un elemento essenziale per garantire la correttezza metodologica del procedimento forense, nonché per permetterne la verificabilità e revisionabilità da parte degli attori processuali.

Tali nuove necessità sono state colte in pieno dal legislatore italiano il quale ha introdotto una normativa specifica, superando quanto previsto dalla normativa internazionale, proprio volta a stimolare e dirigere l'attività forense e processuale verso una maggiore cautela nella gestione e conservazione della prova digitale. Tale indirizzo segnala chiaramente la volontà del legislatore di far emergere le peculiarità della prova digitale e di garantire che queste non incidano sulla correttezza epistemologica dell'accertamento processuale.

In quest'ottica, è lo stesso progresso tecnologico a poter fornire una soluzione; in particolare, la tecnologia block-chain mediante il suo registro immodificabile, trasparente, consequenziale e distribuito potrebbe facilitare l'affidabilità ed accessibilità della catena di custodia sia in ambito nazionale che nella sua dimensione transnazionale; inoltre, l'implementazione di *smart contracts* potrebbe automatizzare il processo di creazione della catena di custodia diminuendo il carico burocratico gravante sulla polizia scientifica e garantendo l'assoluta terzietà del registro stesso. Infine, l'utilizzazione della block-chain migliorerebbe la possibilità di condurre audit del procedimento forense utilizzato per una specifica prova e, in caso di sostanziali modificazioni del quadro scientifico di riferimento, avere una base informativa forte per poter procedere alla revisione della sentenza.