La catena di custodia della digital evidence

In linea generale, una volta raccolto il reperto dalla scena del crimine sorge l'esigenza di conservarne l'originale autenticità in tutti i passaggi successivi – anche mediante documentazione dei singoli spostamenti e indicando chi vi entra in contatto – affinché possa giungere inalterato sino al dibattimento e affinché, in tale sede, possa esserne opportunamente verificata l'attendibilità, valutando la corretta applicazione dei principi cardine della c.d. catena di custodia, espressione con cui «*vengono indicati l'insieme di passaggi, formalizzati con un sistema di tracciamento (manuale o elettronico), attraverso i quali il reperto, o meglio i plichi ed i confezionamenti in cui è conservato, transita dalla scena del crimine alla fase del giudizio*»[1].

In altre parole, la catena di custodia è la «*documentazione cronologica che mostra la conservazione dei reperti dal momento della raccolta a quello della produzione in giudizio*»[2] e che permette in sede giudiziale di poter valutare l'attendibilità del reperto sotto i profili della sua integrità e genuinità, o meglio di verificare che durante tutti i passaggi che hanno coinvolto il reperto sia stato salvaguardato l'insieme di informazioni che intrinsecamente possiede[3].

Alla necessità di rispettare i principi della catena di custodia, basilari per la buona riuscita dell'indagine, non fa eccezione nemmeno la prova informatica; caratterizzata, inoltre, da una fragilità che impone un'attenzione ancora maggiore onde impedirne modificazioni involontarie.

Esaurita, dunque, la fase di acquisizione dei dati dal supporto oggetto d'investigazione, le *digital evidence*

ottenute devono essere salvaguardate per garantire il loro ingresso all'interno del processo nello stesso stato nel quale sono state rinvenute. A tal fine occorrerà conservare adeguatamente sia la copia forense che tutte le altre copie che potranno essere estratte a partire da quest'ultima.

Allo stesso modo, al fine di assicurare l'integrità dell'intero quadro probatorio, occorre che anche rispetto al supporto originale siano dettagliatamente documentati gli spostamenti e le fasi operative o conservative che lo interessano, dal suo rinvenimento fino al giudizio.

Nonostante la centralità di questa fase, esattamente come avviene per l'acquisizione, non è però rinvenibile una normativa atta a disciplinarne con chiarezza i passaggi.

La sola disposizione cui è possibile fare riferimento, infatti, è contenuta nel comma 2 dell'art. 260 c.p.p., rubricato "*apposizione dei sigilli alle cose sequestrate. Cose deperibili. Distruzione di cose sequestrate*"[4], dove non viene indicata una procedura precisa ma è unicamente previsto che "*quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità…*".

Anche in questo caso la strategia del legislatore, stando alla terminologia adoperata, è lasciare la possibilità di fare ricorso alle *best practices* indicate dalle linee guida internazionali, senza imporre modalità attuative già predeterminate agli operatori.

Anche in questo caso però il ricorso alle migliori pratiche, stante l'omissione dell'indicazione di precise conseguenze in caso di violazione, non sembrerebbe comportare conseguenze sul piano della validità del reperto informatico.

Per la giurisprudenza, in particolare, la disposizione non

imporrebbe modalità di custodia obbligatorie, contenendo direttive puramente indicative e di conseguenza derogabili sia per ragioni di assoluta impossibilità che di opportunità. Pertanto, scelte operative inidonee potrebbero avere effetto solo sotto il profilo della valutazione della prova *ex* art. 192 c.p.p., senza alcuna ripercussione nell'ottica della nullità o inutilizzabilità processuale del reperto digitale[5].

In buona sostanza, la giurisprudenza, ha riadattato le medesime conclusioni alle quali era già pervenuta in tema di acquisizione di *digital evidence*, sdoganando – anche nella fase della catena di custodia – il principio in base al quale il mancato rispetto di buone pratiche non costituisce automaticamente motivo di invalidità della prova informatica, potendo semmai costituire uno strumento per calibrare il peso giudiziario dell'elemento probatorio. È chiaro che in ogni caso, al fine di non incappare in un vizio motivazionale, il giudice in sentenza resta vincolato al dovere di evidenziare le motivazioni che lo hanno addotto a prendere in considerazione elementi di prova provenienti da processi investigativi derogatori dei principi della catena di custodia.

Non vi è dubbio, comunque, che il rispetto delle indicazioni elaborate dagli *standard* internazionali fornisca un alto grado di attendibilità al reperto informatico, essendo pertanto detti principi, seppur non cogenti, diffusi nelle prassi operative. Ciò perché seguire tali principi per la custodia dei dati rende di fatto possibile, anche in momenti successivi, verificare l'autenticità del materiale informatico raccolto che potrà essere direttamente visionato, nonché pienamente conosciuto, sia dalle parti sia dal giudice stesso[6].

Dal punto di vista tecnico, nella *digital forensics*, la catena di custodia si concretizza consiste in un documento all'interno del quale viene riportata, oltre alla descrizione

del reperto digitale, ciascuna operazione svolta in relazione al medesimo con l'indicazione del momento di svolgimento (data e ora) e del soggetto materialmente intervenuto. Altre informazioni possono riguardare gli spostamenti, il luogo di custodia e le modalità con la quale questa viene attuata[7].

In termini pratici, all'interno di tale documento viene descritto l'intero arco di vita della *digital evidence* nel contesto investigativo, dal momento della sua raccolta alla presentazione innanzi all'autorità giudiziaria[8].

Per garantire il corretto funzionamento del meccanismo di conservazione è altresì necessario provvedere all'apposizione dei sigilli sia sul dispositivo originale, sia sui supporti contenenti le copie forensi[9].

Un'eventuale compromissione del sigillo potrà infatti rivelare una possibile manomissione dell'evidenza elettronica, con conseguente inattendibilità del materiale probatorio sul piano processuale.

La peculiarità della *digital forensics*, inoltre, impone di ragionare sul concetto di protezione dell'evidenza digitale da fattori esterni, con ciò intesi fenomeni provenienti da fonti estranee all'evidenza digitale e al supporto che la ospita ma capaci di influenzarne irrimediabilmente l'integrità e capaci di alterazioni da remoto, *bypassando* il sistema di sigilli fisico (pertanto molto complessi da individuare).

La questione della protezione della *digital evidence* dal pericolo di aggressioni ha ricevuto l'attenzione dei più importanti *standard* internazionali, tra i quali risalta l'ISO/IEC 27037:2012.

In particolare, le linee guida offerte da quest'ultimo si focalizzano sulla necessità di tutelare il dato informatico da fenomeni di perdita (*loss*), manomissioni (*tampering*) e distruzioni (*spoliation*) di informazioni, durante la fase di

raccolta, trasporto e stoccaggio nel luogo finale di conservazione.

Infatti – prelevata la possibile prova dalla scena del crimine – occorre fare in modo che questa, una volta confezionata, giunga nel sito di deposito senza subire contaminazioni. È proprio un opportuno confezionamento o impacchettamento del materiale probatorio rinvenuto che scongiura quanto più possibile il prodursi di fenomeni deteriorativi, che possono provenire sia da condizioni naturali che da attività dolose o colpose (come ad esempio errori involontari degli operatori).

Le cause di deterioramento naturale che possono colpire il dato digitale possono riguardare fenomeni ambientali (ad esempio l'umidità, che come risaputo danneggia i sistemi elettronici, fonti di calore oppure, qualora il reperto si trovi all'aperto, pioggia e condizioni atmosferiche in generale: dalla grandine che potrebbe colpire la componente *hardware,* ai fulmini che potrebbero mandare in *tilt* il sistema).

I fenomeni volontari, invece, possono consistere sia in danneggiamenti fisici prodotti direttamente sul supporto informatico sia in attacchi da remoto mediante accesso abusivo al sistema. Si pensi a dispositivi accesi con sistema *bluetooth* attivato, collegati ad altri dispositivi o direttamente connessi alla rete, dove qualsiasi utente in linea può rappresentare un rischio concreto di alterazione. Infine, occorre tenere presente l'alta sensibilità degli apparecchi elettronici nei confronti di campi elettromagnetici, onde radio e in generale frequenze generate da altri sistemi elettronici che potrebbero interferire irreversibilmente sull'integrità del dato, se non addirittura rendere inservibile il supporto dove è registrato.

Durante la fase di trasporto dell'evidenza digitale, pertanto, è necessario adottare strategie protettive utilizzando strumenti capaci di isolare il dispositivo prelevato dal mondo

esterno, sia fisico che digitale.

Per i motivi sopra visti, infatti, non è sufficiente riporre l'elemento di prova informatico all'interno di comuni confezioni, come buste di carta o contenitori di plastica, utilizzati ad esempio per l'impacchettamento dei reperti biologici, ma sono necessarie tutele specifiche con l'ausilio di strumenti adeguati.

Tra le diverse soluzioni vi è l'inserimento del supporto prelevato all'interno di una gabbia di *Faraday*, ovvero un particolare contenitore composto da materiale elettricamente conduttore in grado di schermare le onde elettromagnetiche e le frequenze radio esterne, così rendendo impossibile l'interazione tra il dispositivo elettronico in esso contenuto e apparecchi o campi elettrostatici esterni[10].

Un altro strumento – per ovvi motivi di difficile impiego nella pratica – è il c.d. *jammer*, capace di inibire temporaneamente la funzione di emissione e ricezione delle onde radio degli apparecchi elettronici che si trovano all'interno del suo raggio d'azione, rendendo in questo modo impossibile comunicazioni tra questi e il supporto prelevato[11].

Simili strategie, chiaramente, devono essere adottate anche successivamente alla fase di trasporto e più propriamente all'interno del luogo di stoccaggio, dove oltre all'emarginazione del dispositivo dall'esterno potrebbero essere adoperati sistemi di videosorveglianza e sistemi altri accorgimenti per rendere inaccessibile a soggetti non autorizzati l'ingresso ai locali di custodia.

Nonostante tutti gli accorgimenti adottabili sul piano della sicurezza, preme sottolineare come il rischio di alterazione non sia mai completamente eliminabile[12]; talvolta, quindi, potrebbe rendersi necessario analizzare direttamente il

supporto repertato per verificare che non vi siano state manomissioni o accessi da persone non autorizzate durante le fasi di raccolta, trasporto e conservazione.

In tali evenienze, procedere con dei controlli mirati si rivelerebbe quindi un utile strumento di garanzia ai fini dell'attendibilità del reperto, che – seppure trattato con la massima precauzione,– soggiace sempre, anche se in percentuali bassissime, al rischio di subire violazioni.

In particolare, a talune condizioni, con l'ausilio di appositi *software* è possibile ricostruire la *timeline* del dispositivo[13], per verificare che essa coincida con la sequenza cronologica di utilizzo come descritta nel documento della catena di custodia.

In estrema sintesi, nella *digital forensics* la catena di custodia costituisce un sistema procedurale che, seppure non obbligatorio sul piano giuridico, si rivela essenziale per il corretto esito delle indagini.

Il rispetto dei relativi principi e il corretto uso della strumentazione atta alla protezione del dato informatico, infatti, garantiscono la possibilità di condurre verifiche *ex post* sulla vita investigativa del reperto digitale.

Tutto ciò, nell'ottica del giusto processo, consente di consegnare nelle mani dei soggetti coinvolti nella dinamica giudiziale la possibilità di verificare in totale trasparenza l'integrità e l'autenticità del materiale probatorio.

Questo articolo è stato estratto dal white paper "**La Digital forensics nel processo penale**" disponibile in maniera libera e gratuita al seguente link: https://www.ictsecuritymagazine.com/pubblicazioni/digital-forensics-nel-processo-penale/

Note

[1] R. GENNARI e L. SARAVO, "*Tecnica, tecnologia e scienza sulle tracce del reato – Le tracce*", in *Manuale delle investigazioni sulla scena del crimine*, cit., p. 496, dove gli autori specificano che la catena di custodia è meglio nota con il nome inglese "*chain of custody*". Effettivamente, preme sottolineare come tale fase dell'investigazione forense sia propria degli sviluppi avutisi in tale settore nella prassi dei paesi anglosassoni e in particolare in quella dell'ordinamento nordamericano. Su quest'ultimo aspetto si veda R. MURENEC, op. cit., p. 128, nota (269).

[2] F. COLAIUDA, "*La qualità dell'investigazione sulla scena del crimine – il metodo di lavoro basato sui protocolli operativi e sulle check lists*", p. 1, consultabile sul sito http://www.associazionelaic.it/wp-content/uploads/2018/07/Colaiuda-3.pdf.

[3] R. GENNARI e L. SARAVO, op. cit., p. 497, dove dopo aver individuato quale obiettivo della catena di custodia la salvaguardia delle informazioni contenute dal reperto si precisa che la protezione afferisce a tre aspetti: quello «*Scientifico dovuto alla necessità di preservare le tracce da fenomeni degenerativi e degradativi, nonché da possibili contaminazioni*» (si aggiunge che in ottica di *digital forensics* potrebbe tradursi come la necessità di evitare alterazioni del dato digitale); quello «*Formale*» per il quale «*tutte le fasi di custodia, dal repertamento alle analisi di laboratorio, devono essere opportunamente documentate* […] al fine di] *garantire che non vi sia pericolo di scambio e che per l'oggetto e le informazioni in esso contenute non vi possano essere altre provenienze al di fuori di quella documentata*»; quello «*Processuale* [che] *scaturisce dalla necessità di garantire in qualsiasi fase dell'accertamento, a partire quindi dall'ambito nel quale ha origine il reperto,*

l'acquisizione e la perfetta gestione della fonte di prova scevra da qualsiasi pericolo di manipolazione o ipotesi di manipolazione che ne potrebbe diminuire il valore probatorio».

[4] Si veda sul punto anche R. MURENEC, op. cit., pp. 128 e 129, dove viene fatto apposito rimando a quanto previsto da detta disposizione ai fini di garanzia dell'attendibilità e inalterabilità della prova informatica.

[5] D. CURTOTTI, "*Il sequestro*", in "*Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici*", cit., p. 475, dove si legge: «*Si dica subito che le modalità di custodia delle cose sequestrate indicate dall'art. 260 costituiscono, per la giurisprudenza, prescrizioni meramente indicative che, da un lato, sono derogabili per ragioni di assoluta impossibilità o di opportunità, e, dall'altro lato, non sono astrattamente contestabili, tranne che nel caso in cui dalla loro mancata applicazione vogliano dedursi inconvenienti sostanziali attinenti a concrete ipotesi di alterazione, modificazione o sostituzione dei reperti. Ne consegue che l'inosservanza delle norme non è sanzionata da alcuna ipotesi di nullità ma può incidere unicamente sul diverso profilo della valutazione della genuinità della prova, secondo le regole generali dettate dall'art. 192 c.p.p.*».

[6] Si veda L. BARTOLI e C. MAIOLI, "*La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*", in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 141, dove trattando dell'importanza della trasparenza nella *digital forensics* e nella catena di custodia si precisa che «*Un'avvertenza preliminare sembra però opportuna: né le migliori tecniche né le più inespugnabili costruzioni normative possono eliminare in radice il pericolo di errori, perdite o incertezze. Alle norme spetterà il compito di salvaguardare, allora, non tanto la certezza dell'autenticità, quanto la trasparenza del percorso, l'occasione di conoscerne i passaggi. Per il giudice e le parti sarà così possibile*

smascherare i più malsicuri, considerarne il margine di rischio o ripercorrerli – a volte persino replicarli – così da corroborare o smentire la tenuta metodologica delle procedure adoperate». In proposito di tale affermazione, a loro volta gli autori operano un richiamo a E. CASEY, "*Digital Evidence and Computer Crime*", III ed.,*Waltham,Academic Press*, 2011, p. 68 e ss.; ID., "*Error, Uncerainty and Loss in Digital Evidence*", in *International Journal of Digital Evidence*, Vol. 1, 2002, p. 3, www.utica.edu.

[7] Per un esempio grafico di documento di catena di custodia si veda R. MURENEC, op. cit., p. 129.

[8] *Ibidem*, dove in nota (269), facendo riferimento al modello di *chain of custody* dell'esperienza nordamericana, viene precisato che «*questo documento* [la catena di custodia] *deve sempre accompagnare, quasi fosse una "carta d'identità", gli elementi di prova, descrivendone in maniera precisa la res acquisita e indicando inequivocabilmente il nominativo degli individui che con essa entrano in contatto ed il momento e il luogo in cui ciò avviene*».

[9] Si veda D. CURTOTTI, ultima opera citata, p. 476, dove viene riportato un orientamento giurisprudenziale minoritario per il quale, usando le parole dell'autrice, «*risultano inutilizzabili le indagini condotte su un computer regolarmente sequestrato ma custodito in uno scatolone aperto, privo dell'apposizione di sigilli contrariamente a quanto dispone l'art. 260 c.p.p.*», la pronuncia n questione è Cass. Pen., Sez. III del 19 gennaio 2010.

[10] Per un approfondimento sulla *gabbia di Faraday* e il suo impiego nell'informatica forense si veda il sito https://www.bit4law.com/blog/informatica-forense-incident-response/gabbia-di-faraday-informatica-forense/. Per esempi relativi a dispositivi utilizzabili per l'isolamento dei supporti informatici si veda

https://www.dmi.unict.it/~battiato/CF1213/Lezione02%20-%20ISO%20e%20misurazione%20alterazioni.pdf dove vengono riportare in immagine alcune delle soluzioni adottabili.

[11] Occorre precisare che l'uso di strumenti come il *jammer*, proprio poiché volti ad azioni di disturbo delle frequenze radio e quindi ad impedire comunicazioni, è sottoposto a stringenti vincoli legislativi, si veda in proposito il dettato dell'art. 617 bis c.p. rubricato «*Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche*».

[12] Come è risaputo nel campo della sicurezza informatica non esiste il c.d. "rischio 0", sussistendo sempre, nonostante le migliori cautele, una percentuale per quanto bassa di rischio.

[13] Per un approfondimento in tale senso si veda P. DAL CHECCO, "*Hacking-Boat 2019 – Digital Forensics*", consultabile sul sito https://hackinboat.it/wp-content/uploads/2019/05/HackInBoat-Digital-Forensics-Paolo-Dal-Checco.pdf.

Articolo a cura di **Francesco Lazzini**

Profilo Autore

Laureato in giurisprudenza con successivo conseguimento dei master in Scienze Forensi (Criminologia-Investigazione-Security-Intelligence) e in Informatica giuridica, nuove tecnologie e diritto dell'informatica. Attività di studio postuniversitario focalizzata in materia di indagini con l'utilizzo del captatore informatico e digital forensics.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/la-catena-di-custodia-della-digital-evidence/