L'INTERVISTA / SERDAR GÜNAL RÜTSCHE / responsabile NEDIK

«Contro la criminalità informatica il Codice penale è da aggiornare»

Paolo Gianinazzi

Quasi 60 mila episodi segnalati in un solo anno, ossia in media oltre 160 ogni singolo giorno. In Svizzera, nel 2024, la criminalità informatica ha toccato nuovi record (+34,7% rispetto al 2023). Facciamo il punto della situazione con il responsabile della Rete nazionale per il supporto investigativo digitale nella criminalità informatica (NEDIK), l'ente che coordina l'attività delle forze di polizia svizzere nella lotta al cibercrimine.

Secondo l'esperto è «insostenibile» che il Codice di procedura penale non menzioni nemmeno il concetto di dati. © SHUTTERSTOCK

La criminalità digitale è in forte crescita in tutto il mondo. In Svizzera stiamo vincendo o perdendo questa «battaglia»?
«Da un punto di vista di polizia, non sarebbe corretto parlare di una "vittoria" o di una "sconfitta" definitiva. Si tratta, piuttosto, di una tipologia di minacce dinamica, che cambia costantemente a causa del rapido progresso tecnologico. Per affrontare con efficacia questi sviluppi, i corpi di polizia investono continuamente nella formazione specializzata di agenti e promuovono la collaborazione nazionale con altre autorità e con istituzioni scientifiche».

Per sua natura la cibercriminalità non conosce confini. I criminali, infatti, spesso si trovano all'estero. Come funziona la collaborazione internazionale su questo fronte?
«La lotta alla criminalità informatica presuppone una stretta cooperazione transfrontaliera. I corpi di polizia svizzeri sono coinvolti nella cooperazione internazionale sia attraverso accordi multilaterali - in particolare la Convenzione di Budapest sulla criminalità informatica - sia tramite trattati bilaterali di assistenza giudiziaria. Allo stesso tempo, la coordinazione nazionale con altre autorità e istituzioni partner funziona molto bene e contribuisce in modo significativo all'efficienza delle indagini. Oggi, tuttavia, mancano ancora le basi legali nazionali per uno scambio di informazioni e di dati di polizia tra i Cantoni. E ciò complica notevolmente il lavoro investigativo e rallenta la capacità di reazione in un contesto dinamico e guidato dalla tecnologia».

> **Le criptovalute** svolgono un ruolo sempre più centrale grazie alle loro caratteristiche attraenti per i criminali

6133

Nel nostro Paese, dal vostro osservatorio quali sono i fenomeni più preoccupanti in merito alla criminalità digitale?
«Dal punto di vista della polizia emergono attualmente due fenomeni principali: le truffe sugli investimenti online (tramite le quali i truffatori si spacciano per fornitori di servizi finanziari innovativi con rendimenti irrealistici, ndr) e i ransomware (un tipo di virus che cripta i dati di un utente o un dispositivo, rendendoli inaccessibili, per poi richiedere un riscatto, ndr). Le truffe sugli investimenti online causano ogni settimana danni per circa cinque milioni di franchi svizzeri, con notevoli perdite patrimoniali per le vittime. Gli attacchi ransomware, invece, mettono gravemente a rischio la reputazione delle aziende con sede in Svizzera e comportano regolarmente oneri finanziari considerevoli. Ciò dimostra che la criminalità informatica non rappresenta soltanto una sfida penale. Essa ha anche una dimensione economica e di politica della piazza finanziaria che richiede una risposta coordinata da parte di giustizia, economia e mondo accademico».

Che ruolo giocano le criptovalute in questo contesto?
«Svolgono un ruolo sempre più centrale. Il loro utilizzo può avvenire in gran parte in modo anonimo e in molti ordinamenti giuridici non sono soggette ad alcuna o a pochissima regolamentazione. Queste caratteristiche le rendono particolarmente attraenti per i criminali. Inoltre, alcune piattaforme di scambio di criptovalute hanno sede in Stati con condizioni poco favorevoli alla cooperazione giudiziaria, restando così praticamente inaccessibili per le autorità svizzere. Le transazioni avvengono senza ritardi temporali e possono essere rapidamente offuscate o rese anonime tramite procedure tecniche. Ciononostante, i criminali non devono illudersi di trovarsi in un "porto sicuro": la polizia si è attrezzata negli ultimi anni e dispone delle risorse tecniche e del know-how necessario per analizzare questi flussi finanziari e identificare i responsabili in stretta collaborazione internazionale».

Qual è l'identikit generale dei cibercriminali? Si tratta più che altro di «lupi solitari» oppure di vere e proprie «bande» organizzate?
«Le manifestazioni della criminalità informatica sono molteplici e possono essere suddivise in due principali categorie. Da un lato vi è una criminalità attiva dalla Svizzera, spesso costituita da singoli individui che operano con mezzi tecnici relativamente limitati, ma possono comunque causare notevoli danni con attacchi mirati quali phishing, frodi o estorsioni a livello locale. Dall'altro lato esistono strutture criminali professionalizzate, spesso transnazionali, caratterizzate da una suddivisione del lavoro, servizi istituzionalizzati e ampie risorse. Gruppi che hanno spesso sede all'estero e sfruttano strategicamente la loro dimensione internazionale. Una caratteristica evidente della situazione attuale è la crescente commercializzazione di servizi criminali, nota come "Cybercrime as a Service", che abbassa sensibilmente le barriere di accesso alla delinquenza. Attraverso questi servizi è infatti possibile acquistare o noleggiare attacchi DDoS (un attacco informatico volto a rendere un servizio - come un sito web o un server - inaccessibile, ndr) o interi processi operativi supportati da call center. Tutto ciò a condizioni relativamente convenienti. I criminali possono così agire senza possedere tutte le competenze necessarie. Questo sviluppo rende più difficile individuare le responsabilità e allo stesso tempo rafforza il fenomeno della criminalità transfrontaliera basata sulla divisione del lavoro».

Come affrontare questo duplice fenomeno?
«L'azione penale deve concentrarsi sia sui singoli autori attivi in Svizzera, sia sulle strutture organizzate spesso situate all'estero. Per gestire efficacemente queste sfide è necessaria con urgenza una modernizzazione del Codice di procedura penale svizzero. In particolare, la gestione dei dati nel contesto internazionale deve essere rinnovata e adattata. Nell'era dell'intelligenza artificiale è insostenibile che l'attuale Codice di procedura penale non menzioni nemmeno il concetto di dati».

Tre parole chiave: «Collaborazione, prevenzione e repressione»

SINERGIE / Il presidente della Conferenza dei comandanti delle polizie cantonali, Matteo Cocchi, sul cibercrimine: «Non si può lavorare ognuno chiuso nel proprio Cantone»

«Ce ne siamo accorti tutti: il fenomeno della criminalità digitale è in costante aumento e non è destinato a fermarsi. E uno dei tasselli fondamentali per contrastare questo tipo di crimini è la collaborazione». Sì, perché «contro questi fenomeni non si può certo lavorare ognuno "chiuso" nel proprio Cantone». A parlare è il comandante della Polizia cantonale ticinese, Matteo Cocchi, che dallo scorso 25 ottobre - e per un periodo di tre anni - è anche presidente della Conferenza dei comandanti e delle comandanti delle polizie cantonali svizzere (CCPCS). Nel suo duplice ruolo, va da sé, vive dunque ogni giorno l'importanza della collaborazione tra i vari Corpi di polizia. Collaborazione che, come detto, è semplicemente imprescindibile quando si tratta di fronteggiare il cibercrimine. «Un caso scoperto in Ticino, ad esempio, potrebbe essere risolto in Canton Vaud, oppure a Sciaffusa. E viceversa. La collaborazione, il mettersi in rete e scambiarsi le esperienze, è quindi fondamentale», afferma a tal proposito Cocchi. E lo stesso principio, ovviamente, vale anche sul piano internazionale. «Una truffa che colpisce un cittadino elvetico, ad esempio, potrebbe portare all'arresto in un'altra nazione». Motivo per cui, per «unire le forze», già anni fa «abbiamo deciso di creare il NEDIK. Una struttura gestita dalla Polizia cantonale di Zurigo, ma che fornisce supporto e mette in rete tutto il lavoro svolto in Svizzera contro la criminalità informatica», prosegue il comandante.

> **È importante** che cittadini o imprese colpiti da un attacco si facciano avanti

Oltre alla collaborazione, poi, occorrono solide competenze, soprattutto in ottica di repressione. E in questo senso non si può prescindere dall'aiuto dei tecnici specializzati. «Per i reati informatici - evidenzia Cocchi - non serve unicamente l'esperienza del "classico" poliziotto. Occorrono anche collaboratori tecnici e informatici, che portano importanti competenze». Oltre a ciò «in futuro, ed è una priorità della Conferenza, si dovrà agevolare anche da un punto di vista legale lo scambio di informazioni tra le varie Polizie cantonali. Soprattutto in un mondo digitale che non conosce confini e si sviluppa rapidamente».

«Fatevi avanti»
C'è poi un altro aspetto che Cocchi tiene a sottolineare: l'importanza di farsi avanti, di non nascondersi quando si subisce (o si sospetta di aver subito) una truffa informatica. «Occorre capire che i tentativi di truffa sono tantissimi. E su mille tentativi è sufficiente che uno vada in porto per fare danni rilevanti. È dunque importante che il cittadino o l'impresa che incappa in un problema si faccia avanti, segnalando l'accaduto». Le segnalazioni, infatti, sono utili anche in ottica di prevenzione: «Quando riceviamo 50 segnalazioni per lo stesso problema, magari in diversi cantoni, ciò può trasformarsi in un annuncio preventivo per tutta la popolazione». I canali per denunciare e segnalare episodi simili sono quelli «classici», ossia il numero della Polizia (117). Ma, oltre a ciò, anche sul sito cybercrimepolice.ch è possibile segnalare crimini informatici. Un sito attualmente disponibile in tedesco e francese che però, assicura Cocchi nella sua veste di ticinese alla guida della CCPCS, «mi sono impegnato a rendere disponibile in futuro anche in italiano».

E il Ticino - chiediamo infine al comandante - come è messo nella lotta alla criminalità digitale? «Da alcuni anni abbiamo creato e rafforzato un settore specifico, il reparto giudiziario 4, con la Sezione analisi tracce informatiche (SATI), all'interno della quale lavorano inquirenti e collaboratori tecnici. Siamo dunque ben messi in Ticino, con una squadra che può dare il suo contributo anche nel resto della Svizzera: come dicevo, non possiamo prescindere dal collaborare con gli altri Cantoni. È nell'interesse di tutti».