Fondazione Bruno Visentini

SULLA CYBERSICUREZZA MEGLIO L'INTELLIGENCE CHE LE SANZIONI PIÙ SEVERE

di **Andrea R. Castaldo**

Nihil novi sub sole. Il disegno di legge cybersecurity, approvato la scorsa settimana dal Consiglio dei ministri, conferma l'attenzione crescente e la consapevolezza dei rischi che si nascondono dietro la criminalità informatica. Una macrocategoria, convenzionalmente racchiusa sotto l'insegna aggregante dei computer crimes, in realtà aperta a ventaglio in svariate e diverse fattispecie delittuose. Caratteristica che rende più difficile aggredirla, in virtù delle strategie di repressione da differenziare.

Ma andiamo per ordine. Negli ultimi due anni molteplici sono state le novità in tema di sicurezza cibernetica, compresa tra i progetti finanziati dal Pnrr. Tra le disposizioni urgenti in materia di processo penale, figura l'articolo 2-bis del Dl 105/2023 (convertito con modificazioni dalla legge 137/2023), che si prefigge l'obiettivo di innalzare i livelli di cybersicurezza e di implementare gli strumenti di repressione dei crimini informatici, estendendo le misure di contrasto a oggi ristrette alla criminalità organizzata e al terrorismo.

Particolarmente interessanti le norme volte a espandere l'area delle operazioni *under cover* (con annesse prerogative) per il contrasto del cybercrime.

Il percorso tracciato viene ripreso e consolidato con il Ddl di questi giorni, le cui linee portanti si riassumono – in buona sostanza – nella consueta politica dello *stick and carrot*. Miscela divenuta costante nella risposta a fenomenologie criminali nuove o preesistenti mutate geneticamente. E allora, sul versante repressivo, l'inevitabile aumento della pena trova conferma nei reati connessi alla violazione dei dati informatici. La sanzione della reclusione, prevista dall'articolo 615-ter del Codice penale per alcuni reati informatici, si estende infatti «da due a dieci anni» (anziché «da uno a cinque anni»). Nei casi in cui i reati commessi riguardino «sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico», la reclusione varia «da tre a dieci anni e da quattro a 12 anni».

In materia di intercettazione, si inasprisce la pena detentiva dell'articolo 617-quater del Codice penale: «da quattro a dieci anni» e non più da «tre a otto anni».

L'altrettanto collaudato meccanismo del "tendere la mano" si ritrova nella nuova figura dell'hacker pentito. Le pene «sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi».

È difficile prevedere efficacia e portata applicativa di tali misure, stante la peculiarità criminologica del tipo d'autore e della natura del reato. La cybercriminalità ha caratteristiche specifiche. Nessun confine geografico, nessun testimone, nessuna temporalità, con spiccate se non esclusive origini e finalità economiche. L'hacker si muove nell'anonimato, in una rete di complicità diffusa e con condotte seriali e su larga scala, il che assicura una buona dose di impunità. E per converso lo Stato deve investire ingenti risorse tecnologiche in termini di uomini e mezzi per l'accertamento del reato e l'individuazione dei responsabili. Pentirsi e collaborare implica una convenienza (la famosa «controspinta alla spinta psicologica») altrettanto forte e difficile da immaginare.

Per le medesime ragioni la deterrenza sanzionatoria rischia di non colpire nel segno. Semmai è la spia della riconosciuta insidiosità di tali reati e della correlata aggressione a beni giuridici di preminente interesse nella scala costituzionale dei valori.

E qui è utile distinguere nuovamente. Accanto a forme tradizionali e meno pericolose (truffe informatiche), semmai particolarmente odiose perché dirette verso persone fragili, il baricentro della preoccupazione sposta il proprio asse verso condotte in grado di carpire segreti inerenti alla sicurezza nazionale o danneggiare reti informatiche strategiche. Un genere di criminalità che vanta un'organizzazione ramificata e collaudata, sulla base di precise direttive e persino indirizzi governativi, come inchieste internazionali hanno dimostrato.

> SICUREZZA NAZIONALE
> **Severità punitiva giustificata dai valori in gioco ma la prevenzione funziona di più**

> PREVENZIONE
> **L'intelligenza artificiale può sviluppare capacità predittive e strategie di contrasto tarate sull'individualità**

Se in astratto l'opzione di severità punitiva è giustificata dai valori in gioco che si possono spingere fino alla tenuta dell'ordine democratico, è altrettanto chiaro in concreto come l'attività di intelligence e di prevenzione rivesta un ruolo fondamentale.

Prevenzione che si declina in una duplice prospettiva: contenitiva, cioè dotarsi degli strumenti tecnici e dei programmi di sicurezza per impedire l'attacco, proattiva, nel senso di un costante monitoraggio e alert di obiettivi sensibili, finalizzati al riconoscimento precoce dell'hacker. L'intelligenza artificiale si rivela allora un alleato prezioso e lo sarà ancora di più in un futuro ravvicinato, capace come è di elaborare abilità predittive e strategie di contrasto tarate sull'individualità.

Ordinario di Diritto Penale
Università degli Studi di Salerno
Osservatorio Fondazione Bruno Visentini