Commissione

– Prassi distorte del processo –

LA PROVA (NON) DIGITALE DISTORTA

Indice

* * * * *

1. La prova digitale – L'informazione umana, storicamente ancorata a modalità comunicative di tipo tradizionale, ha risentito, negli ultimi anni, dell'influenza esercitata dal progresso tecnologico e scientifico. Se, infatti, per lungo tempo, la rappresentazione del pensiero e delle esperienze vissute è avvenuta tramite il linguaggio parlato o la scrittura, adesso, l'informatica e la telefonia sono diventate le principali piattaforme attraverso cui i consociati organizzano la maggior parte delle attività lavorative, sociali e personali ([1]).

La comunicazione, di conseguenza, è andata incontro ad un processo di dematerializzazione: suoni, video, immagini e messaggi si sono trasformati in carica elettromagnetica, in sequenze numeriche binarie ([2]), memorizzate all'interno di processori, in grado di archiviare una quantità vastissima di dati ([3]).

---

[1] In questi termini, CUOMO, *La prova digitale*, in *Prova scientifica e processo penale*, a cura di CANZIO, LUPARÌA, Milano, 2018, p. 670.

[2] Per meglio comprendere il discorso, si rinvia ad ATERNO, *Digital forensics (investigazioni informatiche)*, in *Dig. pen.*, Agg. VIII°, Torino, 2014, p. 219: «il dato informatico è costituito da una successione di 0 e di 1: paradossalmente, lo stesso dato informatico stampato su un foglio di carta è comunque una successione di 0 e di 1; questa serie di 0 e di 1 sono rappresentati dai simboli riprodotti sul supporto cartaceo utilizzando la codifica *ASCII* o altra codifica. La codifica in questione è una convezione che associa ad una precisa successione di 0 e di 1 un simbolo da riprodurre sul supporto cartaceo. La parola "ciao" corrisponde ad una definita successione di zero e di 1: 01000100101001001010111100101».

[3] Come evidenziato da Cass., Sez. Un., 20.7.2017, n. 40963, in *Guida al diritto*, 2017, 40, p. 56, «un sistema informatico, in linea generale, è costituito dalle componenti *hardware* e *software*, le prime rappresentate, secondo la comune definizione, dal complesso di elementi fisici non modificabili, (quali circuiti, unità di memoria, parti meccaniche etc.) cui si aggiungono periferiche di ingresso (ad. es. tastiera, *scanner* etc.) e di uscita (es. *monitor*, stampante) ed altri componenti comuni (*modem*, masterizzatore, cavi) e le seconde costituite, sempre secondo la comune accezione, dall'insieme di istruzioni e procedure necessarie per il funzionamento stesso della macchina (*software* di base) o per farle eseguire determinate attività (*software* applicativo) e costituiti da programmi o dati memorizzati su specifici supporti».

La documentazione analogica ha, così, lasciato spazio a quella digitale, e tale fenomeno ha comportato inevitabili ricadute anche in tema di accertamento processuale, dove – specialmente in ambito penalistico – si registra un ricorso sempre più diffuso e capillare alla c.d. "**prova digitale**" ([4]).

Dimostrazione emblematica di ciò sono due recenti sentenze emesse dal massimo organo nomofilattico ([5]), dove – tra le righe della motivazione, in maniera velata ed implicita – si è arrivati ad accreditare l'esistenza di una «"tirannia tecnica" ovvero "tecnologica"» ([6]), a tal punto radicata da obnubilare la valenza epistemica insita nei restanti mezzi di prova "a contenuto" non informatico ([7]).

Tale situazione se, per un verso, può ritenersi giustificata e giustificabile alla luce delle costanti sfide che la modernità impone ([8]), per altro verso, riaffiora problemi antichi, che si saldano a principi irrinunciabili del nostro ordinamento processuale ([9]) e che – nel caso di specie – vengono a connaturarsi per criticità del tutto inedite.

---

[4] A livello sia nazionale che sovranazionale, non esiste una definizione di "prova digitale". Tra i tentativi definitori che, in questa sede, possono essere ricordati, vi è quello, risalente al 2000, della *International Organization on Computer Evidence* ("I.O.C.E."), che associò il concetto di "prova digitale" ad una «informazione generata, memorizzata e trasmessa attraverso un supporto informatico che può avere valore in Tribunale».

[5] Cass., Sez. Un., 29.2.2024, n. 23755 e 23756, in *Cass. pen.*, 2024, 9, p. 2553.

[6] MARAFIOTI, *Sezioni Unite e tirannie tecnologiche: diritto di difesa, contraddittorio e "criptotelefonini"*, in *www.dirittodidifesa.eu*, 18 settembre 2024, p. 11.

[7] A fronte di tale situazione, la Rivista Diritto di Internet ha deciso di istituire l'"*Osservatorio di digital evidence nel procedimento penale*", con la dichiarata finalità di «mappare provvedimenti normativi, sentenze di merito o legittimità e orientamenti dottrinali in materia, così da poi analizzare criticamente le modalità di intreccio tra informatica forense, istituti probatori e garanzie del processo penale».

[8] Si riportano, a tal riguardo, le condivisibili riflessioni di LUPARÌA, *Le scienze penalistiche nella "tempesta" digitale. Quali approdi?*, in *Arch. pen.*, 2013, 3, p. 879: «il mestiere del giurista rifugge dai "giardini di pietra". Per sua natura necessita di ciclici rivolgimenti che riescano a squadernare i copioni interpretativi pigramente sedimentati dalla pratica giudiziale e dalla vulgata dei commentari. Per questa ragione, l'emergere di fattori che scuotono categorie e orientamenti ermeneutici deve essere sempre salutato come una benefica ventata di freschezza, capace di spingere l'interprete verso inediti itinerari speculativi o verso una nuova consapevolezza degli approdi teorici già raggiunti nel passato».

[9] Il riferimento è al complicato rapporto tra "scienza" e "processo". Si pensi, a titolo esemplificativo, alle difficoltà che un Giudice potrebbe incontrare nel valutare una prova, quale quella digitale, generata all'esito di procedure connotate da un elevatissimo coefficiente tecnico. L'eventuale impossibilità di fornire un solido discorso giustificativo a supporto di una determinata decisione darebbe adito a problematiche, prima ancora che giuridiche, di carattere etico e politico, posto che un'acritica adesione ad un dato indecifrabile porterebbe la funzione giurisdizionale «ad assumere contorni irrazionalistici e superstiziosi: il giudice sfugge alle sue responsabilità per affidarsi nuovamente a qualcosa che, appunto, gli "sta sopra": ieri la divinità, oggi la scienza» (cfr. CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, 9, p. 3524).

Non deve, infatti, sfuggire come l'immaterialità e l'intangibilità del dato digitale rendano, altresì, lo stesso **fragile** ([10]), **volatile** ([11]) e, ciò che più conta, **facilmente manipolabile** ([12]).

Basti, a tal proposito, considerare che ogni comando impartito, più o meno volontariamente, ad un'apparecchiatura elettronica può rivelarsi foriero di modifiche, anche irreversibili, del documento informatico.

Di qui, l'esigenza di preservare la conoscenza processuale da una indiscriminata acquisizione di **elementi spuri** che, in quanto tali, potrebbero condizionare negativamente l'accertamento giurisdizionale. Qualunque attività estrapolativa di dati contenuti in "sistemi informatici" ([13]) deve necessariamente avvenire in ossequio a specifiche procedure, riconducibili al settore disciplinare della ***digital forensic***, che – supportate da alto rigore metodologico ed adeguata strumentazione tecnica – assicurino la **conformità** e la **genuinità** del *file* acquisito rispetto all'originale ([14]).

In tale direzione, del resto, sembra essersi orientato, oramai da molto tempo, non solo il legislatore comunitario, ma anche quello nazionale.

Come noto, con la Convenzione del Consiglio d'Europa sulla Criminalità Informatica, sottoscritta a Budapest il 23 novembre 2001, sono state dettate una serie di disposizioni a contenuto precettivo per gli Stati membri, preordinate a regolamentare le modalità di acquisizione e conservazione dei dati digitali nell'ambito dei procedimenti penali ([15]). Per quanto qui di specifico interesse, è stato stabilito che sia la perquisizione del supporto

[10] Il danneggiamento di un *hard-disk* o la smagnetizzazione di un CD-rom renderebbero inaccessibili i dati ivi contenuti.

[11] Alcuni tipi di memoria digitale, come la R.A.M. (*Random Access Memory*), laddove il dispositivo venga inavvertitamente spento, non consentono un salvataggio automatico dei dati.

[12] Sul punto, si tornerà *funditus* nel prosieguo del presente lavoro, ma per il momento sia sufficiente dar conto dell'esistenza di una moltitudine di programmi di *editing* in grado di modificare immagini, audio e video in maniera oltremodo realistica.

[13] Locuzione che, ad avviso di Cass., Sez. VI, 4.10.1999, n. 3067, in *Cass. pen.*, 2000, p. 2990, esprimerebbe «il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche». Più calzante appare la definizione fornita dall'art. 1, lett. a), della Convenzione del Consiglio d'Europa sulla Criminalità Informatica, sottoscritta a Budapest il 23 novembre 2001, secondo cui, per "sistema informatico", deve intendersi «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati».

[14] L'Interpol, in un documento programmatico pubblicato sul proprio sito istituzionale, ha precisato come la *digital forensic* sia quella «branca della scienza forense che si concentra sull'identificazione, l'acquisizione, l'elaborazione, l'analisi e lo studio di dati archiviati elettronicamente».

[15] Da segnalare come l'art. 1, lett. b), della "Convenzione di Budapest" fornisca la seguente definizione di "dati informatici": «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione».

informatico che l'eventuale sequestro dei dati in esso memorizzati devono uniformarsi ad appositi **protocolli forensi**, atti a conferire all'intera procedura una **patente di affidabilità, integrità e trasparenza**, indispensabile affinché il materiale oggetto di duplicazione possa assurgere, nel processo di cognizione, a rango di prova ([16]).

Anche lo Stato italiano, con Legge n. 48 del 2008 (*"Ratifica ed esecuzione della Convenzione di Budapest"*), ha cercato di armonizzare, nei limiti del possibile ([17]), l'impianto codicistico alle indicazioni promananti dal Consiglio d'Europa, ispirandosi ad una tecnica legislativa speculare a quella delle "norme penali in bianco": le disposizioni procedurali, così come interpolate, fissano gli obiettivi, rinviando – quanto ai relativi metodi – agli strumenti di *soft law* che, per la loro flessibilità, risultano maggiormente inclini ad adattarsi al progresso tecnologico ([18]).

E così, in materia di ispezione ([19]) e perquisizione ([20]), è stato sancito, in capo all'Autorità Giudiziaria ed alla Polizia Giudiziaria ([21]), il dovere di

---

[16] Cfr. artt. 16, 17, 19, 20, 21, 30, 31, 33 e 34 della "Convenzione di Budapest". Giova, altresì, ricordare come, nel 2013, a valle di un progetto interamente finanziato dal Consiglio d'Europa e dall'Unione Europea, sia stata pubblicata l'*Electronic Evidence Guide* ("E.E.G."), ovverosia una guida destinata ad offrire all'Autorità Giudiziaria alcune preziose regole di comportamento in tema di gestione dei dati digitali. Tale guida – per come aggiornata nel 2022 – fissa i criteri di ammissibilità della prova digitale, stabilendo che: (i) devono essere riportati tutti i passaggi attraverso cui il dato digitale è stato acquisito (*criterio dell'autenticità*); (ii) deve procedersi ad un'analisi integrale, e non parcellizzata, del contenuto del supporto informatico (*criterio della completezza*); (iii) non devono emergere anomalie in ordine alle fasi di raccolta e trattamento dei dati (*criterio dell'affidabilità*); (iv) il risultato probatorio derivante dalle operazioni di acquisizione deve essere facilmente fruibile e comprensibile dal Giudice (*criterio della credibilità*).

[17] Va precisato come la novella legislativa si sia limitata ad emendare vecchi istituti processuali, senza creare nuovi strumenti in grado di rispondere, forse in maniera più efficace, alle sfide imposte dalla prova digitale. In chiave critica, LUPARÌA, *I profili processuali*, in *Dir. pen. proc.*, 2008, 6, p. 717, il quale auspicava in «un'autonomia sistematica delle operazioni di *computer forensics*, ritenute in virtù della loro peculiarità un settore disancorato dal resto del *corpus* normativo, una specie di *insula* nel costrutto processuale».

[18] CONTI, *La prova informatica e il mancato rispetto delle best practices: lineamenti sistematici sulle conseguenze processuali*, in *Cybercrime*, a cura di CADOPPI, CANESTRARI, MANNA, PAPA, Milano, 2019, p. 1329 e ss.

[19] Art. 244, co. 2, c.p.p.: «se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

[20] Art. 247, co. 1-*bis*, c.p.p.: «quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

[21] Art. 352, co. 1-*bis*, c.p.p.: «nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi».

conservare i dati informatici originali, **impedendone ogni possibile alterazione**. Del pari, in tema di accertamenti urgenti ([22]) e di sequestro ([23]), è stata riconosciuta la possibilità di un'apprensione diretta del contenuto di un dispositivo elettronico, a condizione che detto contenuto sia duplicato su adeguati supporti e ne venga garantita la **conformità all'originale** e **l'immodificabilità**.

Da una piana lettura di tali disposizioni emerge, chiara ed evidente, la necessità di un approccio che, in tutte le fasi rilevanti del procedimento (*id est* analisi del *device*, acquisizione dei relativi contenuti e successiva conservazione), si preoccupi di tracciare e documentare le operazioni compiute, così da poter escludere ipotesi di **indebite alterazioni** dei dati acquisiti; un approccio, detto in altri termini, funzionale ad assicurare l'integrità e la genuinità della prova, in vista del suo futuro utilizzo processuale, rispettando quella che, nel gergo anglosassone, sovente viene definita come *chain of custody*.

2. Le operazioni forensi – Sebbene non vi sia una metodologia elettiva attraverso cui clonare i contenuti di un supporto informatico, esistono alcune procedure che, corroborate dai dati forniti dall'esperienza ([24]) e sottoposte ai necessari tentativi di falsificazione ([25]), costituiscono oramai patrimonio consolidato presso la comunità scientifica di riferimento.

---

[22] Art. 354, co. 2, c.p.p.: «se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti».

[23] Art. 254-*bis* c.p.p.: «l'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

[24] Come noto, secondo la concezione positivista, esiste un unico metodo scientifico, l'induzione, utilizzabile in tutte le sfere della conoscenza ed in ogni ambito della vita umana; tale metodo poggia sul c.d. "principio di verificazione" (o verificabilità), in base al quale una proposizione può essere considerata scientifica se, e solo se, la sua verificazione risulti riscontrata dall'esperienza e dal suo costante ripetersi. Con poche, ma significative parole, POPPER, *Logica della scoperta scientifica. Il carattere autocorrettivo della scienza*, trad. it. di TRINCHERO, Torino, 1970, p. 5 e s., coglie l'essenza – ed i limiti – della teoria verificazionista: «per quanto numerosi siano i casi di cigni bianchi che possiamo aver osservato, ciò non giustifica l'asserzione che tutti i cigni sono bianchi».

[25] In contrapposizione al c.d. "empirismo logico", POPPER, *Scienza e filosofia*, trad. it. di

Come noto, la definizione delle *best practices* è affidata, a livello mondiale, all'*International Organization for Standardization* ("I.S.O.") e, con specifico riferimento al settore dell'elettricità, dell'elettronica e delle tecnologie correlate, all'*International Electrotechnical Commission* ("I.E.C.").

Lo *standard* internazionale di maggior rilievo in ambito di *digital forensic* è sicuramente l'**I.S.O./I.E.C. 27037:2012** (*"Guidelines for identification, collection, acquisition, and preservation of digital evidence"*) ([26]), ove sono indicate una serie di prescrizioni tecniche volte a guidare gli operatori nella fase di identificazione, raccolta, acquisizione e preservazione del dato digitale ([27]).

Questi, in estrema sintesi, i diversi stadi che compongono il procedimento ([28]):

- **Identificazione**

- individuazione del *device* che può contenere dati processualmente rilevanti, considerando anche dispositivi di difficile identificazione "geografica" (*Cloud computing*) o di piccole dimensioni (*miniSD*);
- nel caso in cui il *device* abbia un'interfaccia in rete, individuazione dei sistemi con cui può aver interagito;

TRINCHERO, Torino, 1969, p. 146, elaborò le tre linee direttrici del metodo falsificazionista: «tutta la mia concezione del metodo scientifico si può riassumere dicendo che esso consiste in questi tre passi: inciampiamo in qualche problema, tentiamo di risolverlo, ad esempio, con qualche nuova teoria; impariamo dai nostri sbagli, specialmente da quelli che ci sono resi presente dalla discussione critica dei nostri tentativi di soluzione. Ovvero, per dirla in altre parole: "problemi-teorie-critiche"». La ripartizione del metodo scientifico nei tre snodi del problema, della teoria e della critica è ripresa anche da HEMPEL, *Filosofia delle scienze naturali*, trad. it. di BERRA, Bologna, 1978, p. 36, il quale ritiene che la conoscenza scientifica si "conquista" «mediante quello che viene spesso chiamato il "metodo dell'ipotesi", cioè, con l'inventare delle ipotesi come tentativi di risposta al problema in esame e quindi col sottoporle al controllo empirico […]. Un'ipotesi accettabile dovrà adattarsi a tutti i dati rilevanti disponibili […]. Anche numerosi controlli che forniscano dei risultati completamente favorevoli non confermano un'ipotesi in modo definitivo, ma le assicurano soltanto un sostegno più o meno forte».

[26] Altrettanto importante è l'I.S.O./I.E.C. 27042:2015 (*"Guidelines for the analysis and interpretation of digital evidence"*), costituente una guida in tema di analisi ed interpretazione delle prove digitali, con particolare riguardo alle questioni relative alla continuità, alla validità, alla riproducibilità ed alla ripetibilità dell'operazione forense.

[27] L'I.S.O./I.E.C. 27037:2012 individua tre categorie di soggetti responsabili della gestione delle evidenze digitali: (i) il *Digital Evidence First Responder* ("D.E.F.R."), che è un soggetto autorizzato, formato e qualificato ad agire, per primo, sulla *scena criminis*, al fine di eseguire l'attività di raccolta ed acquisizione delle prove; (ii) il *Digital Evidence Specialist* ("D.E.S."), che è un soggetto che, oltre ad avere le stesse capacità e competenze del D.E.F.R., possiede anche conoscenze specialistiche che gli consentono di gestire problematiche di natura tecnica, quali – a titolo esemplificativo – l'acquisizione di una memoria R.A.M.; (iii) l'*Incident Response Specialist* ("I.R.S."), che è una figura professionale che opera normalmente all'interno di un'azienda e che si occupa del primo intervento *post* incidente informatico.

[28] Le informazioni di seguito riportate sono compendiate da CALABRÒ, *Corso di Tecnologie per la sicurezza informatica. Digital Forensics*, in *www.vincenzocalabro.it*.

- cernita dei diversi dispositivi di memorizzazione (*hard disk*, *floppy disk*, memorie *flash*, *memory card*, CD-rom, Dvd);
- documentazione della marca, del modello, del numero seriale, del supporto e del sistema operativo ([29]);
- documentazione dello stato (acceso o spento) in cui si trova il *device*;
- utilizzazione di un rilevatore *wireless* per verificare la presenza di ulteriori dispositivi nascosti.

▪ **Raccolta**

- rimozione del cavo di alimentazione;
- disconnessione di tutti i restanti cavi connessi al dispositivo;
- etichettatura delle porte di ingresso;
- protezione del tasto di accensione;
- messa in sicurezza di eventuali alloggiamenti;
- nel caso in cui il dispositivo sia accesso, immediata acquisizione dei dati volatili, così da avere a disposizione eventuali chiavi di cifratura residenti in memoria.

▪ **Acquisizione** ([30])

- rimozione del supporto di memoria dal dispositivo spento, previa sua etichettatura;
- esecuzione della copia forense, utilizzando un *tool* validato;
- calcolo dell'*hash* e del relativo valore;
- nel caso in cui la copia sia effettuata con sistema acceso, acquisizione dei dati volatili (da riversare all'interno di un contenitore logico) e, successivamente, dei dati non volatili (da riversare all'interno di un dispositivo formattato);
- utilizzazione di una sorgente affidabile per documentare data ed orario delle operazioni compiute;
- laddove il sistema risulti "critico" (come, ad esempio, potrebbero essere i *data center* o i sistemi di sorveglianza), procedere con l'acquisizione *live* (previa copiatura integrale della memoria R.A.M. e di massa) oppure ad un'acquisizione parziale (selezionando le porzioni di memoria di possibile interesse);

[29] Nel caso in cui i supporti risultino danneggiati, è altresì necessario documentarne lo stato.
[30] Tale operazione può essere svolta *on-site* ovvero in laboratorio.

- al termine della fase di acquisizione, proteggere i dati copiati attraverso l'apposizione di un sigillo digitale, costituito da un'impronta *hash* e la firma digitale dell'operatore.

- **Conservazione**
- etichettare ed imballare il *device* e la copia forense;
- bloccare le parti mobili;
- ridurre i rischi derivanti dal trasporto;
- preservare i supporti da ogni tipo di incidente e/o contaminazione ([31]);
- documentare tutti i movimenti e le interazioni con la potenziale prova digitale.

A fronte di un *iter* – quello appena descritto – interamente orientato a garantire la genuinità del dato digitale, mediante la cristallizzazione di plurime regole di condotta che si pongono, l'una con l'altra, in un rapporto di stretta interdipendenza, non può ignorarsi come il **momento acquisitivo** sia quello permeato da profili di maggiore delicatezza. Ed infatti, una copia del *device* eseguita con una metodica non corretta depriverebbe l'accertamen-to della necessaria attendibilità, rischiando, per l'effetto, di pregiudicare l'utilizzo processuale della *digital evidence*.

È per questo motivo che l'I.S.O./I.E.C. 27037:2012 stabilisce che il contenuto del supporto deve essere copiato attraverso la ***Bit Stream Image***, ovverosia una tecnica che, realizzando un'immagine *bit a bit* di tutte le zone del disco fisso o di altro dispositivo di memorizzazione ([32]), ivi comprese quelle non direttamente visibili all'operatore (ci si riferisce, in particolare, alle zone "non allocate" e/o agli *slack spaces*), produce una duplicato perfettamente sovrapponibile all'originale ([33]).

---

[31] Il riferimento è non solo alle cadute accidentali, ma anche agli agenti fisici dannosi, come la luce, l'umidità, le forze meccaniche, i campi elettromagnetici e le temperature eccessive.

[32] Si consideri che la *Bit Stream Image* permette di preservare anche l'allocazione fisica dei singoli *files*, oltreché la loro posizione logica.

[33] DE FLAMMINEIS, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in *Sistema Penale*, 8 marzo 2024, p. 4: «per l'incorporazione statica la modalità che garantisce il rispetto delle cautele sopra indicate è quella della creazione della c.d. *bit-stream image*, ovvero della realizzazione dell'immagine *bit* a *bit* del contenuto del supporto da acquisire; viene quindi formata una copia *bit* a *bit*, cioè viene clonato il supporto originario del documento, specie l'*hard disk*, creando un supporto identico al primo che con il sistema di sigillo digitale (c.d. *hash*) garantisce l'identità assoluta con l'originale. Benché si parli di copia, in realtà il nuovo supporto potrebbe definirsi un secondo originale, proprio perché non è il supporto che identifica il documento informatico, stante la facile trasferibilità, ma il suo contenuto».

Tale operazione, tuttavia, postula l'utilizzo di particolari *software* ed apparecchiature (nel cui novero, si iscrivono anche i c.d. *write-blockers*), in grado di registrare automaticamente le attività compiute ed impedire ogni alterazione del sistema originario:

Strumentazioni, queste, che – una volta terminata la fase di copiatura – assegnano alla c.d. "copia-forense" un sigillo digitale, costituito da un'impronta alfanumerica a chiave simmetrica denominata *hash*, che contraddistingue univocamente la copia ottenuta e ne certifica, in maniera indelebile, la conformità ([34]).

[34] A corollario di ciò, si vuole riportare un passaggio tratto da COSTABILE, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e diritto*, 2010, 3, p. 499 e s., in cui – con dovizia di particolari – viene analizzata la tecnica della *Bit Stream Image*: «la copia forense è una copia 1:1 del supporto di memoria in un dispositivo di memorizzazione equivalente. La copia deve essere, a livello logico, perfettamente identica al dispositivo originale. Dovranno essere preservati quindi non solo i dati, ma anche lo spazio libero sul disco, i metadati, il *master boot record*, ecc. Per fare questo si può ricorrere alla tecnica del "*bit stream image*", che consentirà di replicare su un altro supporto di memoria un'immagine equivalente all'originale in termini di contenuto informativo, fino al livello del *bit*. Verranno preservati, quindi, anche eventuali parti apparentemente vuote, ma che potrebbero contenere *file* (o frammenti di *file*) cancellati e non visibili con i normali strumenti del sistema operativo. Esistono differenti strumenti in grado di eseguire il "*bit stream image*", sia via *software* che via *hardware*. L'operazione di copia non deve in alcun modo modificare l'integrità dei dati contenuti nel supporto di memoria: per tale motivo è opportuno ricorrere all'ausilio di un *Write Blocker*, che impedirà la modifica dei dati sul supporto di memoria contenente la fonte di prova. In altri termini, un blocco in scrittura rende il supporto accessibile in sola lettura, permettendo l'interfacciamento alla postazione forense che ne eseguirà la *bit stream image*. Affinché la duplicazione della fonte di prova abbia maggiore valore, è richiesto che a seguito della duplicazione del dato sia eseguita una verifica d'integrità atta a dimostrare che l'originale sia identico alla sua copia. Per fare questo si ricorre a una funzione matematica detta "*hash*". L'*hash* è una funzione non reversibile, atta a trasformare un dato di dimensione arbitraria in una stringa di lunghezza fissa. L'*hash* di un dato rappresenta una sorta di "impronta digitale" del dato. Le funzioni di *hash* svolgono un ruolo essenziale per verificare l'integrità del dato, poiché l'esecuzione dell'algoritmo su un dato anche minimamente modificato fornisce un "*message digest*" (o "impronta del messaggio") completamente differente rispetto a quello calcolato sul dato originale permettendo di identificare anche le più piccole differenze (anche una virgola su un intero *hard disk*). La funzione di *hash* realizzata attraverso algoritmi pubblici e noti è strumento sufficiente per garantire che la copia e l'originale presentino le medesime caratteristiche. La lunghezza dei valori di *hash* varia secondo gli algoritmi utilizzati. Il valore più comunemente adottato è di 128 *bit* (c.d. MD5), in ambito forense è consigliato l'utilizzo di algoritmi in grado di generare *hash* di lunghezza maggiore come SHA, in grado di fornire *hash* a 224, 256, 384 e 512 *bit* (più resistenti). Il dispositivo di memoria contenente la fonte di prova (solitamente un *hard disk*, o una memoria USB) dovrà essere estratto dal sistema, interfacciato con *Write Blocker* e collegato ad una postazione forense in grado di eseguire la copia attraverso il *bit stream image*. Tale operazione può essere svolta anche attraverso l'utilizzo di sistemi *hardware* concepiti per attività forensi (ad esempio *Talon*, *Shadow*, ecc). Nel caso in cui il supporto di memoria contenente il dato sia in sola lettura, come un CD / DVD rom, sarà possibile eseguire una copia del

Solo in questo modo il dato informatico potrà acquisire dignità probatoria ed essere posto dal giudice a fondamento della propria decisione.

Non vi è, perciò, da stupirsi se le richiamate procedure, pur promanando da organizzazioni non governative e non avendo forza vincolante, risultano oramai largamente recepite e mutuate, a livello sia europeo che internazionale, da tutti i principali organismi investigativi ([35]).

Ad esempio, in Italia, la Guardia di Finanza – con Circolare n. 1 del 2018 – ha rimarcato che l'identificazione, la raccolta, l'acquisizione e la conservazione dei dati digitali deve avvenire in ossequio ai canoni enucleati dall'I.S.O./I.E.C. 27037:2012 ([36]).

Interessante notare come, all'interno di tale documento, la fase di acquisizione sia pedissequamente modellata alla stregua di quanto previsto nei citati *standards* internazionali, tramite riferimenti espliciti alla *Bit Stream Image* ed alla c.d. *hash function*: «è necessario, in tale fase, tenere in considerazione i principi fondamentali dell'integrità dei dati che devono essere acquisiti, con ciò significando che, secondo gli *standard* e le linee guida riconosciute a livello internazionale, nessuna delle attività svolte nella fase di acquisizione dovrebbe andare a modificare i dati, i dispositivi o i supporti elettronici che possono essere successivamente oggetto di acquisizione ed analisi nell'ambito dell'attività ispettiva. Il personale operante deve pertanto adottare ogni utile precauzione a salvaguardia dell'integrità dei dati che vengono acquisiti; in altri termini, **il duplicato di un documento informatico o la copia forense di un supporto di memoria deve essere prodotto mediante processi e strumenti che assicurino che l'evidenza informatica ottenuta sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di *bit* di quella originale**. Le buone prassi a livello internazionale impongono, soprattutto nel caso della duplicazione di unità di memoria, l'utilizzo di specifici dispositivi (*writeblocker*, duplicatori) e/o applicativi (*software* di acquisizione forense), capaci di garantire l'integrità dell'evidenza acquisita. In ogni caso, e quale regola generale […] è opportuno, ove

dispositivo senza porre le specifiche attenzioni legate alla citata protezione dalla modifica accidentale del dato (e quindi senza la necessità di un *Write Blocker*)».

[35] Ad esempio, la Germania, per le indagini informatiche, utilizza le *Bundesamt für Sicherheit in der Informationstechnik "Leitfaden, IT-Forensik"*, ovverosia delle linee-guida che, in buona parte, replicano le prescrizioni contenute nei citati *standards* internazionali.

[36] *Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali*, reperibile su *www.apindustria.vi.it*, 2018, vol. II, p. 28.

tecnicamente possibile in relazione alle competenze degli operanti, calcolare un'impronta logico-matematica detta *hash*. La determinazione dell'impronta (*rectius* valore di *hash* e funzione di verifica) del documento informatico attraverso gli algoritmi di *hash* consente, infatti, unitamente alla documentazione delle attività svolte, di ricostruire le azioni svolte sui documenti informatici di interesse» ([37]).

Analoghe indicazioni possono rinvenirsi non solo in alcune guide operative diramate dall'Arma dei Carabinieri ([38]) e dalla Polizia di Stato ([39]), ma anche in quella pronuncia delle Sezioni Unite della Corte di Cassazione con cui è stato ricordato che «le cosiddette copie-immagine (la cui integrità ed identità all'originale è assicurata dalla funzione crittografica di *hash* alla stregua di un'impronta)» consentono una riproduzione del «dato duplicato nelle stesse condizioni in cui si trova al momento della sua acquisizione», riportando, al loro interno, tutti i *metadati* di riferimento, quali «la data di creazione, quella di apertura, di esecuzione o dell'ultima modifica, la proprietà, i permessi, eventuali codici di controllo, la posizione all'interno di una determinata cartella o gruppo di cartelle» ([40]).

---

[37] *Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali*, cit., p. 30 e s. Del pari, la Guardia di Finanza, anche con riferimento alla conservazione della copia-clone, ha ribadito l'esigenza che venga creato un apposito documento (la c.d. "catena di custodia"), nel quale siano riportati: «i nominativi dei militari operanti, la sede del contribuente e la data; i nominativi dell'eventuale personale tecnico messo a disposizione dal contribuente; l'elenco delle evidenze digitali acquisite; la tipologia delle evidenze digitali acquisite; l'impronta *hash* di ciascuna evidenza e la funzione di calcolo utilizzata; gli eventuali passaggi di consegna dell'evidenza digitale (militare cedente, militare accettante); il luogo ove vengono custoditi i sistemi e/o i supporti informatici ovvero i dati digitali acquisiti nel corso dell'attività ispettiva».

[38] MATTIUCCI, DELFINIS, *Forensic computing*, in *www.carabinieri.it*, dove si arriva, addirittura, ad una tripartizione delle tecniche di acquisizione del dato digitale, a seconda degli scopi perseguiti e della situazione concreta in cui l'operatore si trova costretto a lavorare: «a. copia di livello fisico: o *bitstream copy*, in cui il contenuto dell'unità fisica viene letto sequenzialmente caricando la minima quantità di memoria di volta in volta indirizzabile per poi registrarla nella stessa sequenza su di un comune *file* binario (immagine fisica dell'unità); b. copia di basso livello del *file system*: o *cluster-copy*, in cui il contenuto di una partizione logica (strutturatasi a seguito di una formattazione correlata ad un preciso *file system*) viene letto sequenzialmente caricando la minima quantità di memoria che il *file system* consente di indirizzare di volta in volta per poi registrarla nella stessa sequenza su di un comune *file* binario (immagine di basso livello del *file system*); c. copia del *file system*: in cui parte o tutto il contenuto di alto livello di una partizione logica (strutturatasi a seguito di una formattazione correlata ad un preciso *file system*), ivi intendendo i contenuti di *file* e *directory* evidenti (non cancellati), viene sottoposto a *backup* su di un *file* (*file* di *backup*)».

[39] MORABITO, *Indagini hi-tech*, in *www.poliziamoderna.poliziadistato.it*, 9 gennaio 2024, p. 25, dove il Responsabile della Sezione "*Digital Forensic*" della Polizia di Stato ha tenuto a precisare quanto segue: «noi lavoriamo su delega dell'autorità giudiziaria […] quando con la commissione di un reato sul posto vengono effettuati sequestri di dispositivi cellulari oppure memorie di massa. In tali circostanze, l'AG delega a questa sezione il compito di effettuare la "copia forense" dei dispositivi, sulla quale poi l'ufficio investigativo compirà le proprie analisi, che viene realizzata tramite *software* che consentono di non alterare le informazioni contenute nel reperto, quindi senza modificarlo, ottenendo una copia "*bit a bit*", o il più fedele possibile, che poi viene messa a disposizione dell'ufficio investigativo e dell'autorità giudiziaria».

[40] Cass., Sez. Un., 20.7.2017, n. 40963, cit., p. 60, ove si prosegue affermando: «una simile distinzione è presente nel D. Lgs. n. 82 del 2005 (Codice dell'amministrazione digitale) laddove, nell'art. 1, oltre

Insomma, il sistema normativo e para-normativo appare piuttosto chiaro.

3. La "prassi distorta" – Se si conviene sul fatto che le *best practices* assolvono ad una funzione servente e strumentale all'accertamento processuale, evitando che il vaglio giurisdizionale venga inficiato da elementi intrinsecamente inattendibili o, peggio ancora, dolosamente manipolati, allora, non ci vuole molto a comprendere fino a che punto debba ritenersi esteso il loro raggio d'azione.

Non avrebbe, infatti, alcun senso logico, ancor prima che giuridico, impegnare l'Autorità Giudiziaria nell'espletamento di articolate procedure atte a garantire la genuinità della prova, se – sul fronte opposto – le parti private potessero liberamente derogarvi, introducendo, nell'agone giudiziario, una qualsiasi evidenza informatica, ancorché non validata sul piano metodologico e scientifico.

A ben vedere, le regole in tema di raccolta, acquisizione e conservazione dei dati digitali delineano e sedimentano un **quadro valoriale comune**, alla cui scrupolosa osservanza sono tenuti, in egual misura, tutti i soggetti che, direttamente o indirettamente, prendono parte al processo.

Eppure, nonostante l'ovvietà di una simile conclusione, la realtà che si registra all'interno del Circondario di Roma appare ben diversa.

Riunendo e mettendo a sistema le diverse esperienze professionali dei suoi Componenti e degli altri Soci, la Commissione in intestazione è venuta a conoscenza di una consistente mole di *res iudicande*, in cui le prove digitali a carico dell'indagato e/o dell'imputato sono state fornite direttamente dalla persona offesa, dopo averle acquisite in

---

a distinguere, al comma 1, il "documento informatico" dal "documento analogico" (rispettivamente, nel comma 1, lett. p e p-*bis*) a seconda che la rappresentazione di atti, fatti o dati giuridicamente rilevanti sia o meno inserita in un documento elettronico che ne contiene la rappresentazione informatica, definisce, nella lett. i-*quater*, la "copia informatica" di documento informatico (*"il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari"*) e la distingue dal "duplicato informatico" di cui alla lett. i-*quinquies* (*"il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario"*), operando, peraltro, una analoga distinzione tra "copia informatica di documento analogico" e "copia per immagine su supporto informatico di documento analogico", laddove la prima è *"il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto"* e la seconda *"il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto"*».

violazione – o, meglio, in totale pretermissione – delle procedure poc'anzi descritte.

Tale casistica, pur nella eterogeneità delle fattispecie analizzate, può essere ricondotta a due diversi filoni.

Il primo è rappresentato da **dati – in origine – digitali**, in quanto creati avvalendosi di sistemi informatici e/o telefonici, **ma depositati nel procedimento o nel processo soltanto tramite riproduzione analogica**.

A titolo esemplificativo, possono qui richiamarsi:

- gli ***screenshot*** di conversazioni *whatsapp* (o di altre conversazioni intervenute utilizzando i restanti servizi di messaggistica disponibili sul telefono cellulare);
- le **stampe** di comunicazioni *e-mail*;
- le **fotografie** di *post* pubblicati sui *social network* e dei commenti lasciati in calce ai medesimi dai singoli utenti.

Il secondo filone, invece, riguarda dati che, pur conservando il crisma della "digitalità", sono stati confezionati con modalità tali da renderli **impermeabili** – al pari delle riproduzioni analogiche – **a qualsiasi forma di controllo** da parte della difesa (e, a dir il vero, anche dello stesso Giudice).

Ci si riferisce, in particolare, ai ***files*** **audio e video** riversati su supporti di memoria esterni (CD-rom, chiavette U.S.B., *hard-disk*), mediante una **mera operazione informatica di "copia e incolla"**.

In quasi tutti i casi analizzati, lo strumento attraverso il quale tale materiale è confluito in giudizio è rappresentato dalla **denuncia** o dalla **querela**.

Tuttavia, in nessuno di questi casi, il querelante o il denunciante ha mai:

- messo a disposizione dell'Autorità Giudiziaria il proprio telefono cellulare o il proprio *computer* (ove – a suo dire – sarebbero custoditi i *files* originali);
- incaricato un consulente tecnico affinché copiasse il contenuto di tali dispositivi elettronici, eventualmente nella sola porzione di interesse, attraverso operazioni forensi;

- depositato il dato digitale originale (ad esempio, i *files* di *log* di una conversazione *whatsapp*) ([41]);
- redatto un verbale illustrativo della metodologia seguita nella fase di acquisizione e conservazione dei dati.

Dal canto suo, l'Autorità Giudiziaria – almeno nella casistica presa in esame dalla Commissione – non ha mai sottoposto a sequestro il supporto informatico della persona offesa, al fine di accertare la rispondenza all'originale di quanto da quest'ultima prodotto. E ciò anche quando la difesa dell'accusato aveva effettuato rilievi in ordine alla genuinità delle allegazioni di controparte, paventando il rischio di un'adulterazione delle stesse.

Provviste probatorie, dunque, estremamente instabili, anche e soprattutto perché carenti di qualsivoglia conferma sulla loro affidabilità ([42]), **ma ritenute – nei casi oggetto di studio – sufficienti a legittimare l'esercizio dell'azione penale o, addirittura, l'emissione di sentenze di condanna**.

Il tutto in vicende giudiziarie delicatissime, dove la contestazione elevata nei confronti dell'imputato verte su reati sanzionati con pene edittali particolarmente afflittive e, in buona parte, ostativi a forme di detenzione alternative al carcere.

Al contempo, **prive di sostanziale pregio sono le argomentazioni poste a fondamento delle relative ordinanze acquisitive**, nelle quali campeggia un rinvio recettizio a quei principi giurisprudenziali enucleati dalla Corte di Cassazione, secondo cui le disposizioni di cui alla L. n. 48 del 2008, anche a volerle ritenere (per mera ipotesi di lavoro) applicabili alle parti private, acquisirebbero natura semplicemente «programmatica e di stimolo», senza connaturarsi di specifiche ed inderogabili indicazioni in ordine alle «tecniche di accesso al sistema e di estrapolazione dei dati in esso contenuti» ([43]). L'opzione legislativa, in altre parole, non contemplerebbe alcun tipo di sanzione ([44]): nessun divieto espresso da cui ricavare l'inutilizzabilità della prova

[41] Nei *files* di *log*, sono memorizzate tutte le operazioni informatiche compiute da un determinato utente. Cosa diversa sono, invece, gli indirizzi I.P., ovverosia il numero seriale che identifica ciascun dispositivo elettronico collegato ad una rete telematica.

[42] DE FLAMMINEIS, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, cit., p. 2 e s.: «diversamente, la produzione degli *screenshot* delle *chat* o di *files* (video, foto) non sostituisce la prova digitale; dunque, le informazioni complete di quel dato (riconducibilità soggettiva, data, ora, etc.) non offerte dalla mera riproduzione fotografica dell'immagine del dato stesso, si possono ottenere solo acquisendo in originale il *file* o comunque il contenuto informatico».

[43] Cass., Sez. II, 21.10.2020, n. 35447, in *Cass. pen.*, 2021, 7-8, p. 2495.

[44] Cass., Sez. V, 16.11.2015, n. 11905, in *CED Cass. pen.*, 2016, rv 266477.

eventualmente mal formata, né tantomeno regole di esclusione che potrebbero determinarne l'inammissibilità ([45]). Piuttosto, la *quaestio iuris* afferirebbe alla sola **attendibilità del dato informatico** riprodotto in giudizio e, pertanto, andrebbe rimessa alla **valutazione in concreto del Giudice**, il quale – al momento della decisione – sarà chiamato ad un attento scrutinio sulla corrispondenza del dato acquisito rispetto all'originale e sull'assenza di ogni sua possibile falsificazione ([46]).

Che, tuttavia, tali prese di posizione non possano trovare alcuna forma di adesione lo si ricava da considerazioni fin troppo scontate.

Quanto alla pretesa insussistenza di **divieti d'uso**, sia consentito ricordare come questi ricorrano quando il precetto di una disposizione non solo è costruito in termini di "proibizione", secondo formule linguistiche quali "è vietato", "non sono ammesse" o "non sono consentite" ([47]), ma anche quando è cadenzato nella **forma della "permissione"**, ovverosia quando il compimento o l'uso di un atto è subordinato alla presenza di determinati presupposti, che vanno così ad integrare lo schema tipico della fattispecie ([48]); l'assenza di uno di tali requisiti pone la "condotta probatoria" al di fuori del consentito, integrando il relativo divieto ([49]).

Tradotto in termini pratici, se il sistema normativo vigente presuppone che il dato informatico sia acquisito in giudizio secondo i dettami tecnici della *digital forensic* – che, tra l'altro, costituiscono «presupposto essenziale per il rispetto delle fondamentali garanzie a presidio del diritto di difesa dell'indagato» ([50]) – allora è chiaro come ogni altra forma di apprensione e/o

---

[45] Cass., Sez. II, 1.7.2015, n. 29061, in *Cass. pen.*, 2016, 4, p. 1706.

[46] Cass., Sez. V, 3.3.2017, n. 22695, in *Cass. pen.*, 2017, 12, p. 4466.

[47] Per tutte, Cass., Sez. Un., 27.3.1996, n. 5021, in *Foro it.*, 1996, II, p. 473, secondo cui i divieti probatori devono essere individuati non solo in «quelli espressamente previsti dall'ordinamento processuale, come accade, ad esempio, nei casi indicati dagli artt. 197 e 234, co. 3, c.p.p. e cioè, in materia d'incompatibilità a testimoniare o in relazione all'impossibilità giuridica di acquisire atti il cui contenuto faccia riferimento alle voci correnti del pubblico», ma anche in quelli implicitamente «desumibili dall'ordinamento e ciò, accade tutte le volte in cui i divieti, in materia probatoria, non sono dissociabili dai presupposti normativi che condizionano la legittimità intrinseca del procedimento formativo o acquisitivo della prova».

[48] Cfr. DINACCI, *Sequestro di dispositivi informatici: imposizioni tecnologiche e scelte interpretative. Alla ricerca di un recupero della legalità probatoria digitale*, in *Arch. pen. web*, 2025, 1, p. 18.

[49] Si rinvia, sul punto, a NOBILI, *Sub art. 191 c.p.p.*, in *Commento al nuovo codice di procedura penale*, vol. II, coordinato da CHIAVARIO, Torino, 1990, p. 441.

[50] COLAROCCO, GROTTO, VACIAGO, *La prova digitale : la casistica civile e penale e gli strumenti di acquisizione in ambito cloud*, Milano, 2020, p. 54.

riproduzione dello stesso debba ritenersi non permessa, sì da impedirne un utilizzo processuale ([51]).

Ma anche a voler prescindere da ciò, occorre comunque rilevare che l'invocato controllo giurisdizionale sulla genuinità della prova sia argomentazione destinata a perdere di sostanza, risolvendosi in mera petizione di principio, se rapportata alle fattispecie concrete prese in considerazione nel presente documento. Ed infatti, un Giudice **deprivato del dato digitale originale** non potrebbe compiere alcuna verifica sulla corrispondenza ad esso delle copie analogiche (*screenshot*, stampa o fotografia) ed informatiche (*files* video e/o audio "copiati ed incollati" su supporti di memoria esterni) prodotte dalle parti private; **il suo giudizio si sostanzierebbe in un atto di fede**, in un'acritica adesione ad un elemento di prova imperscrutabile.

Né il problema sembra risolvibile attraverso disinvolte alchimie interpretative in forza delle quali gli *screenshot* sarebbero sempre acquisibili alla stregua di documenti ([52]), mentre il supporto informatico della persona offesa (che ha prodotto quegli *screenshot* in giudizio) sarebbe sottoponibile a sequestro solo laddove quest'ultima, nel corso della sua deposizione, risulti non credibile o inattendibile ([53]).

---

[51] In questi termini, i canoni di genuinità e non alterazione della prova previsti dalla L. n. 48 del 2008 costituirebbero non delle «mere indicazioni operative prive di alcuna sanzione, ma veri e propri divieti impliciti presidiati dalla sanzione dell'inutilizzabilità» (cfr. PITTIRUTTI, *Digital evidence e procedimento penale*, Torino, 2017, p. 159).

[52] *Ex plurimis*, Cass., Sez. III, 6.11.2019, n. 8332, in *CED Cass. pen.*, 2020, rv 278635, ad avviso della quale non vi è «alcuna illegittimità nella realizzazione di una fotografia dello schermo di un telefono cellulare, sul quale compaiano messaggi *sms*, allo scopo di acquisirne la documentazione, non essendo imposto dalla legge alcun adempimento specifico per il compimento di tale attività, che consiste, sostanzialmente, nella realizzazione di una fotografia e che si caratterizza solamente per il suo oggetto, costituito, appunto, da uno schermo sul quale siano leggibili messaggi di testo, non essendovi alcuna differenza tra una tale fotografia e quella di qualsiasi altro oggetto, con la conseguente legittimità della sua acquisizione». Analogamente, Cass., Sez. V, 17.3.2023, n. 25037, in *CED Cass. pen.*, 2023, rv 284879-01; Cass., Sez. V, 26.4.2022, n. 24600, in *Diritto & Giustizia*, 2022; Cass., Sez. VI, 16.3.2022, n. 22417, in *DeJure*; Cass., Sez. V, 5.2.2021, n. 12062, in *CED Cass. pen.*, 2021, rv 280758-02; Cass., Sez. VI, 12.11.2019, n. 1822, in *DeJure*; Cass., Sez. III, 26.4.2017, n. 38681, in *DeJure*.

[53] Cfr. Cass., Sez. VI, 20.6.2023, n. 34089, in *DeJure*: «quanto alle schermate dei messaggi non è dubbia la loro utilizzabilità probatoria alla stregua dell'ormai consolidata giurisprudenza di legittimità, secondo cui è legittima l'acquisizione come documento di una conversazione via *whatsapp* o *sms*, realizzata dalla persona offesa mediante fotografia istantanea dello schermo – *screenshot* – di un dispositivo elettronico sul quale la stessa è visibile, senza che occorra procedere all'acquisizione e alla verifica tecnica del supporto telematico o figurativo contenente la relativa registrazione, tenuto conto – come nel caso in esame – della credibilità della persona offesa e della complessiva attendibilità delle sue dichiarazioni accusatorie in merito alla provenienza e al contenuto dei messaggi». Si veda anche Cass., Sez. II, 21.1.2025, n. 9475, in *DeJure*; Cass., Sez. II, 13.9.2024, n. 41504, in *DeJure*; Cass., Sez. V, 27.10.2022, n. 1358, in *Guida al diritto* 2023, 5; Cass., Sez. V, 6.10.2021, n. 2658, in *DeJure*; Cass., Sez. I, 20.2.2020, n. 14822, in *CED Cass. pen.*, 2020, rv 278943.

Per replicare a tale assunto, è sufficiente rammentare come l'istituto della prova documentale si ponga quale "eccezione" non solo al principio di immediatezza, ma anche a quello del contraddittorio: sicché, la connotazione dell'istituto, quale momento eccettuativo del metodo probatorio prescelto dalla Costituzione, impone – sempre e comunque – letture di stretta interpretazione.

In questa prospettiva, se è vero che l'art. 234, co. 1, c.p.p. consente «l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo», è anche vero che il secondo comma della citata disposizione statuisce che solo «**quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia**».

In sostanza, **la copia di un documento può essere acquisita a condizione che l'originale non sia più esistente e disponibile**.

Applicando tale postulato normativo al caso di specie, è agevole comprendere che quel che potrebbe essere acquisito alla stregua dell'art. 234 c.p.p. non è la stampa cartacea dello *screenshot* eseguito con il telefono cellulare, ma – semmai – l'immagine in formato *jpg* che viene automaticamente salvata nell'archivio delle foto. **Anche tale immagine, tuttavia, non offrirà alcuna garanzia di certezza**, posto che i relativi *metadati* (data, orario, provenienza) potranno soltanto confermare che lo *screenshot* è stato realmente scattato, non anche che quanto in esso rappresentato (ad esempio, una conversazione *chat*) non sia stato precedentemente manipolato.

In tale contesto, vincolare il sequestro del supporto informatico alla coerenza ed alla logicità delle dichiarazioni rese dalla persona offesa appare operazione che, per certi versi, rischia di assumere contorni paradossali ed irrealistici. In questo modo, infatti, **si finirebbe con l'affidare allo stesso soggetto che ha introdotto in giudizio un dato potenzialmente adulterato la conferma in ordine all'esistenza di tali adulterazioni**; con la conseguenza che, solo nell'inverosimile ipotesi in cui la presunta vittima del reato manifesti titubanze sulla veridicità delle riproduzioni analogiche da essa stessa prodotte, l'imputato sarebbe messo nella condizione di poter analizzare il supporto informatico contenente i dati digitali originali.

Interpretazioni ermeneutiche, quindi, in nessun modo condivisibili, ed anzi rese ancor più intollerabili dalla constatazione che le c.d. "regole del gioco" sembrano drasticamente cambiare quando è l'imputato a ricorrere a simili metodiche probatorie.

Solo in quest'ultimo caso, il formante giurisprudenziale è solito affermare che l'utilizzabilità di una conversazione *Whatsapp* – riprodotta dal reo in forma analogica, previa trascrizione della stessa – è «**condizionata dall'acquisizione del supporto telematico o figurativo contenente la menzionata registrazione, svolgendo la relativa trascrizione una funzione meramente riproduttiva del contenuto della principale prova documentale; tanto perché occorre controllare l'affidabilità della prova medesima mediante l'esame diretto del supporto onde verificare con certezza sia la paternità delle registrazioni sia l'attendibilità di quanto da esse documentato**» ([54]).

Delle due l'una: **o** tutte le parti private (nessuna esclusa), che producono "informalmente" dati digitali nel processo, sono tenute, a contestazione di controparte, a mettere a disposizione il dispositivo elettronico da cui tali dati sono stati estratti ([55]), **oppure** l'unico criterio in grado di prevenire il rischio di una contaminazione degli elementi di prova su cui si fonderà la decisione è quello che vincola l'estrapolazione delle "prove digitali" al rispetto delle *best practices*.

In assenza di ciò, il surrogato, analogico o informatico, di un dato digitale deve ritenersi inammissibile ovvero inutilizzabile ([56]).

---

[54] Cass., Sez. V, 19.6.2017, n. 49016, in *Cass. pen.*, 2018, 6, p. 2084. Cfr. anche Cass., Sez. I, 17.2.2024, n. 9436, in *DeJure*, dove la rappresentazione dei fatti rinvenienti da alcuni *screenshot* prodotti dall'indagato è stata ritenuta, da un punto di vista probatorio, *sub*-valente alla diversa ricostruzione dei fatti operata dalla polizia giudiziaria.

[55] In tal senso, si sta già orientando la giurisprudenza civile. Ad esempio, Cass., Sez. II, 18.1.2025, n. 1254, in *DeJure*, ha statuito che «in tema di efficacia probatoria dei documenti informatici, il messaggio di posta elettronica (c.d. *e-mail*) – e così i messaggi *whatsapp* – costituisce un documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti che, seppure privo di firma, rientra tra le riproduzioni informatiche e le rappresentazioni meccaniche di cui all'art. 2712 c.c. e, pertanto, forma piena prova dei fatti e delle cose rappresentate se colui contro il quale viene prodotto non ne disconosca la conformità ai fatti o alle cose medesime. E ciò pur non avendo l'efficacia della scrittura privata prevista dall'art. 2702 c.c.».

[56] Sotto diverso profilo, va ricordato come il ricorso alle *best practices*, oltre a garantire la genuinità dei dati raccolti, serva anche a permettere un controllo, da parte della difesa, sui contenuti e le modalità di acquisizione del documento informatico. Laddove la "prova digitale" fosse acquisita in violazione dei protocolli forensi, ne deriverebbe – in ogni caso – una lesione del diritto di difesa, *sub specie iuris* del diritto al contraddittorio nella formazione della prova, presidiato a pena di nullità dall'art. 178, co. 1, lett. c), c.p.p. e dall'art. 111 Cost.; ed infatti, il mancato rispetto delle citate procedure sottrarrebbe, di fatto, alla

4. Programmi di *editing* ed intelligenza artificiale – Nonostante le considerazioni che precedono risultino oltremodo bastevoli per ritenere esaurito l'argomento, sembra opportuno soffermarsi su alcuni orientamenti giurisprudenziali che colorano l'intera situazione anche in **termini assolutamente anacronistici**.

Secondo la Corte di Cassazione, la riconducibilità soggettiva di un messaggio scambiato, tra due persone, con il telefono cellulare – e, successivamente, depositato in giudizio sotto forma di *screenshot* – potrebbe essere dedotta alla luce delle informazioni rinvenienti proprio da tale *screenshot*. E così, ad esempio, se la conversazione ha avuto ad oggetto una minaccia di morte, e se su quello *screenshot* figura impresso il nominativo dell'imputato quale mittente del messaggio, allora ciò basterebbe per un responso di colpevolezza ([57]).

Affermazioni, queste, che lasciano, francamente, perplessi, ponendosi in una prospettiva a cavallo tra "negazione" e "misconoscenza" di tutto ciò che, negli ultimi anni, si è reso possibile grazie allo sviluppo della tecnologia moderna: **non dovrebbe, infatti, sfuggire che, in un mondo oramai dominato da programmi di *editing* e dall'intelligenza artificiale, ogni interazione umana può essere facilmente replicata, in maniera del tutto realistica, attraverso una banale operazione informatica**.

Alcune esemplificazioni possono aiutare a capire.

Come noto, *Whatsapp* è un'applicazione statunitense di messaggistica centralizzata, con cui i singoli utenti possono scambiare messaggi di testo, immagini, video, *files* audio, informazioni sulla posizione, documenti, contatti, nonché effettuare chiamate e videochiamate.

---

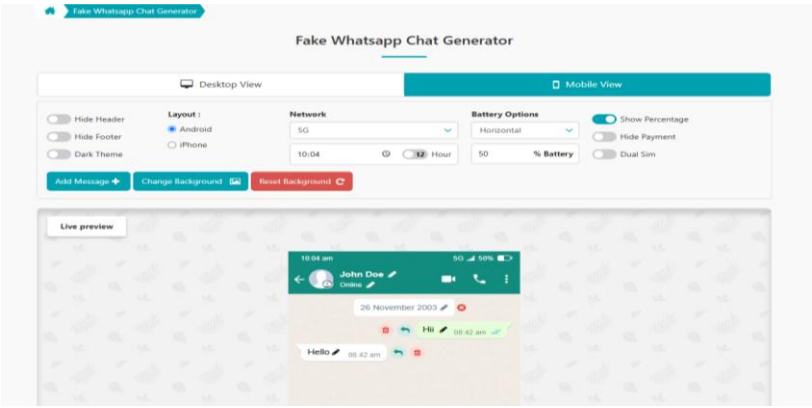
difesa la possibilità di contestare, mediante rilievi specifici, la credibilità della fonte di prova e la genuinità degli elementi da essa prodotti.

[57] Per convincersi di ciò, si veda Cass., Sez. I, 12.12.2023, n. 12673, in *Italgiure*, ove è stato affermato: «le dichiarazioni della Di Pietro hanno assunto, nell'economia della decisione impugnata, valenza centrale, anche perché riscontrate dagli *screenshot* dei messaggi scambiati con la Orlandi, registrata, nella rubrica di *Whatsapp* della Di Pietro, come "Alessandra San Salvo", con univoco riferimento alla località nella quale l'odierna ricorrente, in effetti, risiede». Ancora, Cass., Sez. IV, 19.10.2023, n. 48521, in *DeJure*, in cui si è ritenuta esente da vizi la sentenza impugnata in quanto «i giudici di merito hanno legittimamente ritenuto del tutto superfluo svolgere un accertamento tecnico sugli "*screenshot*" in questione, ritenuti del tutto attendibili in ragione della chiara riconducibilità dei messaggi ai soggetti menzionati, espressamente indicati nei messaggi con i relativi nomi di battesimo e, nel caso dell'Andali, con il soprannome "Totonno" (confermato dalla teste Palermo); inoltre, è stato logicamente considerato che il contenuto di tali messaggi era indiscutibilmente riferito ai rapporti di credito-debito intercorsi tra i vari soggetti di cui si tratta».

L'interfaccia di *Whatsapp* varia a seconda che il cellulare utilizzato sia un Android oppure un IOS ([58]).

Ipotizziamo, allora, una situazione di accesa conflittualità tra moglie e marito, in cui la prima, sapendo che il coniuge ha in uso un cellulare con sistema operativo IOS, decide di precostituirsi prove a proprio favore, da far valere successivamente all'interno di un giudizio civile (per separazione giudiziale) o penale (per minaccia aggravata).

Ebbene, mediante un programma denominato ***Fake Detail***, fruibile gratuitamente *on-line* ([59]), è possibile generare una conversazione *Whatsapp*, modificando – a proprio piacimento – le **impostazioni generali** (mittente, immagine, orario, stato, etc.), i **campi della batteria** e della **connessione**, nonché i **dati del messaggio** (contenuto, orario, spunta di lettura, etc.):



Ora, proviamo a conferire concretezza a tale esempio, riempiendo i suddetti campi nel seguente modo:

- nome del marito: Andrea Rossi;
- stato: *Online*;
- orario: 11:59;
- immagine: foto di Andrea Rossi ([60]);
- livello di batteria: 60%;
- connessione: 4G;

[58] Ad esempio, nel caso di sistema Android, la schermata di accesso si caratterizza per una barra verde posizionata nella parte superiore dello schermo (ove è presente il nome dell'applicazione ed i pulsanti per avviare la fotocamera, utilizzare la barra di ricerca e visualizzare le impostazioni) ed una barra bianca in basso, che consente di accedere alle diverse aree della piattaforma (*chat*, stato, *community* e chiamate).

[59] Www.fakedetail.com.

[60] Per ovvie ragioni, in questa sede, non potendo essere inserita l'immagine di un soggetto reale, è stata caricata un'immagine utilizzando Chat-Gpt.

- testo del primo messaggio inviato dal marito: *"Ti faccio fare una brutta fine. Ti ammazzo"*;
- orario del primo messaggio: 11:34;
- testo del secondo messaggio inviato dal marito: *"Non vivrai ancora per molto tempo"*;
- orario del secondo messaggio: 11:35;
- testo del terzo messaggio inviato dal marito: *"Ti farò passare molti guai. È meglio che non torni a casa"*;
- orario del terzo messaggio: 11:37;
- testo del quarto messaggio inviato dalla moglie: *"Ti prego non mi fare del male"*;
- orario del quarto messaggio: 11:38;
- spunta: blu di avvenuta lettura;
- testo del quinto messaggio inviato dalla moglie: *"Ho paura, sono mesi che mi minacci"*;
- orario del quinto messaggio: 11:39;
- orario del sesto messaggio inviato dal marito: *"È quello che ti meriti"*;
- orario del sesto messaggio: 11:50.

Ecco il risultato:

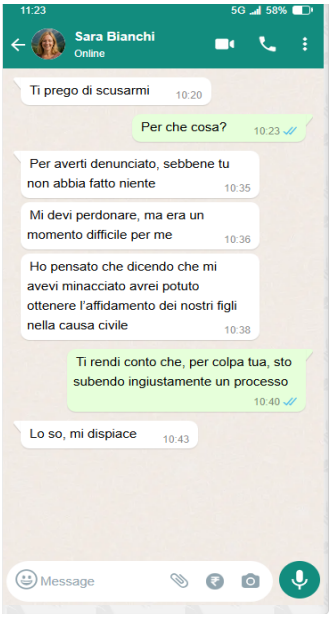
Ipotizziamo, ora, una situazione completamente inversa: il marito che, dopo essere stato denunciato dalla moglie per ripetute minacce realmente rivolte nei suoi confronti, vuole creare prove a proprio discarico, ben sapendo che la coniuge utilizza un cellulare con sistema Android.

In questo caso, servendosi del medesimo programma di *editing*, i campi potrebbero essere riempiti nel seguente modo:

- nome della moglie: Sara Bianchi;
- stato: *Online*;
- immagine: foto di Sara Bianchi ([61]);
- orario: 11:23
- livello di batteria: 58%;
- connessione: 5G;
- testo del primo messaggio inviato dalla moglie: *"Ti prego di scusarmi"*;
- orario del primo messaggio: 10:20;
- testo del secondo messaggio inviato dal marito: *"Per che cosa?"*;
- orario del secondo messaggio: 10:23;
- spunta: blu di avvenuta lettura;
- testo del terzo messaggio inviato dalla moglie: *"Per averti denunciato, sebbene tu non abbia fatto niente"*;
- orario del terzo messaggio: 10:35;
- testo del quarto messaggio inviato dalla moglie: *"Mi devi perdonare, ma era un momento difficile per me"*;
- orario del quarto messaggio: 10:36;
- testo del quinto messaggio inviato dalla moglie: *"Ho pensato che dicendo che mi avevi minacciato avrei potuto ottenere l'affidamento dei nostri figli nella causa civile"*;
- orario del quinto messaggio: 10:38;
- testo del sesto messaggio inviato dal marito: *"Ti rendi conto che, per colpa tua, sto subendo ingiustamente un processo"*;
- orario del sesto messaggio: 10:40;
- spunta: blu di avvenuta lettura;
- testo del settimo messaggio inviato dalla moglie: *"Lo so, mi dispiace"*;
- orario del settimo messaggio: 10:43.

Ecco il risultato:

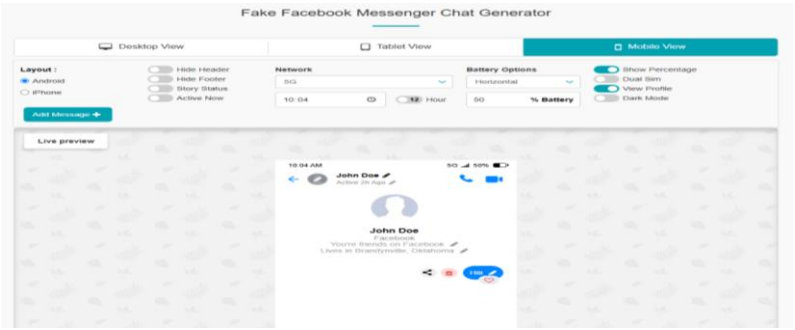
[61] Anche tale immagine, per le medesime ragioni, è stata generata con Chat-Gpt.



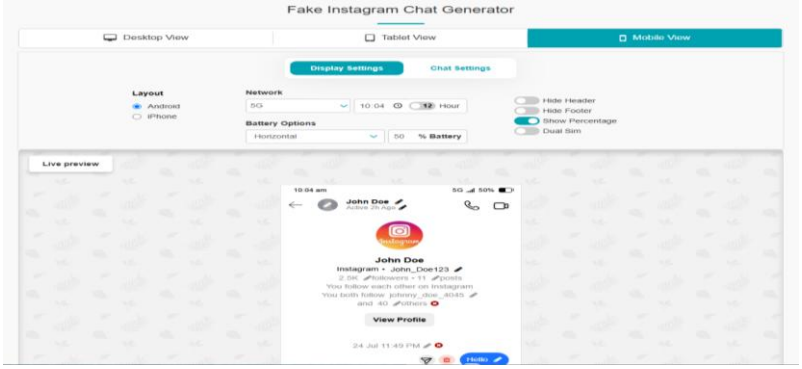
E si badi bene che il discorso non è destinato a mutare laddove si intendesse simulare una qualunque altra tipologia di conversazione, utilizzando i restanti servizi *chat* disponibili in rete.

Ed infatti, *Fake Detail* consente di replicare perfettamente le configurazioni dei seguenti *Social Network*:

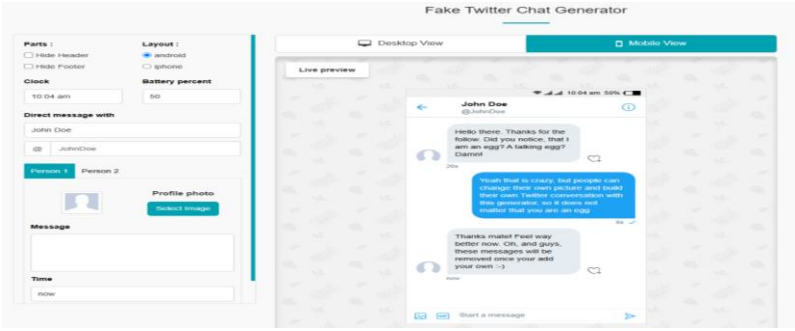
- Facebook



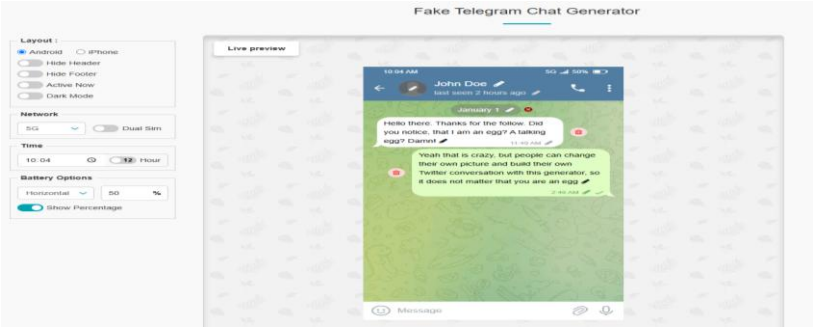
- Instagram



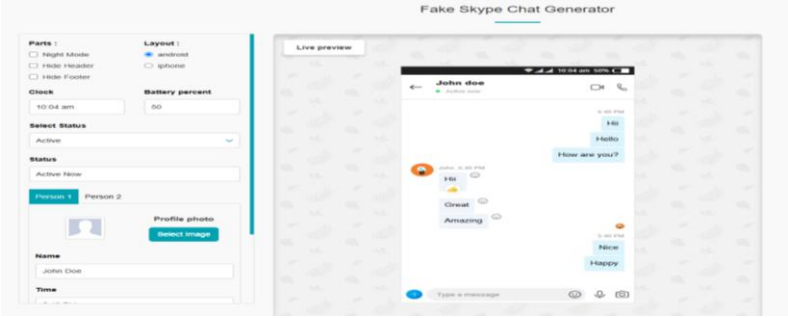
- Twitter



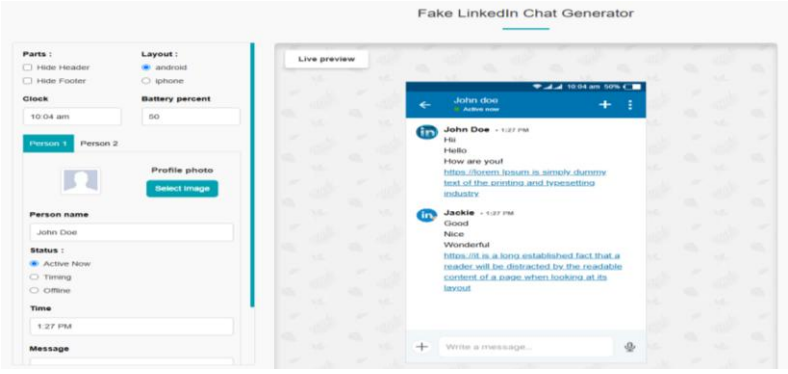
- Telegram



- Skype



- Linkedin



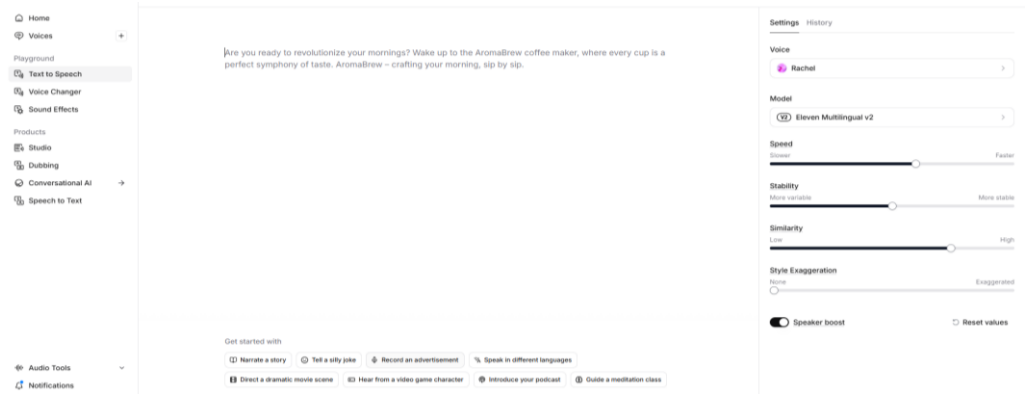
Inutile dire come, sul *web*, siano presenti moltissimi altri programmi di *editing* – alcuni *Open Source*, altri proprietari – che, in maniera del tutto analoga a *Fake Detalil*, permettono di creare, modificare o, comunque, dissimulare conversazioni tra due o più soggetti, in realtà mai avvenute.

Ma vi è di più.

Perché, navigando sul *web*, ci si può facilmente imbattere anche in numerosi altri applicativi di **intelligenza artificiale**, attraverso cui è possibile realizzare sia registrazioni audio, in cui viene clonata la voce appartenente ad una determinata persona, che – addirittura – interi videofilmati.

Si veda, a mero titolo esemplificativo, ***Eleven Labs***, ovverosia un *software* di c.d. "sintesi vocale del suono", in grado di riprodurre un parlato simulato utilizzando come modello di riferimento una registrazione vocale di un parlato reale; ciò tramite l'applicazione di avanzati algoritmi, specificatamente studiati per interpretare e rielaborare la voce umana, regolandone intonazione, ritmo ed emozioni ([62]).

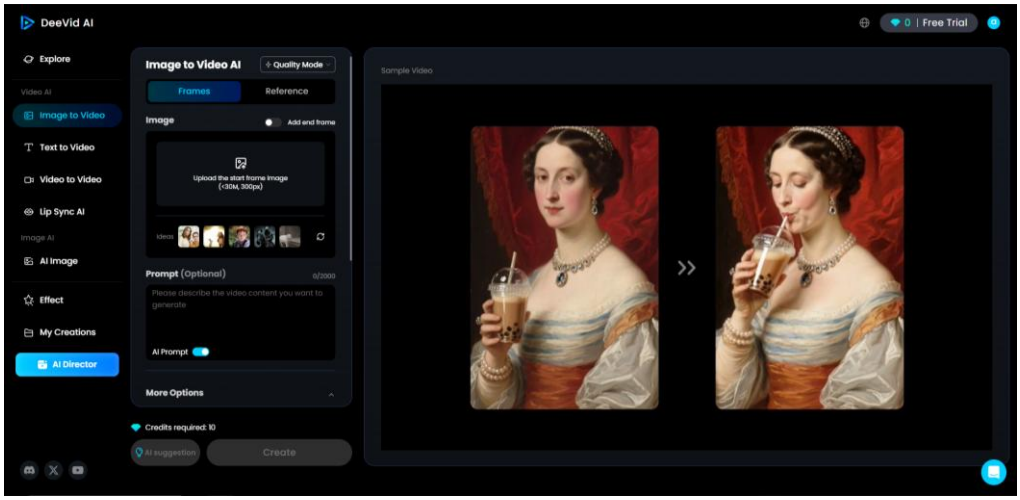
Per creare un vocale artefatto, è sufficiente accedere al sito di *Elen Labs*, inserire nell'apposita sezione una registrazione audio contenente la voce reale di una persona, scrivere – nello spazio dedicato al testo – la frase che si vuole attribuire a questa persona e modulare a proprio piacimento i *voice settings*:



Se, invece, si vuole creare un videofilmato falso, imputando ad un determinato soggetto gesti, azioni, movimenti o anche singole parole, uno dei programmi di intelligenza artificiale a cui si può ricorrere è ***Deevid Ai*** ([63]).

[62] Www.elevenlabs.io.
[63] Www.deevid.ai.

Anche in questo caso, basterà inserire un'immagine di un soggetto reale, scrivere la specifica azione che egli dovrà compiere o la frase che dovrà andare a pronunciare:



Emerge, dunque, dalle considerazioni che precedono la manifesta insostenibilità di quegli arroccamenti ideologici e culturali che, facendo leva su principi giurisprudenziali oramai desueti e non più al passo con i tempi, si ostinano a gestire il tema della "prova digitale" alla stregua dei criteri applicabili alle restanti tipologie di prove previste dall'ordinamento.

5. La richiesta – Il problema fin qui descritto rinvia ad una domanda che, per certi versi, sorge spontanea, una domanda che va rivolta all'intero ceto magistratuale, ossia a coloro che si trovano, quotidianamente, all'interno delle aule di giustizia, a dover dirimere questioni attinenti alle "prove digitali" prodotte dalle parti private: siete così sicuri che un Giudice – per quanto accorto e preparato possa essere – sia realmente in grado di distinguere una "prova digitale falsa" da una "prova digitale vera", pure quando questa prova sia stata depositata in giudizio tramite una semplice riproduzione della stessa, senza poter disporre del supporto informatico contenente il dato digitale originale e senza che, in fase di acquisizione, siano stati rispettati i criteri imposti dalle *best practices*?

La Camera Penale di Roma è convinta che a tale quesito non possa che darsi risposta negativa, e pertanto auspica, nel prossimo futuro, un coordinamento con il Procuratore Capo di Roma ed il Presidente del Tribunale, preordinato ad individuare una soluzione condivisa alla problematica relativa alla

gestione processuale dei dati digitali prodotti dalle parti private, in grado di tutelare tanto i diritti e le aspettative della presunta vittima del reato, quanto l'inviolabile diritto di difesa del soggetto accusato.