

Le procure distrettuali per i reati informatici: l'architettura investigativa italiana nel contrasto al cybercrime



Mentre il dibattito teorico sui diritti fondamentali e sulle garanzie processuali nell'era digitale continua a impegnare giuristi e costituzionalisti, nelle aule delle Procure Distrettuali italiane si consuma quotidianamente la traduzione pratica di quei principi in azione investigativa concreta. I 26 distretti di Corte d'Appello italiani (più 3 sezioni distaccate a Bolzano, Sassari e Taranto), individuati dall'articolo 11 della legge 48/2008, rappresentano l'ossatura del sistema italiano di contrasto alla criminalità informatica, un'architettura organizzativa che ricalca il modello già consolidato per i reati di terrorismo e criminalità organizzata ma che deve confrontarsi con sfide investigative di natura radicalmente diversa.

La scelta legislativa di concentrare a livello distrettuale la competenza sui reati informatici – introducendo il comma 3-quinquies dell'articolo 51 del Codice di Procedura Penale – nasce da una consapevolezza: il cybercrime non conosce confini territoriali e richiede una specializzazione investigativa che non può essere frammentata su base provinciale.

Un attacco ransomware contro un ospedale lombardo può essere orchestrato da un gruppo criminale con base in Estonia, utilizzando server compromessi in Asia e infrastrutture di pagamento in criptovalute registrate in paradisi fiscali caraibici. La Procura territorialmente competente per il luogo

in cui si è verificato l'evento criminoso deve poter disporre di competenze tecniche e reti investigative che trascendono la dimensione locale, ed è proprio questa capacità di coordinamento sovraprovinciale che giustifica la competenza distrettuale.

La genesi normativa: dalla Convenzione di Budapest all'articolo 51 comma 3-quinquies CPP

L'introduzione della competenza distrettuale per i reati informatici non è stata immediata né priva di difficoltà applicative. La legge 18 marzo 2008, n. 48, nel ratificare la Convenzione di Budapest (approvata il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004), ha modificato l'assetto procedurale italiano con una tecnica legislativa che inizialmente ha generato incertezze interpretative. L'articolo 11 della legge 48/2008 ha introdotto il comma 3-quinquies all'articolo 51 CPP, attribuendo al pubblico ministero presso il tribunale del capoluogo del distretto di Corte d'Appello la competenza per i procedimenti relativi ai delitti commessi mediante l'impiego di tecnologie informatiche o telematiche.

La norma, entrata in vigore il 5 aprile 2008, tuttavia non aveva inizialmente previsto il simmetrico adeguamento della competenza del Giudice per le Indagini Preliminari, generando un'asimmetria procedurale che la Corte di Cassazione ha dovuto risolvere attraverso un'interpretazione costituzionalmente orientata. Solo con la legge n. 125 del 24 luglio 2008, attraverso l'inserimento del comma 1-quater all'articolo 328 CPP, si è completato il quadro normativo, attribuendo anche al GIP distrettuale la competenza sugli atti relativi alle indagini preliminari per i reati informatici.

Questa vicenda normativa evidenzia un problema ricorrente

nella legislazione italiana in materia di cybercrime: l'urgenza di adeguare l'ordinamento a fenomeni criminali in rapida evoluzione si scontra spesso con la necessità di garantire la coerenza sistematica del Codice di Procedura Penale. Il risultato sono interventi legislativi stratificati, emendamenti a emendamenti, disposizioni transitorie che rendono complessa l'attività interpretativa e applicativa da parte degli operatori del diritto.

L'operatività delle Procure Distrettuali: tra specializzazione e frammentazione

Le Procure Distrettuali competenti per i reati informatici, presenti nei 26 capoluoghi di distretto di Corte d'Appello più le 3 sezioni distaccate, operano con livelli di specializzazione e dotazioni tecniche estremamente eterogenei. Le Procure di Milano, Roma, Napoli e Torino hanno sviluppato nel tempo pool di magistrati dedicati esclusivamente alla criminalità informatica, con competenze tecniche raffinate e rapporti consolidati con la Polizia Postale e delle Comunicazioni. Altre Procure Distrettuali, invece, affrontano i procedimenti per reati informatici all'interno dei tradizionali gruppi di lavoro, con magistrati che alternano indagini cyber a procedimenti di natura tradizionale.

Questa disomogeneità non è solo questione di organizzazione interna ma riflette anche la diversa incidenza territoriale del fenomeno criminale. Le grandi aree metropolitane, con la concentrazione di infrastrutture digitali, data center, provider di servizi cloud e imprese tecnologiche, sono naturalmente epicentri di criminalità informatica. Una frode informatica perpetrata attraverso un server ubicato a Milano genererà competenza della Procura Distrettuale milanese, indipendentemente dal luogo di residenza delle vittime o degli autori del reato. Questo criterio di collegamento territoriale

– basato sul luogo in cui si trova il sistema informatico attraverso cui il reato è stato commesso – genera una concentrazione di procedimenti presso alcune Procure Distrettuali, amplificando le disparità di carico di lavoro e di specializzazione.

La Polizia Postale e delle Comunicazioni, istituita nella forma attuale con decreto del ministero dell'Interno del 31 marzo 1998, con i suoi 18 Centri Operativi per la Sicurezza Cibernetica (COSC) distribuiti nei principali capoluoghi di regione e le 82 Sezioni Operative per la Sicurezza Cibernetica (SOSC), rappresenta il braccio operativo naturale delle Procure Distrettuali.

La specialità della Polizia di Stato, posta oggi alle dipendenze della Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica (divenuta operativa nel febbraio 2024), dispone di competenze tecniche avanzate in digital forensics, analisi di malware, tracciamento di transazioni in criptovalute, penetrazione di reti anonime. Il rapporto tra magistrati inquirenti e investigatori della Polizia Postale non è semplicemente di delega esecutiva, ma si configura come una collaborazione sinergica in cui la comprensione tecnica del fenomeno criminale informa le scelte strategiche dell'indagine, mentre la direzione giuridica garantisce la conformità procedurale e la utilizzabilità probatoria delle attività investigative.

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC)

All'interno della Polizia Postale opera una struttura di particolare rilevanza strategica: il CNAIPIC, incaricato in via esclusiva della prevenzione e repressione dei crimini informatici che hanno per obiettivo le infrastrutture

informatizzate di natura critica e di rilevanza nazionale. Il Centro opera attraverso tre direttrici principali: intelligence per la raccolta dati e informazioni utili alla prevenzione, attraverso monitoraggio costante della rete e rapporti di collaborazione con organismi di polizia nazionali e internazionali; analisi per l'approfondimento comparativo dei dati raccolti e la predisposizione di rapporti previsionali sull'evoluzione della minaccia; risposta investigativa al verificarsi di eventi criminali in danno delle infrastrutture critiche, avvalendosi della rete territoriale dei Centri Operativi e delle Sezioni Operative della Polizia Postale.

Il CNAIPIC mantiene un punto di contatto operativo 24/7 dedicato all'interscambio informativo con i gestori delle infrastrutture critiche, costituendo un anello di congiunzione tra la dimensione preventiva – di competenza dell'Agenzia per la Cybersicurezza Nazionale (ACN) – e quella repressiva di competenza giudiziaria. Quando un attacco informatico colpisce un'infrastruttura critica, la tempestività della risposta è cruciale non solo per mitigare i danni immediati ma anche per cristallizzare le prove digitali prima che l'attaccante possa cancellare le proprie tracce o che la volatilità intrinseca dei dati ne determini la perdita. In questi scenari, il CNAIPIC opera in stretto coordinamento con le Procure Distrettuali competenti, fornendo supporto tecnico immediato e garantendo la corretta acquisizione forense delle evidenze.

La sinergia pubblico-privato: ACN, CSIRT Italia e l'ecosistema della cybersecurity

L'efficacia dell'azione delle Procure Distrettuali nel contrasto al cybercrime dipende in misura crescente dalla capacità di integrare la dimensione repressiva con quella preventiva e di collaborare con gli attori del settore privato

che gestiscono le infrastrutture digitali del Paese. L'Agenzia per la Cybersicurezza Nazionale, istituita con decreto-legge n. 82 del 14 giugno 2021 e divenuta operativa nello stesso anno, rappresenta l'autorità nazionale con compiti di prevenzione, monitoraggio e coordinamento in materia di sicurezza cibernetica.

All'interno dell'ACN opera il CSIRT Italia (Computer Security Incident Response Team), la squadra nazionale di risposta agli incidenti informatici che monitora costantemente le minacce cyber, emette alert e bollettini di sicurezza, coordina la gestione tecnica degli incidenti che coinvolgono soggetti pubblici e privati. Il CSIRT Italia, trasferito il 16 settembre 2021 dal Dipartimento Informazioni per la Sicurezza alla neonata ACN, costituisce un ponte essenziale tra la dimensione tecnica della sicurezza informatica e quella giuridico-investigativa.

Quando un'azienda subisce un attacco informatico, la prima segnalazione avviene spesso al CSIRT, che fornisce supporto tecnico immediato per il contenimento e la remediation. Parallelamente, se l'evento costituisce reato, il CSIRT facilita il raccordo con la Polizia Postale e la Procura Distrettuale competente, garantendo che le attività di ripristino dei sistemi non compromettano l'integrità delle prove digitali necessarie per l'azione penale.

Questa collaborazione pubblico-privato solleva delicati interrogativi sulla condivisione delle informazioni e sulla tutela dei segreti aziendali. Le imprese che subiscono attacchi informatici sono spesso riluttanti a denunciare l'accaduto per timore di danni reputazionali, perdita di fiducia da parte dei clienti, sanzioni da parte delle autorità di vigilanza per inadeguatezza delle misure di sicurezza.

La normativa sulla data retention, le direttive europee NIS e NIS2 sulla sicurezza delle reti e dei sistemi informativi, il GDPR con i suoi obblighi di notifica dei data breach, hanno

progressivamente ridotto gli spazi di discrezionalità delle imprese, rendendo obbligatoria la segnalazione di determinate tipologie di incidenti. Tuttavia, la frontiera tra obbligo di segnalazione e volontaria collaborazione investigativa rimane sfumata, e le Procure Distrettuali devono spesso bilanciare l'esigenza di acquisire tempestivamente informazioni con la necessità di non compromettere i rapporti fiduciari con il settore privato.

Le sfide operative: carenze di organico, obsolescenza tecnologica, tempi processuali

Nonostante l'avanzamento normativo e l'istituzione di strutture specializzate, le Procure Distrettuali per i reati informatici affrontano sfide operative di straordinaria complessità. La carenza di magistrati specializzati è un problema strutturale: formare un pubblico ministero competente in materia di criminalità informatica richiede anni di esperienza sul campo, aggiornamento tecnico continuo, capacità di dialogare con consulenti tecnici e periti forensi. Il turnover dei magistrati, determinato dalla progressione di carriera e dai trasferimenti, rende difficile consolidare competenze di pool che richiederebbero continuità pluriennale.

Sul versante delle dotazioni tecnologiche, molte Procure Distrettuali operano con strumenti informatici che appaiono anacronistici se confrontati con le tecnologie utilizzate dalla criminalità. I laboratori di digital forensics richiedono investimenti significativi in hardware e software specializzati, formazione del personale tecnico, aggiornamento costante per fronteggiare l'evoluzione delle tecniche di occultamento delle prove. Le sale server delle Procure, quando esistono, spesso non dispongono degli standard di sicurezza che sarebbero richiesti per la custodia di prove digitali relative a reati di particolare gravità. Il rischio di

compromissione dei dati acquisiti, sia per inadeguatezza delle misure di protezione sia per errori nella gestione della catena di custodia, è una preoccupazione costante.

I tempi processuali rappresentano un'ulteriore criticità. Un'indagine per criminalità informatica può richiedere mesi o anni per essere completata: l'identificazione degli autori attraverso l'analisi dei log di connessione, l'ottenimento di rogatorie internazionali per l'acquisizione di dati conservati all'estero, la decrittazione di comunicazioni cifrate, l'analisi forense di dispositivi sequestrati contenenti terabyte di dati. Nel frattempo, gli strumenti utilizzati per commettere il reato evolvono, le piattaforme criminali si spostano, gli autori cambiano identità digitale. Quando un procedimento giunge finalmente a dibattimento, non è raro che le tecnologie oggetto dell'indagine siano ormai obsolete e che le dinamiche del mercato criminale si siano completamente trasformate.

Il coordinamento tra Procure: la Procura Nazionale Antimafia e Antiterrorismo

La frammentazione territoriale delle competenze, pur mitigata dalla concentrazione distrettuale, può generare problemi di coordinamento quando un'organizzazione criminale opera attraverso cellule dislocate in più distretti o quando una piattaforma criminale online serve utenti su tutto il territorio nazionale. La Direzione Nazionale Antimafia e Antiterrorismo (DNA), tradizionalmente competente per il coordinamento delle indagini su criminalità organizzata e terrorismo, ha progressivamente esteso il proprio raggio d'azione anche a fenomeni di cybercrime organizzato, in particolare quando questi si intersecano con attività di riciclaggio, traffico di stupefacenti, estorsioni tramite ransomware.

Recenti proposte legislative hanno ipotizzato l'ampliamento ulteriore della competenza delle Direzioni Distrettuali Antimafia ai reati di estorsione informatica, riconoscendo che i gruppi criminali che operano attacchi ransomware presentano caratteristiche organizzative e capacità offensive comparabili a quelle della criminalità organizzata tradizionale. Questa evoluzione segna un cambiamento di paradigma: il cybercrime non è più percepito come una categoria criminale a sé stante, tecnicamente complessa ma sostanzialmente diversa dalla criminalità "fisica", ma come una delle molteplici manifestazioni dell'azione di gruppi criminali che utilizzano indifferentemente strumenti digitali e tradizionali per perseguire i propri obiettivi di profitto illecito.

Casi paradigmatici: dall'indagine al dibattito

L'esperienza operativa delle Procure Distrettuali offre una casistica ricchissima di indagini che hanno fatto scuola, stabilendo precedenti giurisprudenziali e affinando metodologie investigative. Le operazioni contro i marketplace del darknet – piattaforme anonime dove si commerciano droghe, armi, documenti falsi, dati rubati – hanno richiesto tecniche investigative ibride: infiltrazioni sotto copertura negli ambienti criminali digitali, analisi del blockchain per tracciare i flussi finanziari in criptovalute, collaborazione con agenzie internazionali per smantellare simultaneamente i server in più giurisdizioni.

Gli attacchi ransomware contro ospedali e pubbliche amministrazioni hanno posto problemi etici oltre che investigativi: quando un ospedale vede paralizzati i propri sistemi informatici con conseguente impossibilità di accedere alle cartelle cliniche dei pazienti, la priorità immediata è il ripristino dei servizi essenziali, anche a costo di pagare il riscatto. Le Procure Distrettuali si sono trovate a dover

bilanciare l'esigenza investigativa di non compromettere le prove con la necessità di salvaguardare vite umane, sviluppando protocolli di intervento che distinguono tra acquisizione forense immediata di elementi volatili e analisi approfondita differita a quando l'emergenza sanitaria è superata.

Le frodi informatiche transnazionali, dalle truffe mediante phishing bancario alle frodi nelle piattaforme di e-commerce, hanno evidenziato i limiti degli strumenti investigativi tradizionali quando gli autori operano dall'estero e i server utilizzati si trovano in giurisdizioni non cooperative. In questi casi, l'unica via percorribile è spesso la collaborazione con i gestori privati delle piattaforme (provider di servizi email, social network, sistemi di pagamento) che, pur non essendo obbligati a collaborare con autorità giudiziarie straniere, possono volontariamente fornire informazioni o disattivare account utilizzati per attività criminali.

L'integrazione con il sistema EPP0: competenze concorrenti e coordinamento europeo

L'operatività della Procura Europea (EPP0) dal 1° giugno 2021 ha introdotto un ulteriore livello di complessità nel panorama delle competenze investigative. I reati informatici che ledono gli interessi finanziari dell'Unione Europea – frodi ai danni dei fondi comunitari commesse attraverso piattaforme digitali, manipolazione di sistemi informatici per ottenere indebiti finanziamenti europei – rientrano nella competenza dell'EPP0 e vengono gestiti dai Procuratori Europei Delegati (PED) operanti in Italia.

La competenza concorrente tra Procure Distrettuali nazionali ed EPP0 richiede meccanismi di coordinamento per evitare

duplicazioni investigative o, peggio, interferenze reciproche. I protocolli di collaborazione prevedono che, quando un reato presenta profili di competenza sia nazionale sia europea, le autorità inquirenti si consultino per definire quale sia il forum più appropriato per condurre l'indagine. In questo contesto, le Procure Distrettuali italiane portano la propria esperienza consolidata nel contrasto al cybercrime, mentre l'EPP0 offre strumenti di cooperazione giudiziaria semplificati e accesso diretto a informazioni detenute da autorità di altri Stati membri.

Prospettive di riforma: verso una Procura Nazionale Cyber?

Il dibattito sulla riorganizzazione del sistema delle Procure Distrettuali per i reati informatici si articola su due direttrici principali. Da un lato, vi è chi propugna un'ulteriore concentrazione delle competenze, ipotizzando l'istituzione di una Procura Nazionale Cyber sul modello della Direzione Nazionale Antimafia, che coordini le indagini più complesse e garantisca uniformità di approccio investigativo su tutto il territorio nazionale. Questa proposta si scontra con la resistenza di chi teme un'eccessiva centralizzazione che priverebbe le realtà territoriali della capacità di rispondere tempestivamente a fenomeni criminali locali e che rischierebbe di congestionare un'unica struttura con competenza su una materia – la criminalità informatica – che per vastità e articolazione non è comparabile alle fattispecie tradizionalmente gestite dalle Procure nazionali.

Dall'altro lato, vi è chi sostiene la necessità di un potenziamento delle Procure Distrettuali esistenti piuttosto che la creazione di nuove strutture: incremento degli organici con magistrati specializzati, investimenti significativi in dotazioni tecnologiche, formazione continua obbligatoria non solo per i magistrati ma per tutto il personale amministrativo

e tecnico che opera nelle Procure. Questa visione privilegia un modello distribuito ma fortemente interconnesso, dove ogni Procura Distrettuale dispone delle competenze essenziali ma può attivare rapidamente meccanismi di mutuo supporto quando affronta indagini che eccedono le proprie capacità.

La verità probabilmente risiede in una sintesi: mantenere la competenza distrettuale come livello ordinario di gestione delle indagini per reati informatici, rafforzandola significativamente in termini di risorse umane e tecnologiche; istituire un centro di coordinamento nazionale – non necessariamente con funzioni inquirenti dirette – che funga da hub per lo scambio di best practices, la gestione di banche dati investigative condivise, il coordinamento di indagini multi-distrettuali, la formazione specialistica; sviluppare protocolli standardizzati per l'acquisizione e l'analisi forense che garantiscano uniformità metodologica pur nel rispetto delle specificità territoriali.

Conclusioni: l'equilibrio tra specializzazione tecnica e garanzie processuali

Le Procure Distrettuali per i reati informatici incarnano una delle sfide più complesse del diritto processuale penale contemporaneo: conciliare l'esigenza di un'altissima specializzazione tecnica con la necessaria salvaguardia delle garanzie procedurali che costituiscono il fondamento dello Stato di diritto. Un magistrato che indaga su un attacco informatico deve possedere competenze che spaziano dall'informatica forense alla crittografia, dalla comprensione delle architetture cloud all'analisi delle transazioni blockchain, ma deve al contempo rimanere saldamente ancorato ai principi del giusto processo, alla presunzione di innocenza, al diritto di difesa.

L'architettura investigativa italiana, con i suoi 26 distretti di Corte d'Appello (più 3 sezioni distaccate), la Polizia Postale, il CNAIPIC, la sinergia con ACN e CSIRT Italia, rappresenta un sistema in continua evoluzione, che deve costantemente adattarsi a un panorama criminale caratterizzato da un'innovazione tecnologica vorticoso. Gli autori di reati informatici sviluppano nuove tecniche di attacco, sfruttano vulnerabilità appena scoperte, si spostano verso piattaforme emergenti con una velocità che rende ogni procedura investigativa potenzialmente obsoleta prima ancora di essere stata pienamente implementata.

In questo contesto di perenne mutamento, ciò che deve rimanere costante è l'impegno a garantire che l'efficacia investigativa non sia perseguita a scapito della legalità processuale. Le prove digitali, per quanto tecnicamente inoppugnabili, devono essere acquisite nel rispetto delle norme sulla perquisizione e sul sequestro; le intercettazioni mediante captatori informatici devono sottostare a limiti costituzionali stringenti; l'accesso a dati conservati all'estero deve passare attraverso gli strumenti di cooperazione giudiziaria internazionale. Solo preservando questo equilibrio – difficile, precario, sempre da riconquistare – le Procure Distrettuali possono assolvere alla loro funzione di tutela della legalità nel cyberspazio senza tradire i principi fondamentali del processo penale democratico.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/procure-distrettuali/>