Digeat N.3 - 19 Settembre 2024

La fiducia nel processo penale: la prova digitale transfrontaliera

Di Antonio A. Martino

Abstract

Nel diritto processuale penale la fiducia nella prova digitale comprende l'autenticità, la catena di custodia, la conservazione dell'integrità dei dati e la formazione dei professionisti legali, per valutare correttamente la tecnologia coinvolta, la quale può essere più difficile da manomettere o falsificare rispetto alla prova fisica, il che la rende particolarmente importante nell'era digitale in cui viviamo. Tuttavia, la tematica pone anche delle sfide in termini di privacy e protezione dei dati; infatti, poiché l'elettronica non ha confini, è importante poter utilizzare prove ottenute in altre giurisdizioni, il che non è facile in quanto i codici procedurali sono locali. In tal senso e con questo obiettivo sono nate esperienze internazionali volte a ottenere la validità delle prove digitali in diverse giurisdizioni. È il caso della Convenzione di Budapest, con valore generale, e del progetto EXEC II dell'Unione Europea, che è in vigore e può essere preso come esempio per altre latitudini.

Indice

La modernità tecnologica è già una realtà molto presente nel perimetro della giustizia penale e, ancor prima, nelle modalità di esecuzione dei reati. L'utilizzo di strumenti tecnologici per la realizzazione di reati, prima e dopo l'accertamento di tali atti nei procedimenti penali, pone al centro di ogni analisi la **questione della prova digitale**. Quest'ultima vive costantemente nella dinamica delle trasformazioni tecnologiche e, di conseguenza, anche **l'analisi giuridica su questo tema vive continue sfide interpretative**, necessarie per adattare l'ordinamento giuridico e il sistema giuridico vigente a questi cambiamenti[1].

Mezzi di prova tradizionali e digitali a confronto

Le differenze più evidenti tra i mezzi di prova tradizionali e le prove digitali hanno a che fare con le quattro caratteristiche seguenti:

1. **Duplicabilità**: le prove generate digitalmente presentano un problema importante, ossia la distinzione dall'originalità. Come è noto, il formato digitale di un file consente di duplicarlo quante volte si vuole.

2. **Intangibilità**: questo tipo di prova non può essere apprezzata attraverso i sensi, ma richiede una serie di processi informatici nonché l'uso di determinati dispositivi elettronici per poterla osservare.
3. **Volatilità**: l'intangibilità e la possibilità di duplicare queste prove portano a un nuovo problema da considerare, la volatilità. Gli strumenti utilizzati per crearle, inviarle, conservarle e riprodurle consentono a qualsiasi utente di manipolare, modificare o alterare le prove stesse.
4. **Dilazionabilità**: le prove digitali possono essere distrutte molto facilmente, nella maggior parte dei casi senza la necessità di danneggiare i supporti che le contengono.

Il significato della prova

Il termine "provare" deriva dal latino *probare* che ha lo stesso radicale di *probus*, buono, capace; riconoscere qualcosa come buono o meno.

> Provare significa stabilire la verità di un'affermazione con ragionamenti e dimostrazioni convenienti, con testimonianze, con documenti. In termini più generali, significa indagare, sperimentare, mettere alla prova.

La prova digitale può essere definita come "prova elettronica, o su supporto elettronico, come quell'informazione contenuta in un dispositivo elettronico attraverso la quale si acquisisce la conoscenza di un fatto controverso, o per convinzione psicologica, o per stabilire tale fatto come vero in conformità a una norma giuridica".[2]

Come si è detto, **le prove elettroniche hanno una natura totalmente diversa da quelle fisiche**, soprattutto perché sono intangibili, latenti, volatili e fragili o altamente sensibili nella loro integrità e inalterabilità. Esistono **diversi tipi di prove digitali** che possono essere utilizzate nel diritto penale, tra cui:

- **E-Mail e messaggi di testo**: possono fornire prove di comunicazioni rilevanti per un caso e possono essere rintracciati per identificare mittenti e destinatari.
- **Registri delle chiamate e dati dei dispositivi mobili**: possono localizzare i sospetti in un determinato momento e luogo e rivelare modelli di comunicazione e di movimento.
- **Cronologia di navigazione e registri di attività Internet**: permettono di mostrare ricerche rilevanti, siti web visitati e attività online. Possono altresì essere utilizzati per collegare i sospetti a determinati tipi di contenuti o attività.
- **Dati dei social media**: post, commenti, immagini e video possono fornire prove e rivelare relazioni, luoghi e altri dettagli importanti.
- **Registri delle transazioni finanziarie**: consentono di tracciare i movimenti di fondi legati ad attività criminali. Possono essere utilizzati per collegare gli indagati alle transazioni sospette.
- **Metadati e registri di sistema**: possono fornire informazioni su quando, dove e come determinati file digitali sono stati creati o modificati, e sono utili per stabilire una cronologia degli eventi.

> Le prove digitali necessitano di strumenti per accedervi. Mentre un testo scritto, un disegno ovvero un dipinto possono essere visti direttamente, una prova digitale ha bisogno di un computer, di un telefono o di uno strumento in generale che permetta di vedere quelle tracce digitali (bit)[3].

Si fa perciò riferimento al documento elettronico, definito come un documento creato su un computer, registrato su un supporto informatico e riproducibile, anche noto come un insieme di campi magnetici, applicati a un supporto, secondo un determinato codice.

Certamente non va trascurata la natura internazionale del fenomeno, poiché le comunicazioni digitali non conoscono confini: Internet è una rete universale che può raggiungere qualsiasi parte del mondo da qualsiasi altra parte del pianeta. La maggior parte dei fornitori si trovano in EEUU o in Cina.

La nuova realtà probatoria

In questo contesto, ci troviamo di fronte a una **nuova realtà probatoria che pone diversi dilemmi da risolvere**: la costante evoluzione dei mezzi tecnologici, l'insufficienza delle norme, la loro incorporazione nella procedura, la mancanza di mezzi per la loro verifica e analisi e la scarsa conoscenza da parte degli attori coinvolti nell'amministrazione della giustizia.

> Un'altra sfida nella raccolta di prove digitali è l'immensità dei dati disponibili a causa della diffusione delle tecnologie anche in settori che, fino a pochi anni fa, non rientravano nell'ambito dell'analisi forense.

Oggi un solo **smartphone** può contenere migliaia di messaggi di testo, immagini, video, e-mail e altro ancora, ma memorie elettroniche e massive sono ormai presenti in tutti i **dispositivi IT, compresi quelli indossabili** (si pensi a orologi e cinture per il fitness), nonché in impianti civili e industriali come server di linee di produzione, sistemi di **allarme e sorveglianza integrati con sistemi di analisi comportamentale o di rilevazione di eventi** (incendi, allagamenti, fughe di gas, ecc.) e persino nelle **smart TV** presenti sia nei salotti di casa che nelle sale riunioni delle multinazionali. Ognuno di questi sistemi è dotato di sensori, telecamere e microfoni, che raccolgono anche i dati dei presenti, e ognuno di questi dispositivi ha un proprio sistema operativo e misure di sicurezza, spesso proprietarie, protette da segreto industriale.

Anche la quantità di dati ricavabili da un orologio digitale, con cui un cittadino svolge attività sportive e lavorative, è enorme, perché il dispositivo è spesso collegato allo smartphone e acquisisce, oltre ai dati di posizione geografica, altri parametri come lo stato di stress, l'attività fisica, gli spostamenti in auto o a piedi, l'altitudine, la pressione atmosferica, ecc. (tutti elementi che di solito non vengono utilizzati ma che, nell'ambito di un procedimento civile o penale, potrebbero essere determinanti per la decisione).

Acquisizione di prove digitali da altre giurisdizioni

> A livello transfrontaliero, la raccolta e l'ammissibilità delle prove digitali possono presentare ulteriori sfide a causa delle differenze nelle leggi e nelle procedure legali dei vari paesi coinvolti. È importante determinare quali prove digitali siano rilevanti e ammissibili secondo le leggi del paese in cui si svolge il procedimento penale.[4]

L'Interpol dispone di un gruppo specializzato sulla gestione integrata delle frontiere, per dare un'idea del tipo di crimini informatici di cui si discorre.

Il tema è così importante e attuale da aver dato origine ad un trattato internazionale: la **Convenzione di Budapest sulla criminalità informatica (2021)** e un **Secondo Protocollo Aggiuntivo alla Convenzione sulla criminalità informatica di Budapest (2022)**.

La Convenzione è considerata lo **standard internazionale più completo fino ad oggi**, poiché fornisce un quadro completo e coerente contro la criminalità informatica e le prove elettroniche. Serve come guida per qualsiasi paese che desideri sviluppare una legislazione nazionale completa sulla criminalità informatica e come quadro per la cooperazione internazionale tra gli Stati che fanno parte di questo trattato.

Essa è completata dal **Protocollo Aggiuntivo** che penalizza la criminalizzazione degli atti di natura razzista e xenofoba commessi attraverso sistemi informatici (STCE 189) e mira a fornire standard internazionali comuni per **migliorare la cooperazione in materia di criminalità informatica e la raccolta di prove in formato elettronico per indagini o procedimenti penali**.[5]

Si interviene anche in **materia di privacy e diritti dell'imputato**. Alcuni paesi hanno requisiti più severi per l'ammissibilità delle prove digitali in tribunale, come catene di custodia dettagliate. Altri paesi sono più flessibili e consentono una maggiore discrezionalità giudiziaria sull'ammissibilità.

> Stando così le cose, era necessario realizzare in Europa un apposito progetto per l'ottenimento e l'adeguata circolazione delle prove digitali in materia penale.

A livello nazionale, l'Istituto di informatica giuridica e sistemi giudiziari del Consiglio Nazionale delle Ricerche italiano ha presentato un progetto firmato da Fabio Turchi e Mariangela Biasiotti, volto a realizzare lo scambio di prove digitali sotto il nome di EXEC II.

Progetto EXEC II: scambio di prove elettroniche

Il progetto **EXEC II (Electronic Exchange of Electronic Evidence)** dell'Unione Europea facilita la cooperazione giudiziaria in materia civile e commerciale tra gli Stati membri.

> Viene attuato attraverso la Rete giudiziaria europea (RGE), che collega le autorità giudiziarie degli Stati, fornendo una piattaforma sicura per lo scambio di prove elettroniche e altri documenti giudiziari. Il progetto razionalizza e semplifica il processo di acquisizione di prove elettroniche nelle controversie transfrontaliere e riduce i costi e i tempi necessari per ottenere prove, a vantaggio delle imprese e dei cittadini.

La soluzione, nonostante tutti i problemi presentati dalla circolazione delle prove digitali tra giurisdizioni che hanno così tante normative, è **relativamente semplice e facile da applicare**. La domanda è: perché non utilizzare questo stesso progetto, già operativo in Europa, per estenderlo ad altre parti del mondo, a cominciare dall'America Latina?

Considerazioni finali

La raccolta di prove digitali nei procedimenti penali è diventata essenziale per i processi giudiziari. Tuttavia, ciò richiede una preparazione adeguata, **l'uso di strumenti forensi digitali specializzati** e il rispetto delle leggi volte a salvaguardare i diritti costituzionali delle persone.

Nell'era delle transazioni digitali (acquisti, operazioni bancarie, pagamenti elettronici) la pirateria, la falsificazione o clonazione di dati e la pubblicazione di contenuti illegali sono alcune delle attività criminali più frequenti. Atteso che **i documenti elettronici non hanno confini**, la questione dell'acquisizione di prove da altri paesi è sempre più importante, motivo per il quale è intervenuta la Convenzione di Budapest, in particolare all'articolo 32.

> Esiste già in Europa, grazie a Exec II, una Rete giudiziaria europea (RGE) che serve sia pubblici ministeri che giudici e ovviamente può essere utilizzata da chiunque purché soddisfi i requisiti stabiliti. Le organizzazioni internazionali, come l'Interpol, possono lavorare con precisione e certezza e gli inconvenienti sono più di natura politica, a causa dell'uso che alcuni stati autoritari fanno di questo tipo di prove (o per meglio dire, di tutti i tipi di prove)[6].

La Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto è stata adottata a Strasburgo nel corso della riunione ministeriale

annuale del Comitato dei Ministri del Consiglio d'Europa, che riunisce i Ministri degli Esteri dei 46 paesi Stati membri del Consiglio d'Europa.

L'accordo è il risultato di due anni di lavoro di un organismo intergovernativo, il Comitato sull'Intelligenza Artificiale (CAI), che ha riunito i 46 Stati membri del Consiglio d'Europa, dell'Unione Europea e 11 Paesi non membri (Argentina, Australia, Canada, Costa Rica, Stati Uniti, Israele, Giappone, Messico, Perù, Santa Sede e Uruguay), oltre a rappresentanti del settore privato, della società civile e del mondo accademico, che hanno partecipato in qualità di osservatori.

Siamo solo all'inizio e abbiamo potuto constatare tutti i vantaggi ma anche le insidie provocate dall'azione di un tema così complesso e delicato come l'utilizzo nazionale e internazionale delle prove digitali in materia penale. Tuttavia, sono evidenti i notevoli progressi verso una maggiore consapevolezza della sicurezza dei cittadini nel mondo digitale.

NOTE

[1] A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), Cybercrime, 2023, Torino; Tambien , C. PARODI, V. SELLAROLI, Diritto penale dell'informatica, Milano, 2019; Y por ultimo AA.VV. I reati informatici. Nuova disciplina e tecniche processuali di accertamento, 2010, Padua.

[2] SANCHÍS CRESPO CAROLINA. *Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011*. Editorial Thomson Reuters Aranzadi. 2012. Pág. 713

[3] In un caso famoso, uno degli avvocati intervenuti scrive: "abbiamo ottenuto il sommario completo dell'indagine del 41° Tribunale delle Indagini Preliminari nel caso denominato 'Begoña Gómez'. Purtroppo, è in formato grafico e non può essere analizzato dall'intelligenza artificiale senza passare prima per l'OCR, operazione complicata e noiosa". Comunicazione privata.

[4] Vedi Ver Monserrat de Hoyos , *Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo*, en la Revista de Estudios Europeos de Valladolid.

[5] "Istituto di informatica giuridica e sistemi giudiziari" è il nome attuale del vecchio Istituto di Documenta Giuridica, che ho diretto dal 1983 al 1992 e al quale si è unito Fabio Turchi mentre ne ero direttore.

[6] I giorni 10 e 11 settembre a Firenze nella sede dell'Istituto di informatica giuridica e sistemi giudiziari si è tenuto un convengo sul tema, ricco di spunti e nuove idee. Quello che risulta chiaro è l'urgenza di attuare le riforme digitali sulla prova nel processo penale. In particolare risulta chiaro che in Europa la prova transfrontaliera è un fatto grazie allo Exec II. Ma è anche palese che il digitale non ha frontiere e per farlo adoperare le stesse regole devono valere tanto in Europa (consumatrice) quanto in America Latina (produttrice) quindi dato che lo standard europeo esiste si deve far leva per farlo valere anche in America Latina. I politici e i penalisti vedono come ingerenza questa soluzione semplice, ma non abbiamo tempo, nè risorse per cercar altre soluzioni alternative. Chi avesse una migliore, per piacere la faccia pervenire, altrimenti giochiamoci questa.