Come le mafie si muovono nel mondo della rete.

DOTT. IVANO GABRIELLI
Direttore Polizia Postale e delle Comunicazioni

La proliferazione di fenomeni criminosi che si sviluppano nel mondo di Internet attesta come anche la criminalità organizzata di tipo mafioso sfrutti le opportunità offerte dal cyberspazio. Le nuove modalità di azione dimostrano come i cyber criminali siano sempre più sofisticati ed in grado di fare rete, divenendo un *asset* strategico per la criminalità organizzata contemporanea.

L'assenza di confini geografici nel c.d. *quinto dominio* garantisce loro l'anonimato nonché la rapidità e l'economicità delle condotte, favorendo la realizzazione di scenari criminali che finiscono per influire anche sulla sicurezza nazionale.

Il *Cybercrime* rappresenta oggi una delle principali fonti di allarme per la tenuta del sistema socio/economico del Paese e delle strutture tecnologiche che ne supportano le funzioni essenziali, che ha attraversato nell'ultimo periodo un ulteriore passaggio evolutivo con l'estensione della minaccia alla pacifica convivenza nelle moderne democrazie, con risvolti e dinamiche di livello internazionale. Nel complesso considerata infatti, la minaccia *cyber* conserva una matrice ancora largamente criminale, se si considera che oltre il 70% degli attacchi cibernetici nel mondo risulta perpetrato per la realizzazione di profitti illeciti.

Il mondo cambia e con esso, inevitabilmente, anche il fenomeno criminale, in special modo nella sua dimensione organizzata, proiezione di modelli antropologici ed economici asintotici, che ripercorrono ed affiancano le dinamiche sociali evolutive. La rapidità e la profondità del cambiamento del primo, da sempre, ha inevitabilmente determinato le trasformazioni del secondo.

Oggi, le mafie sono sempre più ibride, flessibili nella loro capacità di agire online e offline, sfruttando ogni opportunità offerta dalle tecnologie digitali. Le "nuove leve" del fenomeno mafioso utilizzano la criptofonia, le comunicazioni cifrate, le criptovalute e, certamente, i social media. Li utilizzano per reclutare nuovi affiliati, misurare il consenso, comunicare minimizzando il rischio di essere intercettati, pianificare e rendere più profittevoli le loro attività criminali.

Le nuove mafie hanno già assoldato i migliori hacker per impegnarli a pieno regime in tutte le loro attività illegali su Internet. Pensare che non approfittino degli immensi affari che possono essere realizzati nel cyberspazio è un gravissimo errore di valutazione. Le cyber-mafie saranno la frontiera criminale del terzo millennio ed useranno il mondo virtuale anche per porre in essere attività di proselitismo, per assicurarsi il consenso da sempre funzionale alla loro sopravvivenza.

È ipotizzabile infatti come a breve le organizzazioni criminali riterranno che il cybercrime sia più redditizio dei vecchi modi, più rischiosi, di far denaro, cominciando ad operare e a far transitare soldi attraverso i sistemi informatici, usando tali protocolli per riciclare i propri profitti illeciti.

Le nuove modalità di azione dimostrano come i cyber criminali siano sempre più sofisticati ed in grado di fare rete, divenendo un asset strategico per la criminalità organizzata

Le statistiche e i dati disponibili evidenziano come attacchi informatici di tipo *phishing* o *Sim swap*, mirati a violare reti aziendali e rubare fondi o ad ingannare i dipendenti inducendoli a effettuare ingenti pagamenti verso destinatari terzi secondo il classico schema criminale meglio conosciuto come truffa del *Ceo* o *Ceo fraud*, sono solo alcune delle condotte delittuose maggiormente riconducibili alla vasta rete di crimini informatici legati alla criminalità organizzata.

A riguardo la Polizia Postale ha condotto un'articolata attività investigativa, coordinata dalla Direzione Distrettuale Antimafia di Milano, che ha portato all'esecuzione di quattro misure cautelari personali ed al sequestro di quote societarie per ipotesi di estorsione aggravata dal metodo mafioso ed usura. Tra gli arrestati vi è un professionista nel settore dell'intermediazione finanziaria, che si appoggiava al principale indagato, soggetto già emerso in altre indagini della DDA di Milano ed espressione di una delle più note famiglie di *'ndrangheta* della Brianza, in quanto rispettivamente figlio e cugino di elementi di vertice della locale di Desio.

L'indagine ha consentito di far emergere un grave episodio di infiltrazione mafiosa nel contesto economico ed in particolare nel settore turistico – alberghiero; il dato, già riscontrato in altre attività investigative, è il tentativo da parte di famiglie mafiose di mettere le mani su realtà imprenditoriali in crisi, mediante iniezione di capitali "freschi" ed utilizzo, ove necessario, di metodi intimidatori per ottenere il controllo di attività economiche di rilievo.

L'attività investigativa descritta prosegue una precedente indagine, di ampio respiro internazionale, c.d. operazione "Bruno", conclusa nel 2018 con l'arresto tra Italia e Romania di 21 individui (e altri 14 indagati) per associazione a delinquere transnazionale, frode informatica e accesso abusivo a sistema informatico e riciclaggio di proventi di massive campagne di *phishing*, che lasciava intravedere un concreto interesse della *'ndrangheta* verso il cybercrime.

Le descritte attività, che rappresentano solo alcuni tasselli di una vasta gamma di operazioni svolte e in atto, testimoniano come la criminalità organizzata stia muovendo passi nel mondo della criminalità informatica e verso il cybercrime, reinvestendo poi i profitti nelle ordinarie attività illegali, tipiche mafiose.

Analogo schema è stato seguito per l'operazione, condotta con la Polizia Spagnola Alma Bahia, che ha portato a 16 arresti sul territorio iberico dove una organizzazione criminale il cui vertice era tutto italiano organizzava enormi campagne di phishing aggredendo i sistemi bancari di Italia, Francia e Germania per poi reinvestire i proventi in "più classiche attività delinquenziali" come la prostituzione ed il traffico di armi e stupefacenti. L'organizzazione criminale con base alle Canarie riusciva, proprio in virtù delle capacità imprenditoriali e quindi organizzative a procacciarsi i dati utili alle campagne di phishing, le tecnologie e quindi i tecnici in grado di ingegnerizzare i sistemi di attacco informatico ed infine a gestire le batterie di *money mules* affidabili, i riciclatori, in grado di drenare dai conti le risorse, decine di milioni di euro nel periodo osservato, e farli confluire nel "fondo" criminale appannaggio dell'organizzazione.

È certamente ampio il catalogo dei reati perpetrati nello spazio digitale dalle mafie, trasversalmente caratterizzato dal perseguimento di ingenti profitti illeciti e soprattutto dalla loro gestione e quindi dalla conseguente esigenza di riciclaggio. La sempre più veloce evoluzione tecnologica e l'esponenziale diffusione dei servizi internet hanno comportato, come è noto, la nascita di un vero e proprio "spazio digitale".

Lo sviluppo del web ha consentito alle consorterie criminali maggiormente capaci di intercettare i cambiamenti in atto di incrementare notevolmente i margini di profitto, aumentandone la pericolosità. Sovente la criminalità organizzata sfrutta i servizi online per riciclare il denaro provento di attività illecite, stante l'estrema facilità con cui è possibile movimentare capitali, anche in maniera totalmente anonima, tramite le moderne tecnologie.

Per di più, si è registrato un significativo utilizzo da parte di criminali di criptovalute, per ricevere o effettuare pagamenti connessi ad attività illegali, atteso che risulta estremamente difficoltoso identificare i soggetti della transazione e l'assenza di un ente intermediario centralizzato rende difficili i sequestri patrimoniali.

Le moderne tecnologie, senza parlare di vere e proprie piattaforme di criptofonia come Encro Chat o Sky principalmente dedicate all'attività criminale, offrono la possibilità,

grazie ad avanzate tecniche crittografiche, di adoperare strumenti di messaggistica istantanea "riservati", quali quelli offerti dalle piattaforme Telegram, Viber, Whatsapp, non intercettabili direttamente dalle Forze di Polizia.

Condotta tipica del cybercrime è la frode informatica che può avvenire in varie forme e con diverse tecniche. In primo luogo, può manifestarsi con l'accesso abusivo a sistemi informatici aziendali con lo scopo di ottenere gratuitamente i servizi erogati dalla società vittima. Inoltre, mediante vari modi è possibile ottenere i dati delle persone, delle carte di credito, dei conti correnti, così commettendo un illecito che spesso è solo un passaggio intermedio verso condotte criminali più ampie. In questi casi ci si trova al cospetto di furto dell'identità altrui con lo scopo di appropriarsi delle risorse, delle informazioni o delle autorizzazioni della vittima.

70%

è la percentuale degli attacchi cibernetici che nel mondo risulta perpetrato per la realizzazione di profitti illeciti

In tal modo le mafie riescono a introitare un'enorme quantità di profitti illeciti, soprattutto se tali operazioni vengono poste in essere su larga scala o a danno di operatori economici di rilevanti dimensioni.

Ancora, le immense opportunità di guadagno offerte dal gioco d'azzardo sul web o dalla commissione di illeciti come il phishing e le frodi informatiche su carte di credito o conti correnti bancari non vengono sfruttate solo dalla criminalità organizzata, ma anche da nuovi gruppi delinquenziali, spesso dotati di elevatissime competenze tecniche nel settore tecnologico. L'interesse delle mafie nei confronti del gioco e delle scommesse illegali è risalente nel tempo, da quando è stata definitivamente percepita l'elevata dimensione economica del mondo del gioco e delle scommesse prodotta dal circuito legale. Negli ultimi anni il settore del gioco d'azzardo è letteralmente esploso in Italia e non solo; cifre enormi che non potevano che rappresentare un fattore d'attrazione per la criminalità organizzata, sempre presente dove circolano enormi capitali.

Il controllo del gioco d'azzardo è certamente un settore di grande interesse mafioso in quanto oltre a rappresentare rilevante fonte di guadagno superiore per redditività al traffico di stupefacenti, alle estorsioni e all'usura, risulta essere uno strumento che ben si presta a qualsiasi forma di riciclaggio.

Le organizzazioni criminali investono consistenti capitali attraverso la gestione diretta o indiretta di società concessionarie di giochi e di sale scommesse o mediante l'imposizione di slot machine, riuscendo a realizzare un controllo diffuso sul territorio di competenza nel mercato legale dei giochi e scommesse online, sfruttando anche società di bookmaker con sede formale all'estero.

Sul punto, non è trascurabile poi l'interesse mafioso verso la gestione del gioco legale, un settore che negli ultimi decenni ha avuto un notevole sviluppo grazie all'ampliamento dell'offerta di gioco da parte dello Stato a partire dalla fine degli anni '90 del secolo scorso. In tale "giro d'affari" inevitabilmente, si creano "nuove opportunità" per la criminalità organizzata sempre pronta ad infiltrarsi nella filiera del gioco lecito.

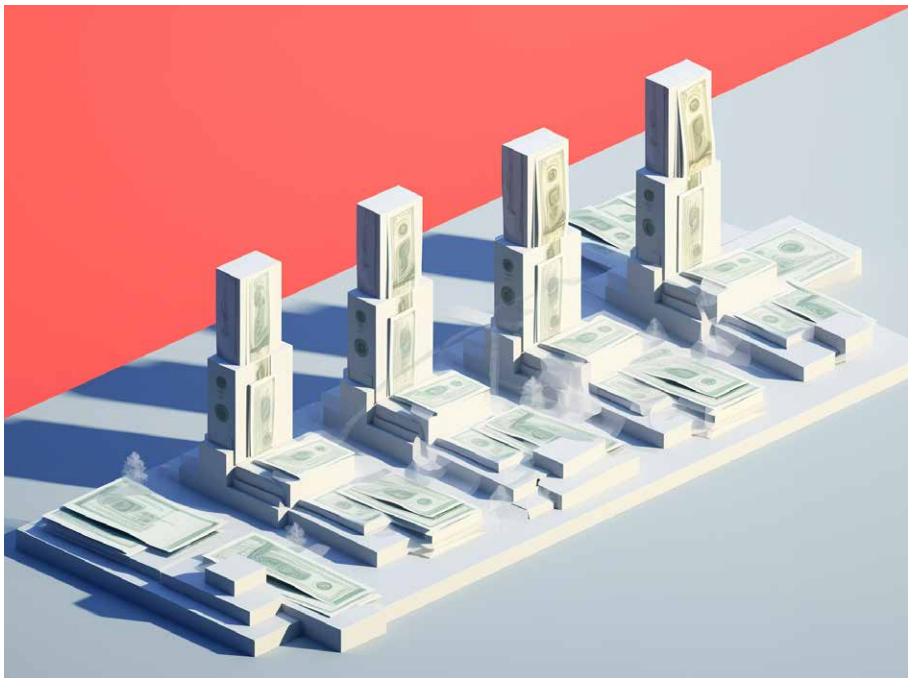
Proprio in materia di scommesse illegali e sodalizi mafiosi, la Polizia Postale, con l'operazione Master Bet, ha smantellato una rete di scommesse clandestine, diffuse su tutto il territorio nazionale e con un giro d'affari collegato di milioni di euro al mese. I soldi venivano poi riciclati attraverso molteplici operazioni finanziarie, anche in rete, per evitarne la tracciabilità. Le indagini sono partite "intercettando" 7 siti web di scommesse abusivi, ossia privi di autorizzazione da parte dell'amministrazione autonoma Monopoli di Stato, con piattaforme di gioco a Malta. Di lì monitoraggi sul web, poi intercettazioni telefoniche e telematiche, pedinamenti e appostamenti, che hanno condotto a 48 denunciati, 46 sequestri preventivi di esercizi commerciali ritenuti centri di scommessa, e 13 persone agli arresti domiciliari. Le persone indagate in totale sono state 107, tra cui numerosi appartenenti a importanti gruppi criminali.

Altro ambiente che necessità di una particolare attenzione è il metaverso, già utilizzato dalle organizzazioni criminali perché ambiente ibrido, in cui i confini tra realtà fisica e virtuale sono pressoché inesistenti, ove si sviluppa un'economia basata su una criptovaluta unificata, ideale per effettuare ad esempio transazioni veloci e anonime e, quindi, potenzialmente per riciclare denaro che passa inosservato ed è difficile da rintracciare.

Aziende virtuali che vendono beni virtuali popolano il metaverso e i riciclatori di denaro possono utilizzare le stesse tattiche del mondo reale di posizionamento, stratificazione ed estrazione per ripulire il proprio denaro, ripetendo questo passaggio più e più volte, impiegando importi diversi ogni volta, rendendo le transazioni estremamente

difficili da tracciare. Il denaro viene prelevato dal metaverso acquistando qualcosa da un altro utente, riconvertito in valuta reale, magari all'estero, così i soldi che sono entrati "sporchi" escono "puliti".

In questo contesto, le mafie puntano inevitabilmente su ogni nuova frontiera offerta da internet che possa agevolare certamente l'attività di riciclaggio su una scala sempre più ampia, producendo in definitiva una sorta di digitalizzazione della criminalità organizzata. Certamente anche l'intelligenza artificiale, intesa come la capacità di un automa di manifestare caratteristiche umane quali il ragionamento, l'apprendimento, la pianificazione e persino la creatività implica una galassia di rischi connessi alla criminalità.



Il cybercrime rappresenta oggi una delle principali fonti di allarme per la tenuta del sistema socio/economico del Paese e delle strutture tecnologiche che ne supportano le funzioni essenziali

L'impiego dell'intelligenza artificiale potrebbe servire, ad esempio, come moltiplicatore di guadagni per le attività di riciclaggio, giacché potrebbe realizzare la commercializzazione di prodotti e il reimpiego del denaro ripulito su vasta scala massimizzando la portata e i profitti.

Paradossalmente l'A.I. potrebbe inoltre rappresentare uno strumento attraverso cui rielaborare e condividere, nel circuito criminale, un determinato "know How" criminale. A tal riguardo, dalla casistica investigativa internazionale, emergono casi di impiego criminale dell'intelligenza artificiale con specifico riferimento alla crittografia di dati e alla gestione di marketplace del dark web per lo scambio di dati di conti bancari e carte di pagamento rubati, strumenti malware, droghe, armi e persino organi umani.

I descritti fenomeni risultano essere certamente suscettibili di influire sul corretto, ordinato sviluppo della vita civile ed economica nonché sulla percezione di sicurezza in seno alla pubblica opinione, minando l'ordine pubblico.

Certamente ad oggi l'attività di contrasto al cybercrime rappresenta uno degli asset strategici nelle agende in tema di politica di sicurezza degli Stati. Allo stato, sicuramente segnali positivi provengono dalla sempre maggiore specializzazione degli organi inquirenti e dalla crescente attenzione posta al riguardo dal legislatore, testimoniata tra l'altro anche dall'istituzione dell'Agenzia Nazionale per la Cybersicurezza e dall'inserimento della sicurezza cibernetica tra le missioni strategiche del Piano nazionale di ripresa e resilienza. Tuttavia, in ragione della rapida evoluzione che connota le tecnologie digitali e della transnazionalità dei reati informatici, risultano necessarie l'implementazione del coordinamento internazionale tra le varie Autorità deputate al contrasto ed una costante attenzione del legislatore ai fenomeni criminali in atto al fine di porre in essere una tempestiva ed efficace azione di contrasto alle nuove forme di cybercrime, anche per il tramite una costante opera di adeguamento della legislazione penale in materia.