Polizia giudiziaria nell’era digitale: tra codice penale e codice binario

La polizia giudiziaria italiana si trova oggi a operare in uno spazio ibrido dove la materialità fisica del reato si dissolve progressivamente in flussi di dati, tracce volatili e infrastrutture *cloud* distribuite su più giurisdizioni. Questa trasformazione non rappresenta semplicemente un’evoluzione degli strumenti investigativi, ma impone una ridefinizione epistemologica del concetto stesso di accertamento del fatto-reato. Quando un attacco *ransomware* paralizza un’infrastruttura critica, quando una frode finanziaria si consuma attraverso *smart contract* anonimi, quando un’operazione di spionaggio industriale avviene tramite *malware* persistente, gli investigatori si confrontano con una criminalità che non lascia impronte digitali nel senso tradizionale, ma genera piuttosto costellazioni di artefatti digitali la cui interpretazione richiede competenze che trascendono la formazione giuridica classica.

L’articolo 55 del Codice di Procedura Penale definisce la polizia giudiziaria come l’insieme degli ufficiali e agenti che svolgono funzioni di prevenzione e repressione dei reati, dovendo prendere notizia dei reati, impedire che vengano portati a conseguenze ulteriori, ricercarne gli autori e compiere gli atti necessari per assicurare le fonti di prova. Questa definizione, cristallizzata in un’epoca in cui il crimine aveva ancora coordinate spaziotemporali definite, oggi si scontra con realtà investigative dove l’autore del reato può trovarsi in una giurisdizione, i server utilizzati in un’altra, i dati compromessi in una terza, e le conseguenze dannose manifestarsi in una quarta. La polizia giudiziaria deve quindi operare simultaneamente su piani giuridici,

tecnici e geopolitici che si intersecano in modi imprevedibili.

L’asimmetria tra velocità dell’attacco e tempi dell’accertamento

Una delle contraddizioni più acute che caratterizza l’attività della polizia giudiziaria in ambito *cyber* riguarda la discrasia temporale tra la rapidità con cui si consumano i crimini informatici e la necessaria ponderazione dell’azione investigativa vincolata al rispetto delle garanzie procedurali. Un attacco DDoS può saturare un’infrastruttura in pochi minuti, un *data breach* può estrarre terabyte di informazioni in ore, ma l’acquisizione probatoria di questi eventi deve seguire protocolli forensi che garantiscano l’integrità della prova, la catena di custodia, l’irripetibilità degli atti quando necessario.

Questa tensione tra urgenza operativa e rigore procedurale non è risolvibile attraverso scorciatoie normative, ma richiede piuttosto una profonda comprensione tecnica che permetta agli investigatori di identificare quali dati sono volatili e quindi da cristallizzare immediatamente, e quali invece possono essere oggetto di successive analisi più approfondite.

La memoria RAM di un sistema compromesso, i *log* temporanei dei *firewall*, le sessioni attive nelle connessioni di rete rappresentano elementi probatori che esistono in una finestra temporale ristretta. La polizia giudiziaria deve quindi sviluppare capacità di *triage* investigativo che permettano di prioritizzare le attività di acquisizione sulla base non solo della rilevanza penale, ma anche della persistenza tecnica delle evidenze digitali. Questo approccio richiede una formazione che integri la conoscenza del diritto processuale penale con competenze sistemistiche profonde su architetture

di rete, sistemi operativi, protocolli di comunicazione e tecniche di *persistence* del *malware*.

Il nodo gordiano della giurisdizione digitale

La dimensione transnazionale del *cybercrime* pone alla polizia giudiziaria sfide che non trovano facile risoluzione nel *framework* normativo tradizionale. La Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001 e ratificata dall'Italia con la legge 18 marzo 2008, n. 48, ha rappresentato il primo tentativo organico di armonizzazione delle norme penali sostanziali e delle procedure investigative in materia di crimini informatici. Tuttavia, l'applicazione pratica di questi strumenti cooperativi si scontra con tempi di risposta alle rogatorie internazionali spesso incompatibili con la volatilità delle prove digitali. Un server utilizzato per un attacco può essere dismesso e riconfigurato in ore, vanificando qualsiasi tentativo di acquisizione probatoria che richieda il passaggio attraverso canali diplomatici tradizionali.

In questo contesto, emergono pratiche investigative ibride che cercano di bilanciare la sovranità territoriale con l'efficacia dell'azione di contrasto. L'accesso transfrontaliero ai dati conservati in *cloud*, la cooperazione diretta tra forze di polizia bypassando parzialmente i canali diplomatici, l'utilizzo di strumenti di *hacking* legale per accedere a sistemi ubicati in altre giurisdizioni rappresentano tutte strategie che sollevano complessi interrogativi di legittimità costituzionale e compatibilità con i diritti fondamentali. La polizia giudiziaria italiana, operando nel perimetro della Procura Europea (EPPO) – divenuta operativa il 1° giugno 2021 – e nel *framework* della cooperazione Europol, deve navigare tra questi strumenti con

consapevolezza dei rischi di invalidità probatoria e delle implicazioni geopolitiche delle proprie azioni.

Digital forensics: quando la tecnica diventa diritto

L'attività di *digital forensics* rappresenta il momento cruciale in cui competenza tecnica e rilevanza giuridica si fondono indissolubilmente. L'acquisizione forense di un sistema informatico non è un'operazione neutra di mera copia di dati, ma un'attività investigativa che deve garantire simultaneamente l'integrità informatica dell'evidenza e la sua utilizzabilità processuale. La metodologia forense richiede la generazione di *hash* crittografici che certifichino l'immodificabilità dei dati acquisiti, la documentazione completa di ogni passaggio della catena di custodia, l'utilizzo di strumenti validati dalla comunità scientifica, la produzione di *report* che siano comprensibili anche a giudici privi di formazione tecnica specifica.

Questa convergenza tra rigore scientifico e utilizzabilità processuale si manifesta in modo particolare nella gestione delle prove informatiche irripetibili. L'articolo 360 del Codice di Procedura Penale prevede che quando gli accertamenti riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, il pubblico ministero avvisa senza ritardo la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici.

Nel contesto digitale, la qualificazione di un'attività come irripetibile diventa questione di estrema delicatezza tecnica. L'accesso a un sistema crittografato potrebbe essere irripetibile se l'autore del reato, avvisato dell'indagine, modificasse le credenziali. L'analisi della memoria volatile di un sistema è per definizione irripetibile. Ma

l’acquisizione di un *hard disk* è irripetibile o può essere oggetto di successive perizie? La risposta dipende dalla comprensione tecnica delle modalità di acquisizione utilizzate e delle garanzie di integrità implementate.

L’intelligenza artificiale come sfida epistemologica

L’ingresso dell’intelligenza artificiale sia come strumento investigativo che come vettore di attacco introduce un ulteriore livello di complessità nell’attività della polizia giudiziaria. L’utilizzo di algoritmi di *machine learning* per l’analisi di grandi volumi di dati sequestrati, per l’identificazione di *pattern* comportamentali sospetti, per la correlazione di informazioni provenienti da fonti eterogenee solleva interrogativi fondamentali sulla spiegabilità delle decisioni investigative. Quando un sistema di AI suggerisce una connessione tra eventi apparentemente non correlati, sulla base di quali parametri la polizia giudiziaria può considerare questa indicazione come elemento indiziario utilizzabile? La «*black box*» algoritmica è compatibile con il principio di verificabilità e contestabilità della prova tipico del processo penale?

Parallelamente, la criminalità organizzata e gli attori di minaccia avanzata (APT) stanno integrando nelle proprie operazioni strumenti di AI generativa per la creazione di *malware* polimorfico, per la produzione di contenuti *deepfake* utilizzati in truffe sofisticate, per l’automazione di attacchi di *social engineering* su larga scala. La polizia giudiziaria deve quindi sviluppare capacità di riconoscimento e analisi di questi artefatti sintetici, comprendendo i limiti tecnici degli attuali strumenti di *detection* e le implicazioni probatorie dell’attribuzione di contenuti generati artificialmente.

La formazione continua come imperativo categorico

La velocità di evoluzione tecnologica impone alla polizia giudiziaria un ripensamento radicale dei modelli di formazione. Non è più sufficiente formare specialisti *cyber* che affiancano gli investigatori tradizionali. È necessario che ogni operatore di polizia giudiziaria possieda una *literacy* digitale di base che gli permetta di riconoscere la rilevanza investigativa di evidenze digitali anche in contesti apparentemente tradizionali. Un'indagine per omicidio può richiedere l'analisi dei metadati di geolocalizzazione degli *smartphone*. Un'indagine per corruzione può necessitare l'esame di *wallet* di criptovalute. Un'indagine per traffico di stupefacenti può coinvolgere l'analisi di comunicazioni su piattaforme crittografate.

Questa formazione non può limitarsi agli aspetti tecnici, ma deve integrare la comprensione delle implicazioni giuridiche delle tecnologie investigative. L'utilizzo di *trojan* di Stato per l'intercettazione di comunicazioni informatiche, disciplinato in Italia dall'articolo 266-bis del Codice di Procedura Penale, richiede agli investigatori la comprensione non solo delle modalità tecniche di *deployment* del captatore informatico, ma anche dei limiti costituzionali di utilizzo di tali strumenti, delle garanzie richieste per la loro attivazione, delle modalità di verbalizzazione delle attività svolte. La formazione deve quindi essere interdisciplinare, coinvolgendo giuristi, informatici, esperti di *intelligence* e accademici in un dialogo costante.

Il bilanciamento tra sicurezza e diritti fondamentali

La polizia giudiziaria opera in una tensione permanente tra l'esigenza di efficacia investigativa e il rispetto dei

diritti fondamentali garantiti dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione Europea. Nel contesto digitale, questa tensione assume connotazioni particolarmente acute. La *data retention*, la conservazione generalizzata dei dati di traffico telefonico e telematico per finalità investigative, è stata oggetto di ripetute censure da parte della Corte di Giustizia dell'Unione Europea che, con sentenze del 2014, del 2020 e del 2022, ha ritenuto tale pratica – quando generalizzata e indiscriminata – incompatibile con i principi di proporzionalità e necessità. Eppure, l'accesso ai tabulati telefonici e ai *log* di connessione rappresenta spesso l'unico strumento investigativo efficace per ricostruire la dinamica di crimini informatici complessi.

La cifratura *end-to-end* delle comunicazioni, sempre più diffusa nelle piattaforme di messaggistica, pone interrogativi sulla sostenibilità del modello investigativo tradizionale basato sull'intercettazione. Le proposte normative che ipotizzano l'introduzione di *backdoor* crittografiche per consentire l'accesso *lawful* alle comunicazioni cifrate vengono contestate dalla comunità scientifica come intrinsecamente insicure e suscettibili di abuso. La polizia giudiziaria si trova quindi a dover operare in un ecosistema digitale dove ampie porzioni di comunicazioni e transazioni sono tecnicamente inaccessibili, richiedendo lo sviluppo di strategie investigative alternative basate sull'analisi dei metadati, sull'infiltrazione sotto copertura, sull'utilizzo di fonti umane.

Prospettive: verso una polizia giudiziaria 5.0

L'evoluzione della polizia giudiziaria nell'era digitale non può essere concepita come un semplice aggiornamento tecnologico dell'apparato investigativo esistente, ma richiede

una trasformazione culturale e organizzativa profonda. La specializzazione settoriale, che ha caratterizzato storicamente l'organizzazione delle forze di polizia, deve essere integrata da capacità trasversali di comprensione dei fenomeni tecnologici che permeano ogni tipologia di reato. Le sezioni di polizia giudiziaria specializzate in crimini informatici non possono più essere percepite come reparti specialistici separati, ma devono diventare *hub* di competenza che irradiano conoscenza e supporto a tutte le articolazioni investigative.

La cooperazione pubblico-privato diventa elemento strategico irrinunciabile. Le infrastrutture digitali critiche sono prevalentemente gestite da operatori privati, i fornitori di servizi *cloud* detengono dati essenziali per le indagini, le aziende di *cybersecurity* producono *intelligence* sulle minacce che può essere cruciale per le attività investigative. La polizia giudiziaria deve quindi sviluppare protocolli di collaborazione che garantiscano la tempestività dell'accesso alle informazioni rispettando i vincoli di riservatezza investigativa e i limiti normativi alla condivisione di dati personali.

La dimensione predittiva e preventiva acquista rilevanza crescente. L'analisi di *big data* provenienti da fonti aperte, il monitoraggio di indicatori di compromissione nelle reti, l'*intelligence* su gruppi criminali emergenti permettono alla polizia giudiziaria di anticipare fenomeni criminali prima che producano danni irreparabili. Questo *shift* da un modello puramente reattivo a uno proattivo solleva ulteriori questioni etiche e giuridiche sulla legittimità di interventi basati su probabilità statistiche piuttosto che su fatti-reato già consumati.

Conclusioni: il diritto alla prova

nell’era dell’immaterialità

La sfida fondamentale che la polizia giudiziaria deve affrontare nell’era digitale riguarda la preservazione del diritto alla prova in un ecosistema tecnologico sempre più complesso, distribuito e inaccessibile. La *legitimacy* del sistema penale si fonda sulla possibilità di accertare i fatti attraverso un contraddittorio probatorio dove accusa e difesa possano confrontarsi su evidenze verificabili e contestabili. Quando le prove diventano artefatti digitali la cui interpretazione richiede competenze specialistiche raramente disponibili anche nelle difese tecnicamente attrezzate, quando le tecniche investigative si basano su strumenti proprietari non verificabili indipendentemente, quando le decisioni algoritmiche influenzano le direzioni investigative senza essere pienamente comprensibili, il rischio è quello di un’erosione della parità delle armi processuali.

La polizia giudiziaria ha quindi la responsabilità non solo di sviluppare efficaci capacità investigative tecnologiche, ma anche di garantire che queste capacità siano esercitate in modo trasparente, verificabile, sottoposto a controllo giurisdizionale effettivo. La documentazione completa delle metodologie utilizzate, la validazione scientifica degli strumenti forensi, la formazione dei magistrati sui limiti e le potenzialità delle prove digitali, la disponibilità di perizie difensive realmente contrapponibili non sono accessori tecnici ma garanzie costituzionali essenziali. Solo preservando questi equilibri la polizia giudiziaria può continuare a svolgere la sua funzione di accertamento della verità processuale in un mondo dove la materialità fisica del crimine è sempre più un’eccezione che una regola.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/polizia-giudiziaria/