ISSN 1971-9892

Sovranità digitale e funzione amministrativa di cybersicurezza

fascicolo
2026/I

CONSULTA ONLINE

MARCO MACCHIA

13 aprile 2026

CONSULTA ONLINE

RIVISTA GIURIDICA SCIENTIFICA DI CLASSE A - AREA 12 - ISSN 1971-9892 – FONDATORE: PROF. PASQUALE COSTANZO

MARCO MACCHIA

Sovranità digitale e funzione amministrativa di cybersicurezza

TITLE *Digital sovereignty and the administrative function of cybersecurity*

ABSTRACT La sicurezza cibernetica emerge come una funzione pubblica complessa, strutturalmente inserita in un contesto multilivello e caratterizzata dall'intreccio tra competenze nazionali e sovranazionali, saperi tecnici e poteri autoritativi. La sua riconduzione nell'alveo delle funzioni amministrative consente di coglierne la natura strumentale alla tutela di interessi pubblici primari – dalla sicurezza dello Stato alla protezione delle infrastrutture critiche, fino alla salvaguardia dei processi democratici – ma al tempo stesso evidenzia i limiti di una gestione confinata entro schemi tradizionali di sovranità territoriale. Il modello di governance che si è progressivamente delineato, fondato su meccanismi di armonizzazione, coordinamento e cooperazione rafforzata tra Unione europea e Stati membri, conferma l'impossibilità di affrontare le minacce cibernetiche attraverso risposte esclusivamente nazionali. In tale assetto, l'Unione europea svolge una funzione di indirizzo e supporto, mentre agli Stati membri spetta l'esercizio diretto dei poteri amministrativi, secondo una logica di complementarità che si riflette anche nel ruolo delle autorità nazionali competenti e nell'impiego di strumenti finanziari e organizzativi dedicati

A multi-level context is what characterises cyber security as a complex public function. It is characterised by the intertwining of national and supranational competences, technical knowledge and authoritative powers. Including it within the scope of administrative functions enables us to recognise its instrumental role in safeguarding primary public interests, ranging from state security to the protection of critical infrastructure and the safeguarding of democratic processes. However, it also highlights the limitations of management confined within traditional territorial sovereignty frameworks. The governance model that has gradually emerged, based on mechanisms of harmonisation, coordination and enhanced cooperation between the European Union and Member States, confirms the impossibility of addressing cyber threats through exclusively national responses. In this framework, the European Union plays a guiding and supporting role, while Member States are responsible for the direct exercise of administrative powers. This logic of complementarity is also reflected in the role of the competent national authorities and in the use of dedicated financial and organisational instruments

KEYWORDS Sicurezza cibernetica, governance multilivello, cooperazione UE–Stati membri, funzione amministrativa
Cybersecurity, multilevel governance, EU–Member States cooperation, administrative function

AUTHOR Professore ordinario di Diritto amministrativo – Università degli Studi di Roma Tor Vergata

Il presente contributo è la rielaborazione della relazione dell'Autore al Convegno dal titolo "Declinazioni, strumenti e prospettive della sovranità digitale", svoltosi presso l'Università degli Studi di Genova l'11 e 12 novembre 2025

* * *

SOMMARIO 1. Introduzione: la *cybersecurity* come funzione amministrativa. – 2. Una funzione condivisa a livello sovranazionale o di competenza prevalentemente nazionale? – 3. Il ruolo dello Stato nazionale. – 4. La rilevanza centrale degli strumenti di partenariato. – 5. Considerazioni conclusive: pace e sicurezza cibernetica.

1. Introduzione: la cybersecurity come funzione amministrativa

È opportuno muovere da due considerazioni di carattere generale, ampiamente condivise nelle scienze sociali. In primo luogo, la pace costituisce il presupposto essenziale dello sviluppo collettivo, in quanto la presenza di conflitti armati impedisce il perseguimento di obiettivi di progresso civile su altri piani, quali la tutela dell'ambiente, la riduzione della povertà e la promozione dello sviluppo economico. In secondo luogo, la prevenzione delle guerre e delle situazioni di ingiustizia presuppone l'esistenza di assetti istituzionali fondati sul diritto internazionale e su principi democratici, idonei a incanalare gli interessi degli Stati all'interno di forme strutturate di cooperazione. In tale prospettiva, la cooperazione organizzata rappresenta lo strumento privilegiato per la tutela degli interessi dei singoli Paesi, in particolare di quelli di minori dimensioni, nella misura in cui consente la definizione di regole comuni volte a contenere l'esercizio del potere fondato sulla mera forza. Essa assume, inoltre, un rilievo centrale nell'affrontare le questioni attinenti alla difesa e alla sicurezza.

Tali presupposti risultano oggi significativamente messi in discussione da un contesto geopolitico caratterizzato da un aumento dei fattori di rischio, da una crescente incertezza e da una riduzione della stabilità complessiva. In questo quadro si colloca l'evoluzione delle politiche della NATO nell'ultimo decennio, che ha condotto a una profonda revisione delle proprie strategie operative: da una fase, risalente al 2014, in cui le sfide emergenti legate alla cybersicurezza e alla militarizzazione dello spazio occupavano una posizione marginale, si è passati a una riorganizzazione orientata a rafforzare la prontezza operativa e la capacità di intervento in scenari di conflitto ad alta intensità tecnologica, con finalità di difesa collettiva degli Stati membri.

Le minacce cibernetiche si configurano allo stato attuale come fattori idonei a compromettere in modo strutturale i processi di pace, anche in ragione dell'assenza di adeguate forme di cooperazione istituzionalizzata e di regimi internazionali capaci di garantire una tutela effettiva degli Stati più vulnerabili[1]. Tale mutamento di scenario ha reso

[1] Il cyber è ormai il quinto dominio operativo della sicurezza, insieme a terra, mare, aria e spazio. Difenderlo richiede capacità dedicate, costanti e integrate. L'importanza dei domini spazio e marino si dimostrano sempre più spesso decisivi e interconnessi. Per quel che concerne lo spazio, la protezione dei satelliti, delle comunicazioni orbitali e dei vettori personali è essenziale per mantenere la continuità informativa e una deterrenza credibile. Anche il dominio subacqueo è sempre più rilevante per la presenza di cavi digitali, gasdotti energetici e risorse minerarie strategiche. Difendere questa dimensione equivale a difendere la sovranità digitale e la sicurezza energetica. Da qui emerge chiaramente il significato dell'integrazione tecnologica e strategica tra cielo, mare e cyber spazio in una visione coerente di protezione nazionale

necessaria una riorganizzazione dell'apparato pubblico, determinando il passaggio da una concezione della cybersecurity quale mero rischio settoriale a quella di interesse pubblico primario, tale da giustificare la predisposizione di strutture amministrative dedicate[2].

Sotto il profilo amministrativo, la cybersecurity assume pertanto la natura di funzione pubblica, intesa come attività finalizzata al perseguimento di obiettivi determinati in via eteronoma, che richiede l'ordinario esercizio del potere pubblico. L'esercizio di tale funzione implica una posizione di sovraordinazione dell'amministrazione, idonea a consentire l'adozione di atti autoritativi suscettibili di imporsi ai destinatari e, in determinati casi, alla generalità dei consociati[3].

Tale funzione si colloca, tuttavia, all'interno di un contesto marcatamente sovranazionale. Le competenze dell'Unione europea in materia di sicurezza cibernetica si inseriscono, infatti, in un sistema di competenze condivise e di sostegno, in cui non è configurabile una competenza esclusiva dell'Unione, ma piuttosto un potere di armonizzazione, coordinamento e rafforzamento delle azioni degli Stati membri. In tal senso, l'art. 4 TFUE riconduce la sicurezza cibernetica all'ambito delle competenze condivise, mentre l'art. 114 TFUE consente l'adozione di misure di armonizzazione funzionali al buon funzionamento del mercato interno, comprese quelle relative alla sicurezza delle reti e dei sistemi informativi.

In questa cornice si inserisce la definizione di sicurezza cibernetica contenuta nell'art. 2 del Regolamento (UE) 2019/881 (c.d. *Cybersecurity Act*), secondo cui essa consiste nell'insieme delle attività necessarie a proteggere le reti e i sistemi informativi, nonché i loro utenti e le altre persone interessate, dalle minacce informatiche[4]. Da tale definizione emerge una concezione della sicurezza umana intesa quale complemento necessario della sicurezza nazionale, secondo un rapporto di integrazione funzionale tra le due dimensioni, in cui la tutela dello Stato si accompagna alla protezione del bene giuridico rappresentato dalla sicurezza delle persone e delle comunità rispetto alle nuove minacce tecnologiche[5].

---

ed europea. Difesa, spazio e cybersicurezza sono tre pilastri fondamentali, strettamente connessi tra loro e solo attraverso essi è possibile garantire la protezione delle infrastrutture critiche. In argomento, S. PIETROPAOLI, *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in *Rivista di filosofia del diritto*, 2019, 390.

[2] I pericoli cibernetici non sono più ricollegati unicamente a singoli obiettivi militari e/o strategici, ma sono da connettere anche ai danni economici e reputazionali che possono essere causati ad un'impresa su scala spesso globale. Non essendo più catalogabili attraverso né la natura dei bersagli (non sempre individuati a monte dai soggetti attaccanti), né l'utilità perseguita dagli stessi (elemento divenuto soltanto eventuale o indiretto), le strategie di attacco hanno così cominciato a distaccarsi sempre più tanto dagli schemi tipici della legge penale, quanto dalle regole proprie dei conflitti tradizionali. Sul tema, A. VENANZONI, *L'ordine costituzionale della cybersecurity*, in *Quad. cost.*, 2024, 34.

[3] Sul punto si rinvia a M. MACCHIA, G. SFERRAZZO, *Sicurezza e rischio tecnologico. La funzione di cybersecurity*, in *Dir. Amm.*, 2025, 112 ss.

[4] In argomento, si v. F. SERINI, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, in MediaLaws, 2023, 186; T. GIUPPONI, *Il governo nazionale della cybersicurezza*, in *Quad. cost.*, 2024, 278.

[5] L. AXWORTHY, *La sécurité humaine: la sécurité des individus dans un monde en mutation*, in Politique étrangère, 1999, 336 ss. Il concetto di cybersecurity non può che essere inteso in modo da coinvolgere non solo le mere attività di gestione e prevenzione dei rischi interni al cyberspazio, ma anche la dimensione virtuale e reale. Del resto, se da un lato

2. Una funzione condivisa a livello sovranazionale o di competenza prevalentemente nazionale?

Una volta ricondotta la cybersecurity nell'alveo delle funzioni pubbliche, in quanto attività amministrativa orientata al perseguimento di interessi generali e caratterizzata dall'esercizio del potere autoritativo, si impone la necessità di interrogarsi sulla sua collocazione sistematica all'interno dell'ordinamento e, in particolare, sulla distribuzione delle competenze tra livello nazionale e livello sovranazionale. Il compito di cura della sicurezza cibernetica affidato alle istituzioni pubbliche nazionali sollecita infatti la scienza giuridica a confrontarsi con una serie di questioni di centrale rilievo, sia sul piano teorico sia su quello applicativo. In tale prospettiva, occorre anzitutto comprendere se la dimensione della sicurezza cibernetica debba essere qualificata come ambito condiviso tra Unione europea e Stati membri, ovvero se essa continui a rientrare prevalentemente nel dominio della sovranità statale. Ne discende l'esigenza di chiarire se la funzione di sicurezza cibernetica, considerata nel suo complesso, possa essere imputata allo Stato in via esclusiva – pur producendo effetti benefici anche a livello euro-unitario – oppure se debba essere ricostruita come funzione amministrativa composita, articolata e condivisa in alcune sue componenti con l'Unione europea[6].

Il problema si pone in termini particolarmente significativi con riferimento al rapporto tra la dimensione europea della sicurezza cibernetica e quella nazionale, segnatamente nel contesto italiano, nel quale tale funzione è stata espressamente ricondotta all'ambito della sicurezza nazionale. Ciò impone di affrontare il nodo teorico del rapporto tra sovranità territoriale e spazio cibernetico, nonché di interrogarsi se il significato giuridico della sicurezza debba essere ricercato primariamente nel rapporto tra individuo e autorità statale, oppure se il paradigma di riferimento debba oggi essere individuato nel contesto europeo[7].

In questa prospettiva evolutiva, l'interesse dell'Unione europea per la sicurezza nazionale degli Stati membri non risulta più circoscritto alla sola esigenza di limitare o relativizzare l'autonomia loro riconosciuta dall'art. 4, par. 2, TUE, ma si manifesta attraverso un'incidenza progressiva, seppur mediata, sulle politiche di sicurezza. Il legislatore europeo affronta ormai tali politiche in una chiave prevalentemente difensiva, orientata al perseguimento del c.d.

---

l'evoluzione delle reti informatiche globali hanno permesso un progresso notevole sul piano economico e sociale di tutte le principali democrazie occidentali, dall'altra la stessa ha esposto individui, imprese e istituzioni a rischi significativi.

[6] Sotto questo profilo, la sicurezza cibernetica non è un problema unicamente tecnico, ma intrinsecamente politico. La sicurezza di uno Stato, della sua economia, delle sue infrastrutture critiche, democratiche, cognitive e industriali passa dalla capacità di coniugare la sicurezza cibernetica e le competenze tecniche di questa alla visione politica, strategica e dottrinale che guidano i vertici dello Stato, i consiglieri, gli analisti e le agenzie di sicurezza e informazione. Non essendo la cybersicurezza un tema tecnico o settoriale, essa va inquadrata tra le questioni attinenti alla sovranità nazionale.

[7] Occorre chiarire insomma se il significato giuridico della sicurezza debba essere ricercato primariamente nell'autorità statale, oppure se sia nel contesto europeo che vada individuato il paradigma di riferimento.

"*de-risking*", muovendo dalla consapevolezza che la sicurezza contemporanea non possa essere efficacemente gestita entro confini rigidamente nazionali.

Si registra, infatti, una chiara tendenza dell'ordinamento dell'Unione a incidere, mediante strumenti indiretti e trasversali, su settori nei quali la sicurezza nazionale degli Stati membri si intreccia con interessi sovranazionali dell'Unione stessa, nella convinzione che la tutela di tali interessi richieda risposte coordinate e integrate. In questo quadro, la competenza dell'Unione europea in materia di sicurezza cibernetica si configura come una competenza di armonizzazione e coordinamento, che non sostituisce quella degli Stati membri, ma la integra, fornendo strumenti normativi e operativi rivelatisi essenziali per il rafforzamento della cooperazione e della resilienza comune.

Emblematica, in tal senso, è l'attività dell'ENISA, Agenzia dell'Unione europea per la cybersicurezza, cui è affidato il compito di fornire supporto tecnico, analisi di rischio e assistenza operativa agli Stati membri. A ciò si aggiunge il Regolamento dell'Unione europea sulla *cyber-solidarietà*, entrato in vigore nel febbraio 2025, volto a migliorare la preparazione, la capacità di individuazione e la risposta agli incidenti di cibersicurezza su scala europea. Tale disciplina introduce, tra l'altro, un sistema europeo di allarme per la cibersicurezza, fondato su poli informatici nazionali e transfrontalieri interconnessi, nonché un meccanismo di risposta alle emergenze, finalizzato ad accrescere il livello complessivo di *cyber-resilienza* dell'Unione.

L'intreccio tra la sicurezza nazionale degli Stati membri e gli interessi sovranazionali dell'Unione risulta ulteriormente confermato dalla compresenza e dalla sovrapposizione di differenti approcci regolatori che caratterizzano il sistema italiano della cybersicurezza. La coesistenza, all'interno dell'ordinamento nazionale, di un modello "*risk-based*" di matrice euro-unionale e di un modello "*security-based*" ancorato alla logica della sicurezza nazionale solleva rilevanti questioni di coerenza sistemica e di tenuta delle garanzie amministrative. Non si tratta, infatti, di una mera pluralità di regimi settoriali, bensì della compresenza di due razionalità regolatorie profondamente diverse, fondate su presupposti, finalità e tecniche di intervento solo parzialmente sovrapponibili.

Il modello NIS2 si inscrive in una concezione cooperativa e funzionale della sicurezza, nella quale il rischio è inteso come variabile dinamica da governare attraverso strumenti flessibili, graduati e proporzionati. In tale prospettiva, l'amministrazione assume un ruolo di accompagnamento e supervisione, orientato alla costruzione progressiva della resilienza complessiva del sistema, e le garanzie procedimentali non rappresentano un ostacolo all'efficacia dell'azione pubblica, bensì una componente essenziale della sua legittimazione[8].

[8] L'approccio *"risk-based"* delineato dalla direttiva NIS2, recepita con il d.lgs. 4 settembre 2024, n. 138, si fonda su un modello di gestione del rischio dinamico e proporzionato. Le entità NIS sono chiamate a valutare in modo continuo la probabilità e la gravità degli incidenti potenziali, tenendo conto dell'impatto operativo, economico e sociale degli stessi, e a commisurare conseguentemente le misure di sicurezza al livello di esposizione al rischio e alla propria dimensione organizzativa. La disciplina, consapevole dell'impossibilità di eliminare integralmente il rischio, non persegue un

Al contrario, il modello del PSNC si fonda su una concezione più tradizionale e difensiva della sicurezza, nella quale la protezione di interessi qualificati come essenziali giustifica un assetto autoritativo, caratterizzato da obblighi puntuali, da un elevato grado di segretezza e da una compressione strutturale degli spazi partecipativi[9].

La convivenza di tali modelli determina, sul piano applicativo, un potenziale disallineamento degli standard di tutela, soprattutto laddove i medesimi soggetti risultino simultaneamente assoggettati a entrambi i regimi. In questi casi, il rischio è quello di una frammentazione della funzione amministrativa, nella quale la qualificazione dell'interesse protetto – economico-funzionale nel paradigma NIS, strategico-nazionale nel paradigma PSNC – finisce per incidere in modo decisivo non solo sull'intensità degli obblighi sostanziali, ma anche sull'ampiezza delle garanzie procedimentali e del controllo giurisdizionale. Ne deriva una tensione latente tra esigenze di effettività della sicurezza e principi di uguaglianza, prevedibilità e proporzionalità dell'azione amministrativa[10].

In tale contesto, il problema non è tanto la legittimità, in astratto, di modelli differenziati di regolazione della sicurezza cibernetica, quanto piuttosto l'assenza di un chiaro criterio ordinatore che consenta di governarne l'interazione. In mancanza di un coordinamento sistematico, la sovrapposizione dei due approcci rischia di tradursi in una stratificazione disorganica di obblighi e poteri, nella quale la logica emergenziale e securitaria tende a prevalere su quella cooperativa e garantista, con il pericolo di una progressiva normalizzazione di strumenti eccezionali in ambiti sempre più ampi dell'azione amministrativa.

La sfida che si pone al legislatore e all'interprete è, dunque, quella di ricondurre tale dualismo regolatorio entro un quadro coerente, capace di preservare l'efficacia delle politiche di sicurezza senza sacrificare, oltre il necessario, i principi fondamentali dello Stato di diritto. In questa prospettiva, la cybersicurezza si conferma non solo come terreno di

---

irrealistico obiettivo di "rischio zero", ma richiede l'adozione di misure adeguate e ragionevoli, in un bilanciamento costante tra efficacia della protezione e sostenibilità dei costi. In tale cornice, l'intervento sanzionatorio assume carattere residuale, collocandosi all'esito di un sistema graduale che privilegia strumenti di monitoraggio, supporto, ispezione e misure correttive prima dell'attivazione della risposta punitiva.

[9] L'approccio "*security-based* proprio del Perimetro di sicurezza nazionale cibernetica (PSNC), disciplinato dal d.l. 21 settembre 2019, n. 105 conv., con modif. nella legge 18 novembre 2019, n. 133, si caratterizza per una logica maggiormente imperativa e prescrittiva. Gli obblighi di sicurezza sono puntualmente predeterminati nei decreti attuativi e il loro mancato rispetto comporta, di regola, l'applicazione automatica della sanzione. In tale modello, la conformità assume tratti rigidi: il livello di rischio residuo o l'adeguatezza parziale delle misure adottate rilevano esclusivamente ai fini della quantificazione della sanzione entro i limiti edittali, senza incidere sulla stessa valutazione della sanzionabilità della condotta. Ne deriva che, mentre la NIS2 configura un obbligo di risultato fondato sulla ragionevolezza e proporzionalità delle misure, il PSNC si impernia su obblighi di mezzo puntuali e predeterminati.

[10] Questa dicotomia regolatoria si riflette in un diverso standard di tutela procedimentale. Nel modello NIS, le garanzie partecipative risultano rafforzate e integrate lungo l'intero svolgimento del procedimento amministrativo; nel modello PSNC, invece, le esigenze di riservatezza, tempestività e operatività, intrinseche alla logica della sicurezza nazionale, tendono a comprimere gli spazi di partecipazione procedimentale, il contraddittorio e, non da ultimo, l'ampiezza del sindacato giurisdizionale sugli atti adottati, ponendo delicati interrogativi in ordine al bilanciamento tra efficacia dell'azione di sicurezza e tutela delle garanzie proprie dello Stato di diritto. Sul tema, M. MATASSA, *La sicurezza cibernetica come funzione pubblica*, Milano, Franco Angeli, 2025, 27 ss.

innovazione tecnologica, ma come banco di prova privilegiato per la ridefinizione contemporanea del rapporto tra sicurezza, amministrazione e garanzie democratiche.

3. Il ruolo dello Stato nazionale

La configurazione della sicurezza cibernetica come funzione amministrativa esercitata in un contesto di competenze condivise impone di analizzare il modello di governance multilivello che ne disciplina l'attuazione concreta. Tale modello si caratterizza per la coesistenza e l'interazione di una pluralità di attori istituzionali, operanti a livello europeo e nazionale, cui sono attribuite funzioni differenziate ma tra loro interdipendenti, secondo una logica di cooperazione rafforzata piuttosto che di sostituzione delle competenze statali.

Sul piano dell'Unione europea, la *governance* della cybersecurity si sviluppa prevalentemente attraverso strumenti di coordinamento, armonizzazione normativa e supporto tecnico-operativo, volti a garantire un livello elevato e uniforme di sicurezza delle reti e dei sistemi informativi all'interno del mercato interno. In tale contesto, l'ENISA svolge un ruolo centrale quale nodo di raccordo tra le istituzioni europee e le autorità nazionali, fornendo linee guida, analisi di rischio, assistenza tecnica e supporto nella gestione degli incidenti, senza tuttavia esercitare poteri autoritativi diretti nei confronti dei soggetti pubblici o privati.

A livello nazionale, l'attuazione delle politiche di sicurezza cibernetica è affidata a un insieme articolato di autorità competenti, cui spetta l'esercizio diretto della funzione amministrativa. Nel caso italiano, tale assetto riflette la riconduzione espressa della cybersecurity nell'ambito della sicurezza nazionale, con la conseguente attribuzione di competenze a strutture inserite nel perimetro della Presidenza del Consiglio dei ministri e del Sistema di informazione per la sicurezza della Repubblica. In particolare, l'Agenzia per la cybersicurezza nazionale (ACN) è chiamata a svolgere funzioni di prevenzione, vigilanza, risposta agli incidenti e coordinamento, operando quale punto di contatto nazionale nei rapporti con le istituzioni europee e con le autorità omologhe degli altri Stati membri.

Se alla Presidenza del Consiglio dei ministri, in veste di vero e proprio "super-ministero", sono attribuite rilevanti competenze di indirizzo strategico e un'estesa potestà normativa – la cui *ratio* è da rinvenire nel suo ruolo di sede istituzionale deputata all'armonizzazione delle politiche di sicurezza secondo l'indirizzo governativo – l'Agenzia per la cybersicurezza nazionale si configura come la autentica centrale operativa del sistema, chiamata a garantirne il funzionamento quotidiano.

Quale "autorità nazionale competente" e "punto di contatto unico" ai sensi della normativa europea, l'ACN concentra in sé, anche mediante l'incorporazione di strutture preesistenti, le principali funzioni di regolazione, vigilanza, coordinamento operativo e certificazione in materia di cybersicurezza. Tale accentramento funzionale è accompagnato

dal riconoscimento di un significativo grado di autonomia organizzativa e operativa, nonché dall'attribuzione di poteri autoritativi che si traducono in specifici obblighi informativi, di cooperazione e di conformazione in capo ai soggetti destinatari della disciplina.

In questa prospettiva, si fa strada una dimensione della sicurezza cibernetica che ha una duplice natura: la difesa del "fortino" tecnologico, che protegge quegli interessi di fronte ad attacchi tesi a minarne la stabilità; l'attività di prevenzione, che si coagula nella promozione della resilienza delle infrastrutture rispetto al pericolo, potenziale o attuale, di pregiudizio al funzionamento delle stesse, al fine di inibire o mitigare i danni alle persone, alle imprese di settori nevralgici per la vita economica, o alle istituzioni democratiche. La funzione amministrativa connessa all'ordine pubblico digitale diventa allora l'organizzazione e la raccolta di risorse, processi e strutture volte a proteggere il cyberspazio e i sistemi abilitati da eventi pregiudizievoli, al fine di tutelare interessi considerati rilevanti anche ai fini della sicurezza nazionale[11].

Ne costituisce un esempio emblematico l'ambivalenza funzionale dell'Agenzia per la cybersicurezza nazionale, la quale opera secondo modalità profondamente differenti a seconda del contesto regolatorio di riferimento. Nell'ambito della disciplina NIS, l'ACN esercita poteri che si avvicinano a quelli tipici delle autorità amministrative indipendenti: monitoraggio, ispezione, prescrizione di misure correttive ed eventuale irrogazione di sanzioni, secondo un approccio *risk-based* di matrice europea. In tale cornice, l'Agenzia non esaurisce la propria azione nella dimensione repressiva, ma assume un ruolo proattivo di accompagnamento alla compliance, attraverso l'elaborazione di orientamenti, il supporto tecnico-operativo e l'attivazione di interlocuzioni strutturate con i soggetti regolati. I poteri istruttori sono funzionali a un modello cooperativo di regolazione, volto a individuare e correggere tempestivamente le vulnerabilità prima che esse si traducano in incidenti rilevanti per la sicurezza del sistema-Paese.

Diversamente, nel contesto del Perimetro di Sicurezza Nazionale Cibernetica (PSNC), l'ACN opera prevalentemente quale snodo operativo tra l'indirizzo politico-strategico della Presidenza del Consiglio dei ministri e l'attuazione concreta delle misure di protezione delle infrastrutture critiche nazionali. In tale ambito, l'Agenzia è chiamata a gestire procedure essenziali ad alto contenuto discrezionale e strategico, quali l'individuazione dei soggetti da includere nel Perimetro, la gestione della piattaforma per la comunicazione degli asset digitali rilevanti e il coordinamento delle attività del Centro di valutazione e certificazione nazionale (CVCN) per l'analisi della sicurezza dei beni ICT. Gli atti adottati in questo contesto si collocano nell'alveo dei poteri speciali a tutela degli interessi strategici nazionali, connotandosi per un'elevata intensità pubblicistica e per un marcato legame con le esigenze di sicurezza nazionale.

[11] Sul tema, R. URSI, *Introduzione, La sicurezza cibernetica come funzione pubblica*, in *Cybersecurity e istituzioni democratiche un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, fascicolo II, Milano, Mimesis, 2025, *passim*.

Questa duplice vocazione dell'ACN produce effetti significativi sul piano delle garanzie e, in particolare, sul controllo giurisdizionale. Se, infatti, nel contesto NIS il sindacato del giudice amministrativo sui poteri esercitati dall'Agenzia non incontra particolari limitazioni, nel regime del PSNC la prossimità delle decisioni alla sfera della sicurezza nazionale comporta un affievolimento delle forme di controllo, soprattutto con riferimento alle scelte strategiche relative alla perimetrazione e alla valutazione degli interessi coinvolti. Ne emerge, così, una tensione strutturale tra esigenze di effettività della tutela giurisdizionale e necessità di riservatezza e rapidità decisionale, che costituisce uno dei nodi più delicati del modello italiano di governance della cybersicurezza.

Il modello di governance che emerge nel complesso non si fonda su una rigida ripartizione verticale delle competenze, ma su un intreccio funzionale tra livelli di governo, nel quale l'Unione europea fornisce il quadro normativo e gli strumenti di cooperazione, mentre agli Stati membri spetta l'esercizio concreto dei poteri amministrativi e l'adozione delle misure autoritative necessarie. Tale assetto riflette una concezione della sicurezza cibernetica come interesse pubblico composito, che, pur rimanendo ancorato alla responsabilità primaria dello Stato, richiede forme strutturate di coordinamento sovranazionale per risultare effettivo.

Tale assetto composito trova ulteriore conferma nella modifica, introdotta dalla direttiva NIS2, dei criteri di individuazione dei soggetti destinatari della disciplina. In particolare, il passaggio dal precedente sistema di designazione amministrativa degli operatori di servizi essenziali (OSE), rimesso alle autorità nazionali competenti, a un meccanismo fondato sull'auto-identificazione degli operatori segna un mutamento significativo nella tecnica regolatoria adottata.

La NIS2 introduce, infatti, un criterio oggettivo di inclusione basato sulla dimensione economico-organizzativa del soggetto. La normativa si applica automaticamente agli operatori che esercitano attività nei settori qualificati come "altamente critici" o "critici" e che superano i parametri dimensionali delle piccole imprese secondo la normativa europea. Ne deriva un'inclusione generalizzata delle medie e grandi imprese, mentre le micro e piccole imprese risultano, in linea di principio, escluse, salvo specifiche eccezioni previste per operatori che, pur di minori dimensioni, rivestano un'importanza sistemica per il funzionamento dei servizi essenziali o per la sicurezza complessiva della rete.

Il decreto legislativo di recepimento (d.lgs. n. 138/2024) ha ulteriormente ampliato l'ambito soggettivo di applicazione, estendendo la disciplina non solo alle amministrazioni centrali espressamente previste dalla direttiva, ma anche alle amministrazioni regionali, a talune amministrazioni locali considerate strategiche[12], nonché ad altri enti pubblici. Tale

[12] Il riferimento è alle Città metropolitane, ai Comuni con popolazione superiore ai 100.000 abitanti, ai Comuni capoluogo di regione, alle aziende sanitarie locali. Del resto, il processo di digitalizzazione della pubblica amministrazione ha inciso in modo pervasivo sull'azione e sull'organizzazione al punto che il digitale è divenuto un

scelta rafforza la dimensione pubblicistica del perimetro NIS e accentua il ruolo della cybersicurezza come funzione trasversale dell'amministrazione.

Nel nuovo assetto, sono dunque gli stessi soggetti potenzialmente rientranti nell'ambito applicativo della direttiva a dover verificare la sussistenza dei requisiti previsti e, in caso positivo, procedere alla registrazione presso l'Agenzia per la cybersicurezza nazionale. Questo meccanismo si inserisce coerentemente nella logica della "sicurezza partecipata", che attribuisce agli operatori un ruolo attivo nella costruzione della resilienza complessiva del sistema, pur comportando il rischio di omissioni o ritardi nell'adempimento degli obblighi di auto-valutazione e registrazione.

A fronte di tali criticità, il legislatore ha previsto correttivi idonei a preservare l'effettività del sistema, attribuendo all'ACN il potere di individuare d'ufficio soggetti non ricompresi nei meccanismi automatici di inclusione. Emerge in questo modo un modello eterogeneo, nel quale l'individuazione dei destinatari della disciplina avviene prevalentemente per effetto diretto della legge, ma resta integrabile mediante interventi autoritativi dell'amministrazione, così da garantire flessibilità e adattabilità del perimetro regolatorio all'evoluzione delle minacce cibernetiche e del contesto tecnologico.

La peculiarità del modello trova riscontro anche nelle più recenti scelte di politica pubblica adottate a livello nazionale. In tale prospettiva si colloca l'accelerazione impressa dal Governo italiano alla sicurezza digitale, testimoniata dall'adozione del decreto del Presidente del Consiglio dei ministri, recante la ripartizione delle risorse finanziarie destinate all'attuazione della Strategia nazionale di cybersicurezza per il triennio 2025–2027[13]. Tale intervento normativo rappresenta un passaggio di rilievo nel processo di consolidamento della capacità cibernetica del Paese, incidendo direttamente sull'assetto organizzativo e funzionale della funzione di sicurezza.

Il decreto si fonda su due strumenti finanziari istituiti con la legge di bilancio per il 2022, che costituiscono leve complementari dell'azione pubblica in materia. Da un lato, il Fondo per l'attuazione della Strategia nazionale di cybersicurezza è finalizzato a sostenere

tassello fondamentale della vita amministrativa. Anche grazie allo sviluppo di strumenti informatici volti a elaborare i dati e i metadati in possesso delle varie amministrazioni, nonché a riutilizzarli, alla *ratio* di efficientamento e ottimizzazione dell'attività amministrativa, specialmente conoscitiva, si è affiancata quella della produzione di conoscenza e di sapere a vantaggio generale e di creazione di prodotti e servizi ai cittadini. Risulta pertanto necessario proteggere le reti e le infrastrutture digitali utilizzate dalle amministrazioni da attacchi o da incidenti di natura cyber (c.d. cyber attacchi e cyber incidenti), proprio in ragione del loro carattere strumentale per la tutela dell'interesse pubblico. L'attacco può essere orientato a danneggiare oppure a criptare i dati e chiederne il riscatto per la loro decriptazione mediante i *ransomware*. La natura non necessariamente bellica degli attacchi cibernetici deriva dal fatto che le reti e le infrastrutture digitali sono impiegate da tutte le autorità pubbliche – grandi o piccole, centrali o periferiche – anche quelle estranee all'esercizio di funzioni amministrative essenziali o alla prestazione di servizi pubblici essenziali. In argomento, M. MATASSA, *La sicurezza cibernetica come funzione pubblica*, cit., 2025.

[13] Pubblicato nella Gazzetta ufficiale del 30 settembre 2025. Il decreto concretizza una tappa di consolidamento della governance nazionale della cybersicurezza, costruita negli ultimi anni intorno all'Agenzia per la Cybersicurezza Nazionale e che si muove volendo perseguire un duplice obiettivo. Rafforzare la protezione del perimetro digitale dello Stato e, al tempo stesso, favorire la nascita di un ecosistema di innovazione capace di rendere il Paese più autonoma sul piano tecnologico e più resiliente sul piano strategico.

investimenti orientati all'autonomia tecnologica e al potenziamento delle infrastrutture digitali; dall'altro, il Fondo per la gestione della cybersicurezza è destinato a finanziare le attività operative e i progetti di implementazione concreta delle misure di sicurezza. Tali risorse, integrate dai finanziamenti del Piano Nazionale di Ripresa e Resilienza e dai contributi delle singole amministrazioni pubbliche, concorrono a delineare uno dei pilastri finanziari del sistema nazionale di difesa digitale, rafforzando la capacità amministrativa dello Stato nell'esercizio della funzione di cybersecurity.

Al riguardo, i dati diffusi dall'Agenzia per la cybersicurezza nazionale attestano l'esistenza di circa trecento interventi attualmente in corso riconducibili alla Strategia nazionale. Si tratta di un insieme eterogeneo di iniziative che spaziano dal rafforzamento delle difese informatiche delle infrastrutture critiche all'incremento delle capacità di prevenzione e risposta agli attacchi, fino alla promozione di un ecosistema industriale e imprenditoriale nel settore cyber. Tale pluralità di progetti evidenzia come la sicurezza cibernetica coinvolga l'intero apparato pubblico, interessando ministeri, autorità indipendenti, regioni e province autonome, e producendo effetti che si riverberano anche sul settore privato e sui cittadini.

In questo quadro emerge con chiarezza come lo Stato non sia più l'unico titolare di competenze esercitate in via esclusiva, ma piuttosto il fulcro di un sistema complesso di attribuzioni e responsabilità condivise, nel quale si rende necessario un costante bilanciamento tra l'esigenza di garantire la sicurezza – quale presupposto dell'ordine democratico – e la tutela dei valori fondamentali che informano l'assetto dello Stato costituzionale. Ne emerge un assetto nel quale lo Stato, pur centrale, non esercita più competenze in forma esclusiva, ma coordina una pluralità di soggetti pubblici e privati, rendendo necessario un equilibrio continuo tra l'efficienza dell'azione amministrativa in materia di sicurezza e la tutela dei principi democratici e delle garanzie dell'ordinamento. La *governance* della cybersecurity si configura così come uno spazio di tensione e di equilibrio tra pluralità degli attori coinvolti e salvaguardia dei principi democratici, confermando la natura strutturalmente multilivello e trasversale di tale funzione amministrativa.

4. La rilevanza centrale degli strumenti di partenariato

Se la governance della *cybersecurity* solleva interrogativi rilevanti in ordine alla distribuzione delle responsabilità, ai meccanismi di coordinamento interistituzionale e alle garanzie di legittimità e controllo dell'azione amministrativa esercitata in contesti altamente tecnici, tali questioni emergono con particolare evidenza nel rapporto tra sicurezza cibernetica, competenze tecniche e coinvolgimento di soggetti privati. La sicurezza dello Stato, della sua economia, delle infrastrutture critiche – materiali e immateriali, democratiche, cognitive e industriali – dipende oggi dalla capacità di coniugare l'esercizio della funzione

pubblica con saperi specialistici e capacità operative che l'amministrazione, da sola, non è sempre in grado di sviluppare o aggiornare con la necessaria tempestività.

La rapidità dell'evoluzione tecnologica rende, infatti, strutturalmente insufficiente un modello di intervento esclusivamente pubblico, imponendo il ricorso a forme di partenariato pubblico-privato. Ciò pone interrogativi centrali circa la delegabilità delle funzioni in materia di cybersecurity: occorre distinguere tra attività che possono essere affidate a soggetti privati — in quanto meramente tecniche o strumentali — e funzioni che devono rimanere riservate all'autorità pubblica, in quanto espressive di poteri autoritativi o incidenti su diritti fondamentali[14]. In tale contesto si manifesta il rischio di una dipendenza strutturale dal settore privato, suscettibile di incidere sull'autonomia decisionale dell'amministrazione e sulla stessa sovranità tecnologica dello Stato.

Parallelamente, le organizzazioni pubbliche e private che gestiscono quotidianamente dati e informazioni digitali sono chiamate a evolvere i propri processi di digitalizzazione, garantendo i requisiti fondamentali di disponibilità, integrità e riservatezza. Un rilievo particolare assumono le infrastrutture informatizzate qualificate come critiche, in quanto fornitrici di servizi essenziali — quali energia, acqua, gas, trasporti e comunicazioni — il cui funzionamento regolare costituisce una condizione imprescindibile per lo svolgimento della vita quotidiana dei cittadini. La protezione di tali infrastrutture rappresenta l'ossatura del sistema di erogazione dei servizi essenziali e, più in generale, delle funzioni chiave delle società moderne.

In questo quadro, la pratica dell'"*information sharing*", tanto a livello nazionale quanto europeo, si configura come uno strumento essenziale per il consolidamento di un approccio cooperativo alla sicurezza cibernetica, funzionale sia al coordinamento politico sia al progresso tecnologico. In tale prospettiva si collocano iniziative quali il progetto "*Cyberkit4SME*", promosso da Sogei, volto a fornire alle piccole e micro-imprese strumenti e metodologie per accrescere la consapevolezza e la capacità di gestione dei rischi cyber, attraverso soluzioni progettate per essere facilmente adottabili e integrate nei processi aziendali[15].

Le minacce cibernetiche, peraltro, non risultano più riconducibili esclusivamente a obiettivi militari o strategici in senso tradizionale, ma sono sempre più frequentemente impiegate per causare danni economici, reputazionali e sistemici su scala globale. Ciò incide profondamente sulla nozione di sicurezza pubblica, che in ambito cibernetico si caratterizza

[14] Basti pensare al fatto che la direttiva NIS2 impone alle strutture tecniche degli operatori di servizi essenziali di riferire tempestivamente agli organi di vertice ogni incidente significativo notificato al CSIRT Italia, nonché di fornire aggiornamenti periodici sullo stato della sicurezza informatica. La gestione degli incidenti diviene così parte integrante della governance, non più un mero fatto tecnico isolato. Su questi temi, R. URSI (a cura di), *La sicurezza nel cyberspazio*, Milano, Franco Angeli, 2023, 117 ss.

[15] Il progetto mira a sviluppare un pacchetto di strumenti e metodologie che permettano alle PMI e alle micro-imprese di innalzare la loro consapevolezza e maturità nella gestione e mitigazione dei rischi cyber. Gli elementi del "toolkit" che verrà messo a punto sono pensati per essere facili da adottare, semplici da usare e da integrare nei processi di business, specificamente pensati per le PMI e le micro-imprese.

per una spiccata dimensione preventiva e cautelare, essendo orientata a dissuadere comportamenti illeciti e a prevenire eventi dannosi sulla base di valutazioni prognostiche formulate *ex ante*.

Tale capacità di risposta al rischio cyber non può tuttavia esaurirsi in una funzione meramente difensiva, ma deve assolvere anche a una funzione di deterrenza, comunicando all'esterno la prontezza dello Stato a proteggere la propria sovranità informativa. In questo senso, la tecnologia diviene una vera e propria linea avanzata di difesa, chiamata a presidiare il fattore tempo, la qualità dell'informazione e la rapidità del processo decisionale.

La difesa dalle minacce informatiche assume così i tratti di un vero e proprio diritto della prevenzione.

Detta impostazione non è tuttavia esente da criticità sul piano delle garanzie democratiche. Il ricorso a strumenti preventivi in contesti caratterizzati da elevata incertezza e atipicità del rischio espone al pericolo – difficilmente conciliabile con uno Stato di diritto – di una indeterminatezza dei presupposti che legittimano l'adozione di provvedimenti restrittivi di diritti fondamentali. La carenza di tipicità delle misure di prevenzione in ambito cibernetico richiama, per molti aspetti, le criticità già evidenziate dalla giurisprudenza della Corte europea dei diritti dell'uomo in relazione alle misure di prevenzione personali.

Le menzionate tensioni emergono in modo particolarmente evidente nei processi di protezione del funzionamento democratico, che includono, tra l'altro, l'utilizzo di applicazioni di tracciamento, la sicurezza delle sedi decisionali digitalizzate – come le camere di consiglio telematiche – e la gestione di dati conservati su infrastrutture *cloud* localizzate all'estero e sottratte, in parte, alla diretta applicazione delle regole statali. In tali casi, a un rischio più elevato deve necessariamente corrispondere un apparato regolatorio più stringente, tanto più in considerazione della particolare vulnerabilità delle pubbliche amministrazioni agli attacchi informatici. Nondimeno, la funzione di *cybersecurity* assume sempre più i tratti di una "frontiera avanzata" nel confronto continuo tra Stato e forme di anti-Stato digitale, imponendo l'impiego di strumenti, accertamenti e modalità operative talvolta atipiche, in ragione dell'altrettanto atipica capacità dei cybercriminali di adattare rapidamente le proprie strategie. In tale contesto, il potere valutativo dell'amministrazione incontra un limite solo in presenza di fatti inesistenti o obiettivamente privi di qualsiasi valore sintomatico, confermando la centralità del controllo di ragionevolezza e proporzionalità quale presidio imprescindibile di legittimità dell'azione amministrativa.

5. Considerazioni conclusive: pace e sicurezza cibernetica

Alla luce delle considerazioni svolte, la sicurezza cibernetica emerge come una funzione pubblica complessa, strutturalmente inserita in un contesto multilivello e caratterizzata dall'intreccio tra competenze nazionali e sovranazionali, saperi tecnici e poteri autoritativi. La sua riconduzione nell'alveo delle funzioni amministrative consente di coglierne la natura

strumentale alla tutela di interessi pubblici primari – dalla sicurezza dello Stato alla protezione delle infrastrutture critiche, fino alla salvaguardia dei processi democratici – ma al tempo stesso evidenzia i limiti di una gestione confinata entro schemi tradizionali di sovranità territoriale. Il modello di governance che si è progressivamente delineato, fondato su meccanismi di armonizzazione, coordinamento e cooperazione rafforzata tra Unione europea e Stati membri, conferma l'impossibilità di affrontare le minacce cibernetiche attraverso risposte esclusivamente nazionali. In tale assetto, l'Unione europea svolge una funzione di indirizzo e supporto, mentre agli Stati membri spetta l'esercizio diretto dei poteri amministrativi, secondo una logica di complementarità che si riflette anche nel ruolo delle autorità nazionali competenti e nell'impiego di strumenti finanziari e organizzativi dedicati.

La crescente centralità del partenariato pubblico-privato, imposta dalla rapidità dell'innovazione tecnologica e dalla specializzazione delle competenze richieste, introduce tuttavia ulteriori profili di complessità, imponendo una chiara delimitazione tra attività delegabili e funzioni riservate all'autorità pubblica, al fine di evitare forme di dipendenza strutturale dal settore privato e di preservare l'autonomia decisionale dello Stato. Parallelamente, la natura preventiva e cautelare della sicurezza cibernetica, intesa anche come strumento di deterrenza e protezione della sovranità informativa, solleva delicati interrogativi in ordine alla compatibilità delle misure adottate con i principi di legalità, tipicità, proporzionalità e tutela dei diritti fondamentali. In definitiva, la cybersecurity si configura come un ambito paradigmatico delle trasformazioni contemporanee del diritto amministrativo, nel quale l'esigenza di efficacia dell'azione pubblica deve costantemente confrontarsi con la necessità di garantire il controllo democratico, la legittimazione del potere e la salvaguardia dei valori dello Stato di diritto. È in questo equilibrio, necessariamente dinamico, tra sicurezza, tecnica e garanzie costituzionali, che si gioca oggi la tenuta giuridica e istituzionale delle politiche di sicurezza cibernetica.

In conclusione, se la pace costituisce il presupposto imprescindibile su cui si fonda lo sviluppo sociale e istituzionale, la sicurezza cibernetica si configura come uno degli strumenti essenziali per la sua tutela, sia in chiave preventiva rispetto ai conflitti emergenti, sia come presidio a difesa della stabilità democratica di un Paese. Le minacce che si manifestano nel cyberspazio, per loro natura svincolate da confini territoriali e riconducibili a un "non-luogo", impongono il superamento di approcci meramente nazionali e richiedono forme strutturate di coordinamento e cooperazione organizzata. In tale prospettiva, il quadro europeo rappresenta lo spazio istituzionale privilegiato per la definizione di regole comuni capaci di contenere l'asimmetria di potere tra gli attori coinvolti e di limitare il rischio che il diritto del più forte prevalga in assenza di vincoli condivisi. La cooperazione multilivello, fondata su principi di solidarietà, responsabilità e armonizzazione normativa, si conferma così come un pilastro imprescindibile delle politiche di difesa e sicurezza, non solo per la protezione delle infrastrutture e delle informazioni, ma anche per la salvaguardia dei valori democratici e dello Stato di diritto.