LA PROVA INFORMATICA NELLA PRATICA INVESTIGATIVA*

*Sandro Cutrignelli***

dis CRIMEN focus
3.7.2023

DIGITAL EVIDENCE

KEYWORDS Cybercrimes – Digital Evidence – Digital Search and Seizure – Impact on Fundamental Principles

Introduzione

L'*escalation* tecnologica, solo più visibile nell'ultimo decennio, da tempo ha fatto irruzione nell'ordinario svolgimento della vita umana scandendone ogni momento senza alcuna selezione generazionale, socio-culturale, geografica, politica, economica: la diffusione progressiva degli smartphone, per citare un esempio estremamente rappresentativo, consta di numeri impressionanti e si registra massiccia-

* Relazione al Corso di perfezionamento in diritto e procedura penale, IV edizione, *Internet tra diritto penale e processo*, tenutasi presso l'Università di Firenze il giorno 18 marzo 2022.

** Sostituto procuratore della Procura della Repubblica presso il Tribunale di Firenze.

mente sin anche nei paesi in via di sviluppo in aree dove la popolazione, in vasta parte con connotati di povertà assoluta e analfabetismo, è ancora afflitta dal problema dell'approvvigionamento di acqua potabile.

La familiarità con strumenti tecnologici sempre più performanti, le politiche di marketing aggressivo dei marchi e la commercializzazione di prodotti innovativi, in uno con l'impressionante tasso di vetustà del bene tecnologico, l'evoluzione del web e della telefonia mobile nelle sue varie declinazioni, ha prodotto trasformazioni socio-comportamentali ormai acquisite: è difficile finanche immaginare un essere umano che non disponga di (almeno) uno smartphone e di una connessione.

All'inconsapevolezza collettiva della reale portata di un tale cambiamento ha fatto riscontro la scettica indifferenza dei legislatori e degli enti sovranazionali, tutti accomunati dal brusco ridestarsi di fronte all'imponente impatto della tecnologia sulla sfera delle prerogative giuridiche della persona.

Big data, raccolta indiscriminata di dati sensibili, tracciamento delle posizioni di utenti e spostamenti, archiviazione seriale di indicazioni commerciali con cui strutturare politiche di marketing aggressivo, credenziali disseminate in luoghi digitali variamente setacciabili con tecnologie vieppiù efficaci e, soprattutto, la rivelazione di una capacità offensiva graniticamente reale delle condotte criminose perpetrate in rete: il web come consesso dei consessi nel quale, più o meno liberamente, agiscono attori che attingono bersagli vulnerabili fortemente esposti all'azione dei cybercriminali.

Su questa linea di tendenza si implementa una trama normativa che passa attraverso il riconoscimento della transnazionalità dei *cyber crimes*.

Dalla L. 23 dicembre 1993 n. 547 alla Convenzione di Budapest del 23 novembre 2001, ratificata con L. 18 marzo 2008 n. 48, al secondo protocollo addizionale alla Convenzione del 2 febbraio 2021 in materia di *subcriber data*; alla L. 23 dicembre 2021 n. 238 (Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea) in vigore dal 1° febbraio 2022, si assiste ad una reazione sempre più consapevole nel tentativo di raggiungere equilibri disciplinari in grado di far fronte alle continue sfide che la tecnologia pone.

Il cittadino digitale dispone di spazi cibernetici senza confini territoriali ai quali accede creando luoghi digitali e interazioni con le comunità globali disponendo di mezzi tecnologici in evoluzione perpetua.

Cambiano i modi d'essere dell'azione in un mondo tutt'altro che virtuale al quale si accede attraversando un *gate* con quella che ormai deve considerarsi

l'estensione tecnologica dell'essere umano: il dispositivo informatico nelle varie forme di *mobile* o *personal computer*.

È ormai comunemente accolto il principio secondo il quale, come in ogni società, anche in quella della rete si registrano fibrillazioni nei rapporti in termini di aggressione ai beni personali: l'insufficienza della *global governance* spinge così i legislatori a presidiare penalmente l'area dei diritti coinvolti nelle interazioni sul tracciato dei principi sovranazionali pattizi.

È possibile tracciare una linea concettuale sulla quale si muove il legislatore? Sono individuabili principi che accomunano l'azione legislativa sul piano sostanziale e processuale? Persistono e resistono i principi giuridici di rango superprimario alle nuove necessità imposte dall'evoluzione tecnologica progressiva? Come contemperare le esigenze di acquisizione e conservazione della prova con il sistema delle garanzie?

Questo lo scenario problematico, denso di aree conflittuali, nel quale collocare il presente contributo che, lungi dall'avere pretese di completezza, intende avanzare spunti di riflessione ed approfondimento piuttosto che fornire soluzioni nette e definitive.

1. *Cybercrimes*: il web e lo strumento informatico

Se è vero che i tratti comuni dei *cybercrimes* sono il web e lo strumento informatico, ormai propaggine umana, è altrettanto innegabile che il legislatore abbia operato una scelta di fondo che, partendo dalla presa d'atto dell'effettività dell'agire digitale e del suo impatto sul mondo reale, rivolge lo sguardo alle evoluzioni tecnologiche.

In tal modo, così come l'art. 615-*ter* c.p. presidia i luoghi digitali dell'avente diritto, al pari del domicilio fisico (art. 615 c.p.), vietandone l'intrusione in ogni modo tecnologicamente possibile, al contempo stabilisce modalità di ricerca e acquisitive libere, sul piano procedimentale, ponendo, con l'art. 247, co. 1-*bis* c.p.p., due obblighi, tecnologicamente orientati, ossia: 1) la conservazione dei dati originali e 2) l'adozione di tecnologie volte ad impedire, a chiunque, l'alterazione dei dati medesimi.

La disciplina del mezzo di ricerca della prova, diventato all'evidenza strumento principale nell'azione di repressione dei *cybercrimes*, evoca chiaramente l'aspetto dinamico e mutevole della categoria principale di riferimento, ossia la tecnologia e, dunque, la scienza, ed attribuisce un ruolo decisivo a quell'aggiornamento permanente rinvenibile in linee guida e *best practices* che anche in altri campi svolgono un ruolo determinante tanto sul piano oggettivo causalistico che su quello soggettivo previsionale.

Si scorge, dunque, un filo conduttore che, a fronte di un campo d'azione fortemente tecnologico e dinamico, lega e collega principi nient'affatto innovativi, principi ben conosciuti dagli operatori del diritto.

Se tale scelta dei criteri selettivi dell'accertamento penale non si discosta dalla tradizione giuridica, le conseguenze applicative concrete producono, come da più parti evidenziato, una traslazione del momento di *effettiva formazione* della prova in un ambito, quello delle indagini preliminari, diverso dalla sua sede processuale naturale, ossia quella tipicamente dibattimentale, così da suggerire una sorta di ossimoro, racchiuso nella intuitiva definizione – questa sì fortemente innovativa – di *prova investigativa*.

2. La perquisizione informatica e la volontarietà dell'azione: ristrutturazione dei dati, analisi e dimostrazione

Qualche dettaglio in ordine alla perquisizione informatica disciplinata dall'art. 247, co. 1-*bis* c.p.p. pare opportuno.

Muovendo dunque da modalità di ricerca e acquisitive libere, in sintonia con linee guida e *best practices* per il raggiungimento del risultato tipico, entro i limiti ordinamentali suindicati (garanzia dell'integrità e genuinità del dato originale, impedimento della sua alterazione), l'esecuzione del mezzo di ricerca della prova presenta profili decisamente innovativi.

Indispensabile fugare dubbi interpretativi e incertezze operative: il legislatore si riferisce chiaramente al rilievo (ed acquisizione) di dati e documenti in *bit* (caratterizzati da immaterialità); tuttavia, bisognerà in prima battuta interrogarsi su:

- quali sono i dati cui la norma si riferisce;
- come si conserva il dato originale nella fase acquisitiva;
- come se ne impedisce l'alterazione;
- se l'integrità da garantire riguardi il dato e non il dispositivo.

2.1. - *I dati*

I dati in questione sono all'occorrenza variegati. Essi non sono soltanto i *bit* strutturati in *file* o *metafile*, così da formare un autonomo documento allocato in un preciso *folder* (*storage*) a disposizione dell'utente, bensì anche i pacchetti di dati de-

strutturati che attengono ai processi eseguiti dalla macchina, alla navigazione ed alla connettività.

Lungi dall'essere dati di mero corredo, la loro analisi e aggregazione consente di ristrutturare l'azione eseguita con il *device* restituendo un quadro preciso dell'agire umano oggetto di indagine; tali dati, analizzati unitamente al *file* bersaglio, forniranno elementi che consentiranno non solo di ristrutturare il profilo oggettivo bensì il tratto psicologico in termini di volontarietà e consapevolezza dell'agire.

Viene così in reale evidenza la tradizionale affermazione secondo cui l'elemento psicologico del reato è desunto dall'azione: essendo questa una manifestazione fenomenica della psiche umana, l'analisi dettagliata consentirà – più che nei tradizionali reati – di collocare nella sfera della consapevolezza e volontarietà tanto l'azione quanto l'evento, escludendo il dolo ove sia la prima che il secondo risultino accidentali (come in passato si è registrato tra utenti dei *torrent*, ad esempio).

V'è chi sostiene, a ragione, che con la perfetta esecuzione delle operazioni di acquisizione e la corretta analisi dei dati la traiettoria probatoria subisca una *traslazione dal piano argomentativo*, tipico delle discipline umanistiche, a quello peculiare della *scienze esatte*, più propriamente *dimostrativo*: l'evocazione chiaramente matematica del termine esprime, infatti, la possibilità di raggiungimento della *certezza* che una *data azione* sia stata *consapevolmente compiuta* e che una *sequenza di azioni riveli inequivocabilmente l'intenzione dell'agente*.

2.2. - *La conservazione e la catena di custodia. La securizzazione*

Quanto alla *conservazione* del dato originale, da garantire sin dalla fase acquisitiva, viene in rilievo la c.d. *chain of custody*, la catena di custodia, nella quale sarà annotata integralmente e dettagliatamente la sequenza delle operazioni compiute, con indicazione dei soggetti e di quanto altro necessario allo scrutinio del momento procedimentale che si concluderà con la *securizzazione*, ossia con quella ulteriore sequenza di operazioni finalizzate ad *impedire l'alterazione del dato* (ablazione delle credenziali, procedura di *recovery* per il loro mutamento con definitiva perdita di controllo da parte dell'originario titolare).

La decisa vocazione tecnologica delle operazioni acquisitive da compiere secondo la sequenza appena esposta consente di affermare che proprio l'utilizzo di software forensi adeguati agli standard tecnologici più evoluti e comunemente riconosciuti come consoni allo scopo rappresenterà un momento di verifica dibattimentale

dell'attendibilità della fonte di prova attraverso il metodo dialettico; ma ad una più attenta analisi della questione, emerge la singolarità costituita dal fatto che *ben poco si potrà ulteriormente compiere rispetto a quanto già compiuto materialmente nella fase delle indagini preliminari* se non *dibattere sul metodo acquisitivo*, con finalità difensive eminentemente demolitorie aventi come bersaglio la *mancata conservazione del dato originale* o la sua *alterazione* come conseguenza di azione umana errata.

Compiute le operazioni di perquisizione e sequestro con impiego di personale esperto di polizia giudiziaria o di consulenti tecnici, l'esito del rilievo eseguito a regola d'arte costituirà un ecosistema chiuso che sarà comunicato al Giudice mediante esame testimoniale o esame del consulente: null'altro al di fuori di questo canale di comunicazione del dato al Giudice al quale si potrà tuttalpiù produrre un sapere demolitorio finalizzato a minare l'attendibilità della relazione/annotazione per il mancato rispetto degli obblighi di conservazione e inalterabilità.

Se tale sostanziale anticipazione al momento delle indagini della prova penale (o di quella che tale diventerà con il semplice passaggio di fase) sembrerebbe sottrarre la prova alla sua collocazione naturale nella fase dibattimentale, così da suggerire – come già accennato – la locuzione definitoria di *prova investigativa***,** ancor più evidente si rivela la questione della *reale capacità critica del Giudice sulla valutazione di un dato di carattere fortemente tecnologico*, cosa che ridonda sulla sostanziale *indipendenza della decisione* da quanto affermato dall'organo tecnico, sia esso operatore specializzato di polizia giudiziaria, sia esso consulente o perito.

A ben guardare, si tratta di una questione non dissimile da altre analoghe che si pongono tutte le volte in cui dal sapere scientifico/tecnologico dipende la decisione del Giudice, per quanto il passo dell'evoluzione della scienza informatica sembra decisamente più celere degli altri campi di scienza; la pretesa di un *know how* sempre più specialistico da parte del PM e del Giudice sembra attestarsi, oggi, come soluzione pressante nella misura in cui una conoscenza progressivamente adeguata ed aggiornata della materia in questione consentirebbe l'affrancamento dei due organi dalla produzione di sapere scientifico dell'operatore specialista, del consulente o del perito che, solitamente, precede e determina la decisione.

E non è in una sola direzione che va ricercato il rimedio posto che, più che alla possibilità di condanna basata su di un sapere scientifico erroneo o inattendibile, è la possibilità di sfuggire a responsabilità a preoccupare oggi maggiormente poiché, vuoi per la tecnica elusiva impiegata dall'agente, vuoi per la sofisticatezza tecnologica dell'azione, può ingenerarsi quel dubbio rilevante sull'effettiva (doppia) riferibilità

del fatto all'indagato/imputato che condurrà inevitabilmente all'assoluzione.

Le ricadute di queste riflessioni sul piano della domanda di qualità dell'azione investigativa sono molteplici: al di là dell'ovvia sollecitazione alla cura massima da riporre nell'esecuzione delle operazioni, reputo necessario richiamare l'attenzione a quel momento fondamentale dell'aggiornamento permanente cui si è fatto cenno.

La documentazione dell'attività dell'operatore dovrà essere meticolosa pur non sovrabbondante, dettagliata benché sintetica ed essenziale, e dovrà contenere indicazioni relative alle implementazioni dei software impiegati per l'estrazione del clone immagine della memoria del *device*, con menzione dell'ultimo *upgrade* o *release* disponibile al tempo dell'esecuzione delle operazioni.

Il ricorso alla riproduzione videografica sarà opportuno nelle fasi salienti delle operazioni, e la documentazione video dovrà riguardare anche i momenti nei quali è richiesta la partecipazione attiva dell'indagato, questione problematica per il potenziale conflitto con aree costituzionalmente presidiate (*nemo tenetur se detegere*).

Sul filo della ricerca del giusto contemperamento degli interessi confliggenti e sullo sfondo dei principi di minimo sacrificio e di proporzionalità si muove, del resto, la giurisprudenza più evoluta e sensibile alle elaborazioni delle Corti sovranazionali.

2.3. - *Criticità possibili: la rimozione delle misure di sicurezza e l'accensione del dispositivo*

Ultima notazione di carattere tecnico-giuridico: al di là della stretta qualificazione del *device* (e in generale del contenitore materiale dei dati) come cosa pertinente al reato o corpo di reato in senso stretto, e della considerazione della necessarietà della sua materiale apprensione, sovente si pongono due questioni, la cui corretta soluzione influenzerà le sorti dell'accertamento: la prima attiene alla c.d. *forzatura dell'accesso*, ossia alla rimozione delle variegate misure di sicurezza che proteggono il *device* dall'intrusione (biometriche, alfanumeriche, a doppio fattore e consimili); la seconda riguarda gli *effetti dell'accensione* del dispositivo rinvenuto spento del quale la Polizia Giudiziaria voglia ispezionare il contenuto, posto che la connessione sempre attiva del dispositivo al web comporta aggiornamento di taluni dati e mutamento sostanziale degli stessi.

Entrambe le problematiche impattano potenzialmente su uno degli obblighi imposti dal legislatore che ha disciplinato la perquisizione informatica, dovendosi as-

sicurare la *conservazione* dei dati originali, nella misura in cui entrambe le operazioni potrebbero comportare l'alterazione dei dati medesimi.

È richiesta una attenta riflessione dell'operatore, unitamente ad una elevata capacità valutativa tecnica, posto che in entrambi i casi bisognerà svolgere una analisi preliminare di carattere strutturale del *device* e del *software* disponibile, valutare se la tempestività dell'accesso è inevitabile, se l'operazione è differibile e, soprattutto, se si sarà in grado di adempiere all'obbligo conservativo.

2.4. - *Atto ripetibile o irripetibile: rilevanza della distinzione*

Erroneamente, sembra, viene posta la questione della ripetibilità o meno dell'accertamento: sul punto, la giurisprudenza di legittimità è ormai irremovibile.

Così, del resto, l'esemplare pronuncia della Suprema Corte n. 38909/2021[1]: "L'estrazione di dati archiviati in un supporto informatico, quale è la memoria di un telefono cellulare, non costituisce accertamento tecnico irripetibile, e ciò neppure dopo l'entrata in vigore della legge 18 marzo 2008, n. 48, che ha introdotto unicamente l'obbligo di adottare modalità acquisitive idonee a garantire la conformità dei dati informatici acquisiti a quelli originali, con la conseguenza che né la mancata adozione di tali modalità, né, a monte, la mancata interlocuzione delle parti al riguardo comportano l'inutilizzabilità dei risultati probatori acquisiti, ferma la *necessità di valutare*, in *concreto*, la sussistenza di eventuali *alterazioni* dei dati originali e la corrispondenza ad essi di quelli estratti".

In sostanza, l'estrazione della copia clone non è un accertamento di carattere irripetibile, essendo più simile ad un rilievo: partecipata o meno che sia l'operazione tecnica, resta unicamente il problema della *conservazione del dato originale* e della *corrispondenza ad esso del dato estratto*, non potendo discendere l'utilizzabilità dalla mera partecipazione dell'indagato, dovendosi al contrario escludere l'utilizzabilità dei dati ove ne venga messo in crisi il *processo acquisitivo* e, per tale via, la *corrispondenza ai dati originali.*

Si apre così uno scenario potenzialmente critico con conseguenze a cascata: è infatti possibile che, per errore umano, 1) siano irrimediabilmente modificati i dati originali e venga, dunque, definitivamente compromessa la loro conservazione o 2) che i dati originali siano integri essendo invece non corrispondenti ad essi i dati clonati.

[1] Cass. pen., sez. I, 10 giugno-28 ottobre 2021, n. 38909 in *Ced* rv. 282072 – 01.

Ferma restando la necessità di scegliere il percorso tecnologico più confacente ad accedere al *device* aggirando l'eventuale misura di sicurezza posta a suo presidio (senza la collaborazione dell'indagato, s'intende) ed all'estrazione della copia clone dei dati complessivi (comprendenti i dati di navigazione e di connettività), c'è da chiedersi quali siano le sorti dell'accertamento, e dunque del processo stesso, ove una delle suddette evenienze si verifichi.

Orbene, è piuttosto *agevole* dare *risposta* al problema della *irrimediabile compromissione* del *dato originale*: un siffatto errore sarà semplicemente fatale per il procedimento penale, non potendosi neppure immaginare un recupero (ed utilizzo) parziale di singoli elementi ove sia stata messa in crisi l'originalità.

Diversamente, ove sia nella disponibilità il dato originale integro e sia messa in crisi la corrispondenza ad esso della copia clone, il Giudice potrà ripetere l'operazione tecnica *a condizione che sia ancora disponibile il* device: tale puntualizzazione è più che opportuna, ed apre la via ad una ulteriore ed importante riflessione, ove si consideri che, se per un verso il legislatore mostra variamente di non gradire un sequestro in perpetuo del dispositivo elettronico, suggerendone la restituzione dopo l'estrazione della copia clone, per altro verso, l'aumentata funzionalità dei dispositivi nello *storage* diretto o indiretto di quantitativi enormi di dati variegati, solo alcuni dei quali connessi da pertinenzialità con il fatto-reato per il quale si procede, spinge la giurisprudenza nazionale (in sintonia con quella di provenienza sovranazionale)[2] a sostenere univocamente che "*lo smartphone sequestrato deve essere restituito al legittimo proprietario dopo che è stata realizzata la copia forense*" in mancanza di specifica e completa motivazione sulla persistente esigenza investigativa e sulla conseguente necessità di mantenere il vincolo sul bene, *dovendosi escludere che la potenziale erroneità dell'estrazione della copia clone possa essere posta a fondamento del diniego di restituzione*.

Sicché, in definitiva, potrebbe darsi il caso in cui, avvenuta la restituzione del dispositivo all'avente diritto, e accertata la non corrispondenza della copia clone all'originale per difetto della procedura acquisitiva, l'accertamento non sarà più fenomenicamente ripetibile dal Giudice dibattimentale o, quand'anche si rimettesse a disposizione il *device*, giuridicamente non più attendibile per esser stato il dato complessivo modificato.

[2] Cass. pen., sez. VI, 18 novembre 2022, n. 44010.

2.5. - *Restituzione del dispositivo e necessaria conservazione delle fonti di prova: prospettive esegetiche e tensione tra principi costituzionali*

E allora v'è da dubitare della costituzionalità di un siffatto orientamento, pur giustificato dal principio di ragionevolezza del sacrificio e proporzionalità dell'acquisizione, a fronte di altri principi altrettanto ben definiti dalla Corte Costituzionale quali quello di "necessario accertamento dei fatti aventi rilevanza penale"[3] e quello "di conservazione e non dispersione degli elementi di prova legittimamente acquisiti"[4].

È dunque sul piano dell'alta definizione tecnica dell'accertamento e della reale capacità valutativa degli operatori del diritto, PM e Giudice compresi, che si giocherà la partita del giusto ed efficace processo penale.

2.6. - *Integrità del dato e del dispositivo*

La dissertazione che precede consente inoltre di dare risposta ad un quesito, posto in premessa, dall'apparenza neutra: l'obbligatorietà dell'integrità del dato si estende al dispositivo? La risposta è, all'evidenza, negativa, fatta la tara dal principio di indispensabilità del sacrificio delle prerogative della persona, in maniera non dissimile dalla rimozione degli ostacoli fissi che si frappongano all'esecuzione di una perquisizione ordinaria.

3. I dispositivi e l'azione umana: il nuovo senso della doppia riferibilità. Principi fondamentali ed assolutezza mitigata

L'accresciuto interesse dei giuristi per il mondo *cyber* e la consapevolezza progressivamente raggiunta della reale portata sociale del cambiamento globale già avvenuto da tempo ed in continua evoluzione conduce spesso ad operare prove di resistenza dei tradizionali principi giuridici nel contesto delle nuove relazioni digitali.

La connessione pressoché perpetua dell'uomo al web, l'astrazione dalla percezione fenomenica tradizionale del reato e la sua traslazione nell'ambito delle relazioni digitali, la spersonalizzazione di attaccante e bersaglio, dell'azione e delle sue conseguenze, la dispercezione della reale portata degli attacchi *cyber* alla sicurezza nelle sue varie articolazioni sostengono sempre più il dibattito relativo alla tenuta dei

[3] Corte cost., 26 marzo 1993, n. 111, in www.cortecostituzionale.it.

[4] Corte cost., 2 novembre 1998, n. 361, in www.cortecostituzionale.it.

principi delle Carte Fondamentali, nazionali e sovranazionali, nel contesto globale delle *new technology* e della mutata morfologia delle interazioni umane.

L'azione dei governi e dei legislatori nazionali, così come quella degli organismi sovranazionali, ha recentemente mostrato un progressivo orientamento vero la mitigazione dell'assolutezza dei principi fondamentali.

Qualche esempio.

3.1. - *Le limitazioni nelle pronunce della CGUE*

3.1.1. - *Corte di Giustizia dell'Unione Europea, sez. grande, 5 aprile 2022, C-140/20 (in materia di conservazione dei dati relativi al traffico e all'ubicazione di persone diverse da quelle sospettate)*

Sulla base dell'art. 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al *trattamento dei dati personali* e alla tutela della vita privata nel settore delle comunicazioni elettroniche, come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli artt. 7, 8 e 11 e dell'art. 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, sono legittime le misure legislative nazionali che prevedano, per finalità di *lotta alla criminalità grave e di prevenzione delle minacce gravi* alla sicurezza pubblica, sia la *conservazione temporalmente limitata allo stretto necessario*, ma *rinnovabile*, e *mirata*, sulla base di elementi oggettivi e non discriminatori, dei *dati relativi al traffico e all'ubicazione di mezzi di comunicazioni elettronica*, sia la *conservazione generalizzata* e *indifferenziata* degli *indirizzi IP* attribuiti all'origine *di una connessione* e *dell'identità civile degli utenti* di questi mezzi di comunicazione elettronica, per un periodo temporalmente limitato allo stretto necessario. In questa ottica di *bilanciamento proporzionato*, per le medesime finalità e purché in presenza di norme chiare e precise sulle condizioni sostanziali e procedurali e delle garanzie effettive a favore delle persone interessate contro il rischio di abusi, la Corte reputa, altresì, *legittimo* il ricorso a un'*ingiunzione* – emessa da autorità competente, anche fin dal primo atto d'indagine, e soggetta a un controllo giurisdizionale effettivo – rivolta *ai fornitori di servizi di comunicazione elettronica*, di procedere, per un *periodo determinato*, alla *conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione* di cui essi dispongono, anche se riguardanti *persone diverse da quelle sospettate*, ma che anteriormente al verificarsi di una minaccia grave per la si-

curezza pubblica o alla commissione di un atto di criminalità grave, abbiano avuto *contatti con la vittima* attraverso mezzi di comunicazione elettronica (sullo sfondo, tra gli altri, *i requisiti di indipendenza e di imparzialità*).

3.1.2. - *Corte di Giustizia dell'Unione Europea, sez. grande, 26 aprile 2022, C-401/19 (estensione di responsabilità ai fornitori di servizi di condivisione per la violazione del diritto d'autore e limitazione al diritto alla libera manifestazione del pensiero)*

La Corte di Lussemburgo si è occupata nella pronuncia in commento della legittimità dell'art. 17 della direttiva 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale, il quale prevede che i fornitori di servizi di condivisione di contenuti online siano direttamente responsabili nel caso in cui materiali protetti dal diritto d'autore siano *caricati illegalmente* dai propri utenti.

Con ricorso presentato alla Corte, la Polonia ha infatti chiesto l'annullamento del suddetto articolo in quanto sarebbe stato contrastante con la tutela del diritto alla libera manifestazione del pensiero (art. 11 Carta di Nizza). In particolare, è stato contestato che il regime previsto dal paragrafo 4 dell'art. 17, secondo cui i *fornitori* di servizi, per andare esenti da responsabilità, hanno l'obbligo di compiere i *massimi sforzi*, da un lato, per assicurare che non siano disponibili contenuti protetti specifici per i quali i titolari di diritti abbiano fornito le informazioni pertinenti e necessarie e, dall'altro, per impedire che i contenuti protetti oggetto di una segnalazione sufficientemente motivata da parte di tali titolari *siano caricati in futuro*, costringa gli stessi fornitori di servizi ad operare una *sorveglianza preventiva tramite filtraggi automatici dei contenuti*, con *grave pregiudizio delle libertà d'espressione e d'informazione*.

Pur riconoscendo che il regime previsto dalla norma europea comporta effettivamente una *limitazione dell'esercizio del diritto alla libertà di espressione e d'informazione* degli utenti di tali servizi di condivisione, la Corte afferma che tale limitazione deve ritenersi *legittima e giustificata*, secondo i criteri previsti dall'art. 52 della Carta di Nizza, in virtù del complesso regime previsto dall'art. 17, comprensivo di paragrafi successivi (da 7 a 10), contenenti correttivi che mirano a garantire che la limitazione della libertà d'espressione sia espressamente prevista dalla legge nei suoi contenuti e nelle sue modalità, nonché debba essere necessaria e proporzionata al *contro-interesse* che si intende tutelare: in questo caso, la *proprietà intellettuale*.

3.2. - *Le limitazioni nel diritto convenzionale. La Commissione Europea.* The Strengthened Code of Practice on Disinformation *2022 (ancora in materia di limitazione al diritto d'espressione)*

Il 16 giugno 2022 è stata adottata la *versione rafforzata del codice di buone pratiche* per le piattaforme online, le associazioni di categoria e i principali operatori del settore pubblicitario per *contrastare la disinformazione* e migliorare le loro politiche online, adottato per la prima volta nel 2018.

Mentre il codice del 2018, con 16 firmatari, prevedeva impegni basati sull'autoregolamentazione, inerenti al *vaglio degli inserzionisti pubblicitari*, l'integrità dei propri servizi, la responsabilizzazione dei consumatori, nonché dei verificatori di fatti e dei ricercatori, la *versione rafforzata*, con 34 firmatari, 44 impegni e 127 misure specifiche, si richiama alle *forme di co-regolamentazione* cui sono soggette le piattaforme online di dimensioni molto grandi nel quadro della normativa sui servizi digitali (*Digital Service Act*). Il codice rafforzato si prefigge inoltre di aumentare l'incisività delle misure e della *trasparenza della pubblicità politica e tematica*, nonché di garantire una sorveglianza completa dei *comportamenti manipolativi* attuali ed emergenti.

Tra gli impegni maggiormente rilevanti, si prevede di ampliare e rafforzare gli strumenti che consentono agli utenti di individuare e segnalare *contenuti falsi o fuorvianti*, istituire un solido quadro di monitoraggio e comunicazione, istituire un centro per la trasparenza e creare una *task force* permanente per l'evoluzione e l'adeguamento del codice.

Gli esempi citati concorrono a definire un *trend* che, complessivamente, si attesta sulla comune considerazione dell'accresciuta aggressività e dannosità delle condotte cybercriminose per contrastare le quali è necessario adottare misure la cui specialità si coglie, essenzialmente, nella compressione dell'estensione di diritti fondamentali.

3.3. - *La doppia riferibilità del fatto nei* cybercrimes

Tali premesse mirano a guidare il giurista di ultima generazione verso l'esegesi dinamica di principi costituzionali irrinunciabili, tradizionalmente evocativi di scelte politico-filosofiche ed espressione di un diritto punitivo oggettivamente orientato, di fronte alla esigenza pressante di arginare forme dilaganti di criminalità cibernetica.

Uno dei principi costituzionali in tensione crescente è, appunto, quello della

c.d. doppia riferibilità del fatto all'agente sia sotto il profilo oggettivo-causalistico che sotto quello soggettivo-doloso: il fatto-reato in ambiente *cyber* resta pur sempre, nel diritto penale, un fatto umano, commesso con volontà colpevole, la cui attribuzione all'agente, e la conseguente responsabilità, non può prescindere dall'accertamento della previsione e volizione dell'evento quale conseguenza della propria condotta consapevole e volontaria.

Richiami recenti del legislatore all'accertamento del profilo psicologico nitidamente doloso, come nell'art. 600-*quater*, co. 3 c.p. che richiede l'accesso *intenzionale* ed *ingiustificato* a siti web a contenuto pedopornografico, confermano la tendenza alla limitazione controllata di taluni diritti quale scelta di politica criminale.

4. Prospettive

4.1. - *Identificazione del dispositivo e dell'autore del reato. Linee guida e proposte operative*

Sul piano più strettamente procedimentale, le novità dell'investigazione tecnologica sono per lo più votate a scrutinare contenuti e connettività dello strumento informatico impiegato per la commissione del reato, ossia del dispositivo, che il sistema identifica attraverso il *matching* della combinazione utenza-*IP adress*.

Ciò porta sovente a ritenere, semplicisticamente, che nell'accertamento del reato *l'identificazione del dispositivo* coincida con *l'identificazione dell'autore* del reato; non è affatto così. Si scorge inoltre l'opinione, invero non isolata, secondo cui l'investigazione nei *cybercrimes* sia *esclusivamente tecnologica* e che la tecnica tradizionale di indagine sia semplicemente *superata*.

L'accostamento delle due questioni non è casuale, perché in sostanza si tratta di verificare la perdurante tenuta del principio costituzionale, irrinunciabile nel diritto penale, della *doppia riferibilità* del fatto all'agente sia sul piano oggettivo che su quello soggettivo; sicché una investigazione che si arresti all'identificazione dell'IP e, attraverso la ricerca dei *file* di *log*, dell'utenza associata, è incompleta nella misura in cui identifica soltanto il titolare dell'utenza: il fatto che usualmente quest'ultimo sia anche l'utilizzatore del *device* il cui codice IMEI risulta associato all'utenza non è argomento risolutivo perché non soddisfa di per sé il criterio della doppia riferibilità del fatto sul quale si fonda la responsabilità penale.

Una indagine accurata, che miri a definire in maniera lineare l'accertamento della responsabilità penale per un crimine cibernetico, deve invece far ricorso tanto alla tecnologia quanto alla tradizionale verifica di tutte le circostanze che, congiuntamente, identifichino un soggetto, ed uno solo (tranne che nel caso di reato plurisoggettivo, s'intende) come colui che abbia effettivamente compiuto l'azione volontaria per la realizzazione dell'evento considerato e vietato dalla fattispecie incriminatrice.

Sarà dunque, più che opportuno, addirittura necessario svolgere una accurata ricerca, nei tabulati relativi all'utenza, per identificare i contatti, esaminare le ricorrenze, verificare le posizioni tramite le celle attivate, effettuare in sostanza una attenta analisi preliminare per comprendere se il titolare dell'utenza sia effettivamente il bersaglio soggettivo alla cui rivelazione mira l'indagine.

Una volta identificato e localizzato il soggetto sarà ancora il caso di esaminare la connessione per verificare se essa serva una rete domestica e se questa sia aperta o protetta, da quante e quali persone è composto il nucleo familiare, da chi è solitamente frequentato il luogo servito dalla rete; e tutto ciò dovrà antecedere l'accesso materiale ed il momento della perquisizione informatica.

Effettuato poi l'accesso, la materiale apprensione del dispositivo potrebbe di per sé già essere un problema: quanto spesso e quanto frequentemente viene oggi cambiato uno smartphone? E quanti dati, nelle operazioni di migrazione, vengono dispersi? È spesso capitato, nell'esperienza pratica, di rimpiangere il fatto di non aver esteso la ricerca ai dispositivi in disuso.

Con l'apprensione materiale del dispositivo di interesse si avrà più o meno celermente accesso ad una serie di informazioni utili ad indirizzare l'indagine in maniera corretta: lo scandaglio dei luoghi digitali consentirà abbastanza rapidamente di comprendere se il titolare di utenza ed utilizzatore del dispositivo sia il bersaglio giusto.

Le attività che ne seguiranno, la formazione della *chain of custody*, l'estrazione della copia clone, l'analisi complessiva dei dati e la loro ristrutturazione, costituiranno un momento logicamente e cronologicamente successivo.

La cornice giuridica e normativa dell'azione investigativa è la stessa del procedimento di accertamento della responsabilità penale: è necessario attribuire ad un soggetto determinato il fatto reato argomentando – e talvolta dimostrando – che egli ha preveduto e voluto realizzare l'evento contemplato dalla fattispecie incriminatrice come conseguenza del suo agire; tutto ciò, si rammenta, *al di là del ragionevole dubbio*, perché tale parametro codicistico amplia e puntualizza l'estensione del principio della *doppia riferibilità*.

Il decalogo delle operazioni sopra riportato è esemplificativo, non categorico né esaustivo: linea guida di massima, serve a comprendere la direzione e la fluidità dell'agire investigativo.

4.2. - *L'estensione del principio della doppia riferibilità; prospettive future. Web 3 e metaversi*

Rientra, dunque, tra i principi ad assolutezza mitigata quello in esame? Se per un verso ci avviciniamo alla risposta, recisamente negativa, al quesito posto, per altro verso è opportuno interrogarsi sulle concrete possibilità di riuscita delle investigazioni, in un ambito nel quale la tecnologia evolve rapidamente in favore dei cybercriminali, ove si consideri che il principio portante della doppia riferibilità del fatto al di là di ogni ragionevole dubbio, come indicato dall'art. 533 c.p.p., deve interpretarsi nel senso che "*la pronuncia di condanna deve fondarsi sulla certezza processuale della responsabilità dell'imputato*"[5].

Lo spazio entro il quale collocare l'esito favorevole dell'indagine è vieppiù angusto ove si consideri che una delle direzioni nelle quali più rapidamente evolve la tecnologia è quella dell'elusione del tracciamento, dell'occultamento dell'identità digitale (pseudonimizzazione, anonimizzazione, falsa identità, mascheramento dell'IP): alle normali preoccupazioni dell'investigatore, chiamato all'identificazione certa di un singolo soggetto spesso collocato in un più ampio consesso di attori (*wi fi* domestica, cessione e condivisione di credenziali di accesso, reti aperte e consimili situazioni), dunque, si aggiungono quelle, per quanto straordinarie sempre più ordinarie, derivanti dall'impiego di tecnologie elusive oggi facilmente accessibili all'incommensurabile popolazione del web nelle sue variegate forme (*surface*, *deep*, *dark web*): VPN, *Proxy server* facilmente accessibili, NAT, computer violati, *Fake Identity Generator*[6], rendono talvolta inutile, talaltra impossibile l'indagine.

---

[5] Cfr. per tutte, Cass. pen., sez. II, 13 febbraio 2013, n. 7035; nel testo: "*il procedimento logico, (…) non dissimile dalla sequenza del ragionamento inferenziale dettato in tema di prova indiziaria dall'art. 192 c.p.p., comma 2, (…) deve condurre alla conclusione caratterizzata da un alto grado di credibilità razionale, quindi alla "certezza processuale" che, esclusa l'interferenza di decorsi alternativi, la condotta sia attribuibile all'agente come fatto proprio*".

[6] Di seguito talune indicazioni di sintesi:

a) VPN (*Virtual Private Network*): una VPN è un sistema che fa da tramite tra il computer dell'utente e i siti (o i servizi) utilizzati, nascondendo la sua identità (la connessione, tramite VPN, può risultare come proveniente da un altro paese) e proteggendo il traffico in entrata e in uscita. Consente di creare una rete privata virtuale che garantisce *privacy*, anonimato e sicurezza dei dati attra-

Anche alcune moderne forme di *storage* su *cloud* pressoché inaccessibili, protetti da crittografia avanzata, sono in grado di ostacolare il passo decisivo e finale dell'indagine nella misura in cui impediscono l'accesso, e dunque l'acquisizione, dei *file* oggetto di ricerca: per esemplificare, pur in presenza della certezza procedimentale dello scambio di *file* a contenuto pedopornografico, il loro *storage* su un *cloud* inaccessibile vanifica totalmente l'indagine.

Non più rischioso possesso materiale dei *file* scaricati in memoria, bensì disponibilità ideale dei *file* allocati su *cloud*; non più accesso ad una piattaforma con il

verso un canale di comunicazione riservato tra dispositivi che non necessariamente devono essere collegati alla stessa LAN; *link di interesse*: https://www.routech.ro/it/5-delle-migliori-alternative-tor-per-lanavigazione-anonima/(firefox); https://vpnoverview.com/it/la-privacy-online/navigazione-anonima/il-browser-tor/. Tra i fornitori di servizi più famosi VPN si segnalano Kaspersky e Cyberghost oltre che il *browser* TOR.

b) *Proxy server*: Un *proxy* è un "server intermediario", un computer che si posiziona tra un *client* (utente che naviga) ed un sito/pagina web che vogliamo visitare (ospitati in un server), facendo da tramite tra i due. Il processo è il seguente:

– L'utente (*client*) si collega al *proxy* e gli invia le richieste.

– Il *proxy* si collega al server ospitante il sito web e gli inoltra la richiesta dell'utente.

– Ricevuta la risposta, il *proxy* manda la risposta al *client*.

In pratica, non siamo più connessi direttamente al server del sito che visitiamo ma passiamo attraverso questo filtro chiamato *proxy* sia in entrata che in uscita. L'indirizzo IP del computer o della rete da cui l'utente naviga non comparirà mai direttamente nel corso della navigazione, risulterà visibile soltanto quello associato al server *proxy*. *Link di interesse*: https://www.aranzulla.it/server-proxy-63922.html#; https://www.aranzulla.-it/come-proxare-lip-32328.html; https://www.netinformatica.it/server-proxy/

c) *Fake Identity Generator*: generatori di identità fittizie da impiegare per registrarsi su siti web e *social* con falsi *account*; generalmente associati all'utilizzo di VPN o *Proxy server*. I siti specializzati attribuiscono anche numeri telefonici temporanei (tecnologia VOIP) sui quali dirottare i codici di autenticazione provenienti dal fornitore del servizio richiesto; *link di interesse*: https://www.navigaweb.net/2017/01/creare-account-web-falsi-anonimisu.html; https://www.fakenamegenerator.com/gen-male-it-it.php

d) NAT (*Network Address Translation*): è la tecnologia che consente ad un router di tradurre un indirizzo IP pubblico in un indirizzo IP privato e viceversa mantenendo gli indirizzi IP privati nascosti. Nasce storicamente per rimediare alla scarsità di indirizzi IP attraverso la *procedura dinamica di assegnazione degli indirizzi IP*. NAT permette dunque di "nascondere" dietro un unico indirizzo pubblico decine e decine di indirizzi privati (e quindi altrettanti dispositivi connessi alla rete). Sequenza: Il dispositivo richiede al *provider* internet di assegnargli un indirizzo IP; il *provider* (che ha a disposizione un ben determinato *pool* di indirizzi) ne assegna uno al computer richiedente uno degli IP disponibili; all'atto della disconnessione dalla rete l'indirizzo IP viene "liberato" e torna tra quelli disponibili e pronti per essere riassegnati. Non è materialmente possibile approntare l'indagine per identificare l'utilizzatore di una singola connessione NAT/CONDIVISA in mancanza di una presenza reiterata dello stesso in almeno due connessioni registrate in tempi diversi. *Link di interesse*: https://it.wikipedia.org/wiki/Network_address_translation; https://www.internetto.it/che-cose-il-nat-e-a-cosa-serve/.

proprio IP visibile ed una identità svelata, bensì mascheramento dell'IP tramite VPN e registrazione al servizio di posta elettronica, così come a *social network* e portali di servizi vari, con numeri telefonici fittizi, e *mail* ed identità false create da intelligenze artificiali (generatori di false identità, di numeri cellulari usa e getta, di *account* mail temporanei[7]).

Il passaggio dal regime della "*Voluntary Disclosure*" a quello della "*Mandatory Disclosure*" previsto dal Secondo Protocollo addizionale alla Convenzione di Budapest, che obbliga gli ISP a fornire alle autorità giudiziarie le informazioni, ancorché transfrontaliere, sulle identità degli utenti registrati (*subscriber data*), ratificato dall'Italia il 12 maggio 2022, rappresenta un tentativo comune di reagire al dilagante fenomeno dell'anonimizzazione, ma è illusorio credere che la soluzione al problema sia prossima, e ciò non soltanto a causa dell'elevatissimo numero di fornitori di servizi di messaggistica e della proliferazione incontrollata di piattaforme multifunzionali bensì a causa della trasformazione stessa del web e della sua progressiva decentralizzazione: l'avvento di Web 3, caratterizzato dalla mancanza di un fornitore centralizzato, di fatto vanifica a monte ogni sforzo volto all'identificazione.

Anche i più noti ISP, a ben guardare, benché adempienti già in passato agli ordini di esibizione, difettano di una procedura KYC di elevato livello, attendibile al punto da restituire la certezza dell'identificazione del sottoscrittore ed utente del servizio.

Un altro mondo digitale in continua espansione, inoltre, rappresenta oggi l'ennesima ardua sfida per gli investigatori prima ancora che per gli operatori puri del diritto: parliamo del Metaverso o, meglio, dei metaversi, agglomerati organizzati di luoghi digitali nei quali si articola una realtà virtuale i cui massicci effetti sulla realtà sono sotto gli occhi di tutti.

Dalle capacità di espansione addirittura imprevedibili, il metaverso è altresì dotato di un proprio ecosistema economico-finanziario e *block chain* secondarie che consentono, persino in un settore delicato come quello delle criptovalute, di eludere la normativa di settore ed aggirare gli obblighi informativi imposti agli *exchange*.

[7] Generalmente, per l'iscrizione a tutti i siti gratuiti, può bastare usare una *E-mail* temporanea ed anonima.

In tutti i casi in cui è richiesta invece una registrazione completa della persona, con tanto di indirizzo di casa, numero di telefono e codici di carte di credito, ci sono modi per *creare una identità falsa* ma realistica.

Sul sito *FakeNameGenerator* è possibile *creare una persona fasulla*, con tanto di nome, cognome e indirizzo di casa (con CAP e provincia), data di nascita, numero di Carta d'Identità, occupazione, peso, altezza ed anche numero di carta di credito. Ovviamente *ogni dato è assolutamente falso* e generato casualmente secondo gli *standard reali*.

Se questo è lo scenario nel quale si collocano le investigazioni sui *cybercrimes*, pur nella consapevolezza che l'evoluzione tecnologica contribuirà comunque ad implementare le tecniche di indagine, gli spazi per l'investigazione utile ed efficace sembrano restringersi.

4.3. - *Considerazioni conclusive e proposte operative. Lo statuto della prova nei* cybercrimes*. La rilevanza della presunta eccentricità.*

La cornice normativa primaria e secondaria entro la quale si disegna la traiettoria probatoria è, dunque, quella tradizionale: per quanto la tecnologia influenzi massicciamente tanto l'agire del cybercriminale e quanto lazione investigativa, motivazioni e punto d'approdo di entrambi restano quelli di sempre, ciascuno per parte propria.

Non è il contenuto tecnologico del fatto oggetto della prova a cambiarne il regime: lo statuto resta quello ordinario così come sulla stessa linea argomentativa si pone la considerazione che nessun algoritmo predittivo potrà mai determinare una sentenza di condanna ove non venga tradizionalmente dimostrato, in misura assai prossima alla certezza, ed in maniera conforme al modello normativo delle garanzie, che un soggetto ha preveduto e voluto l'evento quale conseguenza della propria condotta consapevole.

È dunque nel sistema della prova penale di derivazione costituzionale che deve collocarsi il percorso di ricerca e conservazione degli elementi di prova, a prescindere dall'elevato tasso di tecnologia che connota il fatto e l'indagine: il principio di doppia riferibilità del reato all'agente, al di là del ragionevole dubbio, non subisce alcuna compressione; al contrario, lo studio della direzione nella quale le fonti internazionali operano mitigazioni o espansioni delle prerogative soggettive rivela dati interessanti.

Mentre le limitazioni dei principi nel diritto internazionale, delle quali si è fatto innanzi qualche esempio, operano più propriamente sul piano delle politiche di salvaguardia dell'ordine e della sicurezza pubblica, mediante imposizione di obblighi a parti terze che giocano un ruolo decisivo nel momento informativo, le *espansioni* dei principi ad opera delle stesse fonti sovranazionali mirano oltremodo a rafforzare diritti e garanzie nell'ambito del diritto penale sostanziale e processuale, restando indifferente la natura del reato.

Se attraverso le operazioni di a) attribuzione del *device* (*matching*), b) intrusione nei luoghi digitali della persona, c) scandaglio delle app installate e delle modalità di utilizzo, d) esame della connettività e della navigazione, e) studio dello *storage*

(nel *device*, in unità esterne, utilizzo di NAS e altri supporti, ricorso a *cloud*) si perviene alla dimostrazione della volontarietà dell'azione, l'elaborazione complessiva del percorso probatorio dovrà pur sempre essere sottoposta al vaglio del Giudice terzo nella sede appropriata, dibattuta con metodo dialettico dalle parti, risultare lineare ed univoca nella ricostruzione così da poter determinare l'affermazione di responsabilità in termini di certezza processuale.

Poco senso ha, dunque, la pur suggestiva locuzione definitoria di "prova investigativa": la sostanziale anticipazione nella fase delle indagini dell'acquisizione decisiva per la futura decisione, infatti, discende esclusivamente dalle modalità acquisitive che il legislatore ha disegnato contemperando i principi costituzionali di necessaria acquisizione conservazione delle fonti di prova e di effettività dei diritti difensivi, volgendo inevitabilmente uno sguardo all'evoluzione tecnologica ma ponendo precisi obblighi la violazione dei quali comporta una irrimediabile invalidazione della pretesa punitiva.

V'è piuttosto da prendere atto che la tecnologia non è più considerabile una opzione comportamentale: essa pervade la quotidianità dell'agire umano, impatta direttamente sulle relazioni umane, determina essa stessa comportamenti che non possono più essere considerati straordinari o isolati: nuovi scenari legati alla progressiva evoluzione tecnologica pongono sfide per fronteggiare le quali sono indispensabili attenzione e lungimiranza, ossia l'esatto contrario della scettica indifferenza mostrata in tempi recenti.