# ACN

## Sicurezza digitale e governance nazionale: il ruolo dell'ACN tra *cyber threats*, disinformazione e intelligenza artificiale

*Michela Mastrantonio*

*Il contributo analizza il ruolo dell'Agenzia per la Cybersicurezza Nazionale nella costruzione di un ecosistema di sicurezza digitale integrato, capace di affrontare minacce informatiche complesse, fenomeni di disinformazione e sfide poste dall'intelligenza artificiale. Viene approfondito l'approccio multilivello e partecipativo adottato dall'Agenzia, fondato sull'integrazione tra infrastrutture resilienti, cooperazione istituzionale e consapevolezza collettiva. L'analisi evidenzia la centralità della governance coordinata per garantire sicurezza, fiducia e sovranità digitale.*



### 1. Premessa

Negli ultimi anni il panorama delle piattaforme digitali ha conosciuto una trasformazione profonda e radicale, sostenuta da un incremento esponenziale nella gestione dei dati, della fruizione di servizi digitali e dell'informatizzazione dei processi nelle Pubbliche Amministrazioni, nelle imprese e nelle abitazioni private. Questa evoluzione è stata largamente facilitata dalla convergenza di tecnologie innovative quali la dematerializzazione documentale, il *cloud computing*, l'*Internet of Things* (IoT). In altre parole, l'adozione di soluzioni digitali pervasive ha rimodellato in modo sostanziale il concetto stesso di sicurezza, con l'effetto di esporre il sistema-Paese a nuove e complesse minacce informatiche, non più efficacemente contenute da misure di protezione tradizionali basate su barriere perimetrali[180].

[180] Si sta consolidando sempre più diffusamente l'idea di *safety* come ambito che intende tutelare l'intera collettività dai rischi e dalle minacce capaci di compromettere o indebolire

La sicurezza digitale assume oggi una dimensione multidisciplinare e multifattoriale, ulteriore rispetto alla mera gestione informatica di criticità di natura tecnica. Diviene un vero e proprio pilastro imprescindibile per lo sviluppo economico, sociale e democratico del Paese. Da qui – a partire dal riconoscimento della natura strumentale e vitale per cittadini e imprese – reti informatiche, infrastrutture digitali e dati personali si manifestano al contempo come potenziali vettori di vulnerabilità e di rischio sistemico.

La frammentazione della *governance* della cybersicurezza, associata alla marcata dipendenza da tecnologie e *software* di provenienza estera, aggrava questo scenario – evidentemente già compromesso – generando fragilità significative. Ancora, il *digital divide* territoriale accentua disuguaglianze tra aree più o meno resilienti, con l'effetto di rendere più complicata la messa in sicurezza delle piattaforme considerate essenziali sul piano socio-economico globale.

La sofisticazione e la crescente frequenza degli attacchi informatici evidenziano l'urgenza di adottare misure proattive e integrate per la protezione di sistemi e dati sensibili. Nello specifico ambito delle piattaforme digitali, l'obiettivo di protezione si estende anche ad aspetti di natura sociale: lungi dall'essere meri strumenti neutrali, le piattaforme digitali si configurano come infrastrutture critiche che influenzano profondamente le dinamiche sociali, culturali e politiche. Si tratta piuttosto di strumenti che, interamente considerati in termini di funzionamento tecnico-operativo e delle conseguenti ricadute sulla collettività, hanno il potenziale di generare il c.d. fenomeno della "disinformazione digitale", che in alcuni contesti assume profili di *cybercrime*[181].

Le c.d. "*filter bubble*", così come la crescente diffusione degli attacchi mirati di natura *cyberpsicologica*, la manipolazione degli ecosistemi informativi e l'uso sempre più massiccio di tecniche quali *social engineering* e *phishing*, emergono come episodi chiave nei recenti studi specialistici e nelle analisi empiriche. Questi rilievi impongono la necessità di un approccio alla sicu-

il regolare funzionamento delle dinamiche democratiche. Questa accezione si distingue da quella di *security*, che assume invece un profilo ancillare, limitato al garantire l'affidabilità e la solidità dello spazio cibernetico.

[181] Le evidenze raccolte nel corso di indagini di questo tipo mettono in evidenza in modo sempre più chiaro la presenza e la diffusione pervasiva di modelli organizzativi di tipo "*as-a-service*". La criminalità informatica tende, infatti, a pianificare e a condurre operazioni illecite per conto di terzi, consentendo anche a soggetti con competenze limitate di eseguire attacchi grazie a strumenti e infrastrutture messe a disposizione da altri, con il risultato di rendere questo fenomeno ampiamente accessibile e strutturalmente consolidato.

rezza digitale che sia non solo tecnologico, ma multidimensionale, partecipativo e orientato al coinvolgimento attivo della cittadinanza.

È infatti la centralità delle infrastrutture nel contesto dello sviluppo socioeconomico a imporre una riflessione anche sui profili inerenti alla previsione, alla prevenzione e alla gestione del rischio informatico. Considerata la trasversalità della cybersicurezza, individui, imprese, istituzioni e Stati si trovano inevitabilmente a collaborare secondo un approccio per cui risulta fondamentale il coordinamento delle parti nella gestione e nel controllo del rischio che si pone in un'ottica di "bene comune" o "bene pubblico".

In questo scenario, l'Agenzia per la Cybersicurezza Nazionale (ACN) si afferma come attore strategico essenziale e propone un modello di *governance* che supera la tradizionale dicotomia tra tecnologia e diritto. La sua azione si fonda su una duplice prospettiva: da un lato, investimenti strutturali per rafforzare infrastrutture resilienti, sistemi automatici di difesa e capacità di risposta tempestiva; dall'altro, programmi di sensibilizzazione e formazione per innalzare il livello di consapevolezza collettiva sulle minacce digitali e sulle modalità di prevenzione. Questo modello integrato si riscontra nel quadro normativo e nelle politiche delineate dall'ACN che, come si dirà, intende realizzare un'azione coordinata su più livelli istituzionali e sociali, allineata ai migliori standard europei e internazionali.

## 2. *Governance* della cybersicurezza: quadro normativo e implicazioni strategiche

La *governance* della cybersicurezza si configura come un sistema complesso e multilivello che coinvolge una vasta gamma di attori pubblici e privati e si avvale di molteplici strumenti normativi, tecnici e organizzativi. La natura pervasiva e senza confini del cyberspazio rende inadeguata la tradizionale prospettiva statuale di sovranità su un territorio. Nel contesto cibernetico, garantire un adeguato livello di tutela richiede un approccio strategico capace di superare la sola dimensione regolatoria, orientandosi, invece, anche alla salvaguardia degli interessi pubblici essenziali mediante il coordinamento tra attori istituzionali, sul piano sia nazionale sia sovranazionale. Di conseguenza, in ambito *cyber* un idoneo livello di protezione impone un approccio non più basato solo sulla regolazione, bensì anche sulla difesa degli interessi pubblici rilevanti, attraverso un'interrelazione di soggetti all'uopo preposti. Due principi fondamentali guidano l'efficacia di questa impostazione: (i) la necessità di coinvolgere tutti i settori dell'ordinamento, privato e pubblico; (ii) l'importanza della cooperazione, della stan-

dardizzazione dei processi e della condivisione d'informazioni a più livelli.

Questo è il modello d'azione adottato dall'Unione europea, che si riverbera direttamente e in modo coordinato nei piani d'azione interni degli Stati membri. La Direttiva NIS[182] e il suo più recente aggiornamento[183] (Direttiva NIS 2)[184], ha rappresentato una svolta fondamentale in ambito *cyber*: a partire dalla constatazione della forte interdipendenza tra le reti e della necessità di un approccio coordinato sovranazionale, ha definito un quadro comune di misure relative alla sicurezza delle reti e dei sistemi informativi e ha consentito di creare un impianto normativo armonizzato per garantire un alto livello di protezione in tutto il territorio dell'Unione. Questa armonizzazione si è resa indispensabile date la natura transnazionale delle infrastrutture digitali e la forte interconnessione tra reti; diversamente, la sicurezza europea sarebbe stata insufficiente. A rafforzare questo sistema, il Cybersecurity Act[185] ha affidato all'ENISA un ruolo operativo centrale e ha instaurato un quadro di certificazione comune per prodotti e servizi digitali, con effetti concretamente apprezzabili tanto per la libera circolazione nel mercato unico, quanto per la fiducia degli operatori e degli utenti.

[182] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[183] La Direttiva NIS 2 rafforza e amplia il quadro introdotto dalla prima NIS, colmando le lacune precedenti e imponendo un sistema più rigoroso di gestione del rischio e di segnalazione degli incidenti. Estende il proprio ambito di applicazione a nuovi settori strategici e introduce la distinzione tra "soggetti essenziali" e "soggetti importanti", richiedendo livelli elevati di sicurezza lungo tutta la catena di fornitura. Sul piano strategico, consolida il modello europeo di cybersicurezza basato su cooperazione istituzionale, armonizzazione degli *standard* e cultura del rischio; rafforza l'approccio integrato e resiliente che sostiene la protezione dei diritti fondamentali e la stabilità del mercato digitale europeo. In questo modo, la Direttiva promuove una responsabilizzazione diffusa delle organizzazioni e impone obblighi di sicurezza proporzionati, ma stringenti anche sotto il profilo della catena di fornitura e della resilienza operativa.

[184] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

[185] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013.

In coerenza con la strategia europea sopra descritta, il D.L. 82/2021[186] ha istituito l'Agenzia per la Cybersicurezza Nazionale. Questo intervento normativo ha segnato un passaggio epocale nella definizione di una tutela organica dello spazio cibernetico del Paese: ha definito un modello di *governance* che attribuisce al Presidente del Consiglio un ruolo di indirizzo politico e strategico e colloca l'ACN come soggetto di raccordo tra istituzioni pubbliche, imprese strategiche, centri di *intelligence* e operatori privati. L'ACN, infatti, assume un ruolo che si distingue per la sua duplice natura di autorità strategica da una parte[187] e di centro di coordinamento tecnico-operativo dall'altra[188]. Questo modello di *governance*, com'è evidente, si basa su un approccio ibrido che integra capacità normative e operative, spingendo verso un dialogo costante tra pubblico e privato e tra ambienti politici e tecnici.

L'istituzione dell'Agenzia rappresenta il punto di arrivo di un percorso di sistematizzazione delle esperienze maturate nel quinquennio precedente, in particolare nel quadro del DPCM 17 febbraio 2017[189], recante gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, nonché delle migliori prassi sviluppate in ambito internazionale. Con questo intervento normativo si è riconosciuta autonomia e centralità alla

[186] Decreto-Legge 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale".

[187] Dal punto di vista funzionale, l'Agenzia si configura quale centro di elaborazione della strategia nazionale di cybersicurezza.

[188] Oltre all'elaborazione della strategia nazionale di cybersicurezza, l'Agenzia si occupa anche dello sviluppo concreto di capacità operative di prevenzione, rilevazione e risposta agli incidenti. Essa svolge, inoltre, attività di supporto tecnico al CSIRT Italia ( *Computer security Incident Team* – è il *team* nazionale di risposta agli incidenti informatici, istituito presso l'ACN che gestisce la sicurezza cibernetica del Paese) e promuove la crescita di un ecosistema di collaborazione pubblico-privato per rafforzare la resilienza del sistema Paese. In virtù dell'assetto normativo vigente, l'ACN ricopre anche il ruolo di Autorità nazionale competente per l'attuazione della direttiva NIS e delle sue successive evoluzioni (NIS2), fungendo da punto di contatto unico (PoC) per la sicurezza delle reti e dei sistemi informativi, da Autorità nazionale di certificazione della cybersicurezza e da Centro Nazionale di Coordinamento (NCC) in relazione al Centro europeo per la cybersicurezza industriale, tecnologica e di ricerca.

[189] Decreto del Presidente del Consiglio dei ministri 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali".

dimensione della sicurezza e della resilienza cibernetica, ricondotta alla diretta responsabilità del Presidente del Consiglio dei ministri quale componente essenziale del processo di digitalizzazione del Paese. Questa scelta sottolinea la volontà di garantire una *governance* più unitaria e strategica della cybersicurezza, basata su una stretta sinergia e un coordinamento operativo tra tutte le Amministrazioni competenti per assicurare coerenza e tempestività d'intervento[190]. Si è così voluto costruire un pilastro ulteriore – affidato a un unico soggetto governativo – complementare alle strutture già esistenti in materia di sicurezza nazionale. Concretamente, l'ACN opera quale interfaccia unitaria, nel rispetto delle competenze specificamente attribuite dalla normativa vigente alle altre amministrazioni, per il coordinamento dei soggetti pubblici coinvolti nella sicurezza e nella resilienza cibernetica, nonché per la rappresentanza univoca del Paese nei contesti internazionali, assicurando una postura nazionale coerente con le linee strategiche definite dalla Presidenza del Consiglio dei ministri. Sembra che in questo modo sia stata superata la frammentazione istituzionale inizialmente determinata dalla dispersione di competenze tra più soggetti.

Alla luce del carattere multidimensionale delle sfide affidate all'ACN, l'intelligenza artificiale assume una posizione strategica: l'Agenzia è investita del compito di garantire un impiego sicuro e affidabile delle tecnologie di AI nei sistemi critici, vigilando sulla coerenza tra innovazione tecnologica, sicurezza cibernetica e tutela dei diritti fondamentali. L'integrazione dell'AI nei processi informatici di analisi, prevenzione e risposta consente infatti di anticipare le minacce attraverso modelli predittivi e apprendimento automatico, migliorando la capacità di rilevamento in tempo reale e la resilienza del sistema Paese. Parallelamente, l'Agenzia agisce quale autorità di riferimento nazionale per l'attuazione del quadro regolatorio europeo in materia di AI – in particolare dell'AI Act[191] – assicurando che lo sviluppo e l'adozione di queste tecnologie avvengano nel rispetto dei principi di trasparenza, tracciabilità e *accountability*. Questo ruolo attribuisce

[190] Di prevenzione e repressione dei reati informatici si occupano le Forze di Polizia; la difesa e la sicurezza militare dello Stato nello spazio cibernetico è di spettanza del Ministero della Difesa; la ricerca e l'elaborazione informativa è di competenza degli organismi di informazione per la sicurezza.

[191] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

all'ACN una funzione di collegamento tra cybersicurezza e *governance* algoritmica, ponendola al centro di un nuovo paradigma strategico in cui innovazione e sicurezza diventano pilastri sinergici della sovranità digitale italiana ed europea.

## 3. Disinformazione digitale: *filter bubble*, attacchi mirati e vulnerabilità sociale

"La complessità e l'interdipendenza dei sistemi è cresciuta fino a sfumare la dualità tra la dimensione digitale e il mondo reale, rendendo spesso problematica l'identificazione di confini e rispettive caratteristiche"[192]. In questo contesto la disinformazione digitale assume un ruolo cruciale, tanto da comparire come uno dei tre rischi sistemici individuati dall'Agenzia stessa[193].

La proliferazione della disinformazione digitale e delle minacce *cyber* collegate alle piattaforme e ai motori di ricerca costituisce oggi uno dei problemi più sofisticati e complessi affrontati nel campo della sicurezza informatica nazionale e internazionale. La loro intrinseca natura ibrida, che combina aspetti tecnologici, sociali e politici, amplifica le vulnerabilità dell'intero ecosistema digitale, compromettendo la credibilità e l'affidabilità dell'informazione pubblica.

Alle fondamenta di questi preoccupanti effetti si trovano le c.d. *filter bubble* (letteralmente "bolle di filtraggio"), ambienti informativi polarizzati, generati da algoritmi che profilano gli utenti sulla base delle loro preferenze e comportamenti digitali. Gli algoritmi che operano nell'ambito dell'offerta dei principali servizi digitali, quali *social network*, motori di ricerca e piattaforme *streaming*, selezionano automaticamente i contenuti mostrati, in funzione dei dati preesistenti raccolti sugli utenti stessi. La costruzione di queste *filter bubble*, oggetto di discussione scientifica fin dal 2011[194], av-

[192] "Strategia nazionale di cybersicurezza 2022-2026" dell'ACN, p. 4.

[193] Gli altri due rischi riguardano gli "attacchi cyber dovuti a cybercriminali, attivisti o a campagne statuali coordinate" e le "tecnologie impiegate, le quali sono sviluppate e prodotte da grandi realtà aziendali, talvolta controllate o, comunque influenzate nel loro operato dai Governi in cui hanno sede" ("Strategia nazionale di cybersicurezza 2022-2026" dell'ACN, p. 10).

[194] L'elaborazione teorica è frutto del lavoro di Eli Pariser, che nel volume "The Filter Bubble", pubblicato dal Saggiatore nel 2011, descrive il fenomeno come una sorta di spazio digitale costruito su misura in base agli interessi e ai comportamenti online dell'utente:

viene attraverso sistemi di *machine learning* e algoritmi predittivi che analizzano costantemente le interazioni digitali: *click*, *like*, condivisioni, commenti e tempo trascorso su singole pagine, vengono impiegati per prevedere interessi futuri e proporre contenuti che rafforzano le preferenze già manifestate, creando una spirale di selezione e restringimento dell'orizzonte informativo. Questo meccanismo genera l'illusione che ciò che osserviamo *online* rappresenti un quadro completo della realtà, mentre di fatto si tratta di una selezione parziale e costruita esclusivamente in base ai nostri comportamenti e alle nostre precedenti interazioni.

L'urgenza di affrontare la questione non attiene solo alla pubblicità mirata né influisce unicamente sulle nostre abitudini di consumo. Per una quota sempre più consistente di utenti, infatti, piattaforme di notizie personalizzate, come Facebook, stanno assumendo un ruolo centrale come fonti informative principali[195].

Se da un lato questo meccanismo mira a massimizzare il coinvolgimento e la permanenza sulle piattaforme, dall'altro favorisce la formazione di comunità digitali omogenee, che ricevono informazioni convergenti e incrementano il rischio di diffusione di *fake news* e di campagne manipolative. Questi fenomeni alimentano una crisi democratica profonda, attraverso l'influenza che esercitano sulle scelte politiche degli individui e la creazione di divisioni sociali, con conseguenze che si manifestano con-

dalle pagine consultate ai link selezionati, fino alla traccia dei clic compiuti nella navigazione quotidiana. Quanto più ci si muove all'interno della rete, tanto più quest'ultima tende a riflettere e replicare le nostre preferenze, modellandosi su di esse. Si tratta di una "bolla" proprio perché invisibile e inconsapevole: nessuno vi accede intenzionalmente e la maggior parte degli utenti ignora di esserne immersa.
Il fenomeno della *filter bubble*, concettualizzato nel 2011 deve essere tenuto bene distinto da quello dell'*echo chamber*. Quest'ultima rappresenta una dinamica di natura principalmente psicologica e sociale, in cui gli individui scelgono consapevolmente di esporre sé stessi esclusivamente a contenuti, idee e opinioni affini alle proprie convinzioni, isolandosi da prospettive divergenti e rigettando sistematicamente punti di vista alternativi.

[195] L'Osservatorio annuale sul sistema dell'informazione 2025 di Agcom rappresenta come "Tra i più giovani è prevalente, più che nel resto della popolazione, la propensione ad utilizzare un solo mezzo per informarsi che, come facilmente intuibile, può essere identificato in internet." (p. 3). Nello specifico "In Italia la ricerca di notizie in rete avviene prevalentemente tramite i social network (19,8%). Il loro utilizzo anche quale strumento di informazione si caratterizza e distingue per la spiccata pervasività del mezzo, e per la possibilità di condividere e commentare in tempo reale una notizia. " (p. 10). Alle stesse conclusioni giunge anche la ricerca condotta da Pew Research Center "Social Media and News Fact Sheet", pubblicata a settembre 2025.

cretamente nella polarizzazione e nel rafforzamento delle ideologie estreme[196].

Oltre al fenomeno della polarizzazione, assume crescente rilevanza il problema dell'isolamento informativo. Le analisi condotte sui comportamenti degli utenti assidui di *social network* mostrano una tendenza marcata a fidarsi esclusivamente di fonti e notizie che confermano le proprie convinzioni pregresse, evitando o addirittura rifiutando attivamente contenuti che presentano punti di vista divergenti. Questo comportamento genera una rappresentazione parziale e distorta della realtà, aumentando la vulnerabilità degli individui alla diffusione di *fake news* e fenomeni di disinformazione sistematica. Le ripercussioni psicologiche derivate da queste "bolle informative" sono altrettanto significative: studi recenti mettono in luce come l'isolamento informativo favorisca l'incremento di stati emotivi negativi quali ansia e frustrazione, oltre a stimolare processi di radicalizzazione cognitiva. Questi stati contribuiscono a un aumento dell'aggressività nelle comunicazioni *online*, trasformando i dibattiti in confronti ostili e rendendo sempre più difficile la costruzione di dialoghi costruttivi. Seppur il senso di *comfort* e rassicurazione derivante dalla conferma continua delle proprie posizioni appaia immediatamente gratificante, questa dinamica comporta rischi concreti e rilevanti per il tessuto sociale complessivo: limita fortemente la capacità critica e analitica degli individui, concorre a diffondere e radicare la disinformazione e ostacola il confronto dialogico, determinando fratture sociali profonde e difficilmente sanabili. In sintesi, non solo si assiste a un indebolimento della capacità critica, ma paradossalmente si manifesta una crescente ostilità verso quanti si collocano al di fuori della propria bolla informativa.

Dinamiche dello stesso tipo hanno interessato e riguardano tuttora anche contesti bellici e rendono ancora più preoccupante il fenomeno e urgente l'intervento per contenerlo[197].

---

[196] Uno studio dell'Università di Oxford del 2022, focalizzato sulle piattaforme Twitter e Facebook, ha evidenziato che gli utenti esposti in modo continuativo a contenuti polarizzati tendono a rafforzare progressivamente le proprie convinzioni iniziali.

[197] Un'indagine della BBC ha svelato una campagna di propaganda russa condotta attraverso migliaia di account falsi su TikTok, creata per diffondere disinformazione sulla guerra in Ucraina e indebolire il sostegno europeo a Kiev. I video, che hanno raggiunto milioni di visualizzazioni, accusavano falsamente funzionari e familiari di alti ufficiali ucraini di arricchirsi durante il conflitto, diffondendo immagini e voci generate dall'intelligenza artificiale. BBC Verify ha individuato circa 800 profili legati a questo network, mentre TikTok ha dichiarato di aver già eliminato oltre 12.000 account creati in Russia,

Sul fronte specifico delle piattaforme digitali, queste vulnerabilità aumentano in ragione delle logiche di progettazione orientate alla viralità e all'interazione, accompagnate dalla proliferazione di *bot*, *troll farms* e campagne di amplificazione automatizzata. La diffusione di contenuti *deepfake*, ormai difficilmente distinguibili dalla realtà, mette in discussione le regole della moderazione e la responsabilità delle piattaforme nel garantire un ambiente informativo sicuro e affidabile. Il fenomeno interessa intensamente anche i motori di ricerca, ora tutt'altro che neutri. Numerose attività malevole, mirate al furto di dati, alla distribuzione di *malware* di tipo information *stealer* e alle violazioni delle identità digitali, sfruttano infatti la navigazione *online* e i risultati delle ricerche per veicolare sofisticate campagne di phishing e frodi digitali. I dati forniti dall'Agenzia[198] indicano un incremento dell'8,6% nel 2025 degli attacchi basati su URL malevoli, confermando la persistente evoluzione delle minacce. Il phishing continua a rappresentare la tecnica più diffusa poiché coinvolge oltre il 70% degli incidenti registrati.

Quanto alla sicurezza delle reti, gli attacchi di *Distributed Denial of Service* (DDoS) registrano un costante incremento in termini sia di frequenza sia di complessità. Nel corso del 2025, l'Agenzia ha documentato episodi di particolare rilevanza, tra cui appunto una campagna DDoS che ha interessato infrastrutture strategiche italiane per un periodo continuativo di tredici giorni, durante i quali sono stati rilevati oltre 275 attacchi distinti. Questo fenomeno testimonia la crescente sofisticazione e capacità di persistenza delle minacce dirette alla disponibilità dei servizi critici.

Gli stessi risultati si riscontrano anche sul piano europeo. Il Rapporto ENISA Threat Landscape 2024 individua tra le minacce più rilevanti, oltre ai *ransomware* e agli attacchi che compromettono la disponibilità dei servizi (DoS e DDoS), anche le minacce rivolte ai dati, quali violazioni e fughe di informazioni sensibili. Particolare attenzione viene riservata agli attacchi di *social engineering*, che si avvalgono ormai di strumenti tecnologici

che avevano accumulato circa 850.000 follower e miravano a promuovere punti di vista favorevoli al Cremlino anche in Paesi come l'Italia. La strategia comprendeva anche l'uso coordinato di profili con immagini rubate di celebrità e la pubblicazione simultanea di video quasi identici per manipolare l'algoritmo della piattaforma.

Parallelamente, un'indagine del Threat Analysis Center di Microsoft ha riportato un'altra operazione di disinformazione iniziata a luglio 2023: alcuni video di attori noti, manipolati digitalmente, venivano diffusi per screditare il presidente ucraino Zelensky con la falsa accusa di tossicodipendenza.

[198] "Operational Summary 1° semestre 2025. Dati e indicatori della minaccia cyber in Italia" di ACN.

avanzati, in particolare l'intelligenza artificiale generativa, per rendere più efficaci tecniche quali *phishing*, *vishing*, *qishing* e *smishing*.

L'insieme di queste dinamiche solleva interrogativi sulla coesione sociale e sulla tenuta democratica della società. L'ACN riconosce l'urgenza di affrontare la disinformazione e le minacce correlate con un approccio sistemico e integrato, che vada oltre la mera componente tecnologica. È infatti necessario combinare strumenti automatizzati di rilevazione e intelligenza digitale con strategie formative ed educative rivolte alla cittadinanza (all'utenza in questo contesto) per accrescere il pensiero critico e la capacità di orientamento nell'ecosistema informativo complesso e spesso fuorviante.

Senza una consapevolezza attiva e critica da parte degli utenti, la modalità di consumo informativo basata sulle piattaforme digitali e sui risultati delle ricerche, così come l'esposizione quotidiana ad attacchi informatici anche di semplice natura, rischiano di minare o comunque di indebolire l'efficacia delle altre componenti strategiche dell'azione dell'ACN.

## 4. L'intelligenza artificiale nella cybersicurezza: prospettive per la sicurezza nazionale

In questo panorama, l'intelligenza artificiale, se correttamente progettata e implementata, rappresenta oggi uno degli strumenti più potenti e promettenti nel rafforzamento della sicurezza nazionale in ambito cybersicurezza. Le sue capacità di elaborare grandi quantità di dati in tempi brevissimi, riconoscere *pattern* complessi e adattarsi dinamicamente a contesti in rapido cambiamento la rendono fondamentale per la protezione delle infrastrutture critiche e la difesa degli interessi sovrani dell'intero sistema-Paese[199].

[199] Nel corso del dibattito sull'innovazione tecnologica e la sicurezza digitale in Italia, tenutosi l'8 ottobre scorso presso l'Università Federico II di Napoli nell'ambito del Disclaimer Tour – "AI e criminalità", iniziativa promossa dal Corriere della Sera in collaborazione con CINECA, il Direttore generale dell'ACN, Bruno Frattasi, ha chiarito che "L'intelligenza artificiale è un potente alleato della minaccia cibernetica. Ce ne siamo accorti già da qualche tempo. […] Il phishing è 'migliorato' per quanto riguarda la capacità di ingannare il destinatario. Così come le fake news e i deep fake. L'intelligenza artificiale sta aiutando gli 'attaccanti'. Però va anche aggiunto che l'intelligenza artificiale può rivelarsi una potente arma di difesa dalla stessa minaccia, come tutte le tecniche avanzate che hanno una doppia faccia: la Red e la Blu. La prima è quella nella quale identifichiamo gli attaccanti e gli aggressori informatici, quella Blu è quella con la quale identifichiamo la parte buona, quella che combatte i criminali".

L'IA consente un rilevamento precoce e una risposta tempestiva a minacce informatiche sofisticate, abbattendo i tempi di reazione e massimizzando la precisione nell'individuazione di attacchi potenziali come intrusioni, *malware* o campagne di disinformazione automatizzate. Attraverso sofisticati algoritmi di *machine learning* e *deep learning*, è possibile analizzare in modo proattivo flussi di dati complessi provenienti da fonti eterogenee e individuare anomalie che sfuggirebbero ai tradizionali sistemi manuali o basati su firme statiche.

Questa trasformazione tecnologica si traduce in un vantaggio strategico cruciale per la cybersicurezza nazionale, poiché rende possibile non solo la possibilità di difendersi efficacemente, ma anche di anticipare le mosse degli attori ostili, siano essi gruppi criminali, enti statali o attori ibridi. Inoltre, l'IA consente di automatizzare e ottimizzare le risorse umane e tecnologiche dedicate, incrementandone così l'efficienza e riducendo la possibilità di errore umano.

Naturalmente, un'adozione responsabile e consapevole dell'IA deve includere un rigoroso controllo sui profili di sicurezza, trasparenza, rispetto della *privacy* e limitazione dei *bias* algoritmici. L'ACN si pone come garante di queste condizioni, promuovendo l'uso delle tecnologie IA all'interno di un quadro normativo e deontologico rigoroso, che salvaguardi i diritti fondamentali e la sovranità digitale. Sul piano operativo, si sta investendo nel rafforzamento delle competenze tecniche, nella formazione di esperti di alto profilo e nella creazione di *partnership* pubblico-privato per lo sviluppo di soluzioni IA innovative. Questi sforzi consentono di integrare efficacemente l'IA nelle infrastrutture di monitoraggio, prevenzione e risposta agli incidenti *cyber*, migliorando la resilienza complessiva del sistema-paese.

In questo scenario, la dimensione internazionale gioca un ruolo altrettanto cruciale. La cooperazione con organismi europei e internazionali nella definizione di *standard* comuni e nella condivisione di conoscenze è fondamentale per contrastare minacce che, per loro natura, non possono essere contenute entro confini nazionali. L'IA emerge quindi come uno strumento di sicurezza nazionale non soltanto tecnico, ma anche geopolitico, in grado di migliorare la capacità di deterrenza e di risposta coordinata sul piano globale.

## 5. L'approccio integrato tra consapevolezza dei cittadini e investimenti strutturali per il Paese

Nell'attuale contesto caratterizzato da sfide informatiche sempre più pervasive e sofisticate, l'Agenzia per la Cybersicurezza Nazionale adotta un modello strategico che coniuga, in modo sinergico e integrato, il rafforzamento infrastrutturale con la promozione della consapevolezza e della formazione digitale tra la popolazione e gli operatori economici e istituzionali, secondo un approccio *whole-of-society*[200]. Questo approccio riconosce la cybersicurezza non solo come una questione tecnica, ma come una dimensione sociale che coinvolge attivamente cittadini, imprese, enti pubblici e privati nell'adozione di comportamenti responsabili e nella costruzione di una cultura condivisa della sicurezza digitale.

L'idea di fondo è che "l'obiettivo ultimo della sicurezza cibernetica nazionale può essere raggiunto solo attraverso il contributo di tutte le componenti del tessuto sociale, nessuno escluso"[201].

A partire da questo tipo di impostazione, l'ACN fonda il proprio piano di azione su un duplice fronte: quello tecnico e quello sociale. La Strategia nazionale di cybersicurezza 2022-2026 a questo proposito parla di "fattori abilitanti," che comprendono formazione tecnico-specialistica e diffusione della cultura del rischio, in un quadro sistemico e partecipativo.

Sul fronte tecnico-infrastrutturale, la strategia dell'ACN si orienta verso la realizzazione e il potenziamento di sistemi resilienti e interoperabili, capaci di assicurare la continuità operativa e di contrastare efficacemente minacce digitali di crescente complessità. Questo include, in particolare, lo sviluppo del Polo Strategico Nazionale (PSN), piattaforme di monitoraggio avanzato e reti di laboratori d'eccellenza, che fungono da pilastri tecnologici del sistema nazionale di difesa cyber. Essenziale è l'aderenza a standard internazionali ed europei, come quelli previsti dal Regolamento NIS2 e dal Cybersecurity Act, che garantiscono obblighi rigorosi di audit e certificazione, salvaguardando la sicurezza lungo l'intero ciclo di vita delle infrastrutture digitali.

Parallelamente a questa dimensione tecnica, l'ACN rivolge un'attenzione prioritaria allo sviluppo di competenze e alla diffusione di una cultura della sicurezza *cyber* che permei tutta la società. Operando in sinergia con istituti scolastici, università, aggregazioni industriali e centri di ricerca,

[200] Così viene definita la propria strategia dall'ACN nel documento "Strategia nazionale di cybersicurezza 2022-2026".

[201] Strategia nazionale di cybersicurezza 2022-2026", p. 8.

l'Agenzia promuove iniziative di alfabetizzazione digitale fin dalla scuola primaria, sensibilizzazione continua e formazione specialistica mirata. Progetti come "Repubblica Digitale" e "Punto Digitale Facile"[202] sono emblematici di questa strategia: offrono strumenti e risorse per l'inclusione digitale e per il rafforzamento delle capacità critiche degli utenti, in particolare tra le fasce più vulnerabili e meno esperte. La promozione di un programma capillare di educazione digitale, da attuare anche mediante strumenti online, mira a sensibilizzare la collettività sull'adozione di *best practices* e sulla capacità di riconoscere contenuti *fake* e manipolativi. Analogamente, si investe in campagne di sensibilizzazione all'interno delle organizzazioni pubbliche e private che intendono promuovere una "*cyber hygiene*" diffusa, l'incremento della consapevolezza sui rischi e sulle minacce presenti e la gestione attenta del rischio residuo anche attraverso strumenti di autovalutazione basati su indicatori specifici quali i "*cyber index"*.

L'integrazione tra gli investimenti strutturali e la formazione degli individui genera un ecosistema complesso di sicurezza in cui l'adozione di tecnologie avanzate si accompagna a comportamenti virtuosi e a una responsabilizzazione attiva dei cittadini. La piattaforma "Cybersicurezza Italia" costituisce un luogo privilegiato di confronto, formazione e diffusione delle *best practices*, rafforzando la fiducia collettiva e stimolando la partecipazione civica alla tutela della resilienza digitale nazionale.

L'integrazione di competenze e risorse tra attori istituzionali, aziende strategiche e operatori tecnologici consente di fronteggiare efficacemente eventi critici e minacce emergenti, assicurando un adeguato grado di preparazione e risposta nell'intero tessuto produttivo e infrastrutturale.

[202] "Punto Digitale Facile" rappresenta una rete capillare di sportelli e servizi dedicati a facilitare l'accesso digitale per i cittadini, distribuita su tutto il territorio nazionale. Al 2024, secondo i dati forniti dal Dipartimento per la Trasformazione Digitale (DTD) in collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), sono stati attivati all'incirca 2.220 punti di accesso digitali, che hanno fornito supporto diretto a oltre 264.000 utenti. Il profilo prevalente degli utenti assistiti comprende donne adulte con livello di istruzione che va dalla scuola primaria a quella secondaria, nonché persone disoccupate o lavoratori dipendenti. Il progetto ha prodotto un miglioramento significativo nella consapevolezza digitale di base, traducendosi in una riduzione stimata del 18% negli incidenti di phishing e nelle frodi online nelle aree servite, rispetto agli anni precedenti. Il progetto rappresenta un esempio concreto dell'impegno dell'ACN nell'estendere l'accesso alle competenze digitali e nell'abbattere il *digital divide*, con un impatto tangibile sulla riduzione di incidenti di phishing e frodi online nelle aree di intervento.

## 6. Conclusioni

L'esperienza quotidiana e le responsabilità istituzionali dell'Agenzia per la Cybersicurezza Nazionale orientano la consapevolezza sull'importanza cruciale di un approccio integrato e multilivello nella lotta alla disinformazione online e nella tutela della sicurezza nazionale digitale. La molteplicità e la complessità delle minacce, amplificate dalla rapida evoluzione tecnologica e dalla proliferazione di contenuti digitali manipolativi, impongono un impegno costante e articolato, che solo un'efficace *governance*, in cui l'ACN svolge un ruolo di coordinamento primario, può gestire con efficacia.

Guardando al futuro, è chiaro che l'innovazione tecnologica – in particolare l'adozione responsabile e avanzata dell'intelligenza artificiale – rappresenta una risorsa strategica imprescindibile per rafforzare la resilienza del sistema Paese. La capacità di anticipare, monitorare e rispondere alle minacce *cyber* va necessariamente accompagnata da un investimento continuo nella formazione, nella sensibilizzazione e nella costruzione di una cultura digitale diffusa, che coinvolga trasversalmente tutti i cittadini, le istituzioni e le imprese. Solo la partecipazione attiva e consapevole dell'intera comunità nazionale può trasformare la cybersicurezza da mero obiettivo tecnico a una dimensione condivisa di tutela collettiva di e sovranità digitale.

L'ACN è chiamata a rinnovare il proprio impegno non solo nel perfezionamento degli strumenti tecnologici e normativi, ma anche nell'ampliamento delle collaborazioni strategiche con il mondo accademico, industriale e internazionale, favorendo lo scambio di best practice e la ricerca di soluzioni innovative e sostenibili. In questa prospettiva, la costruzione di un ecosistema *cyber* nazionale integrato, capace di rispondere in modo tempestivo ed efficiente alle sfide future, si configura come la priorità assoluta per i prossimi anni. Sarà fondamentale sviluppare modelli di cooperazione internazionale ancora più efficaci, in quanto nessun Paese, da solo, può affrontare adeguatamente quel panorama globale di rischi e opportunità che caratterizza il cyberspazio contemporaneo.

Il ruolo dell'Agenzia, pertanto, si conferma centrale nel promuovere una cultura della prevenzione che unisca capacità tecnologiche, competenze umane e responsabilità pubblica, creando le condizioni perché il digitale resti uno spazio di partecipazione libera, sicura e affidabile.