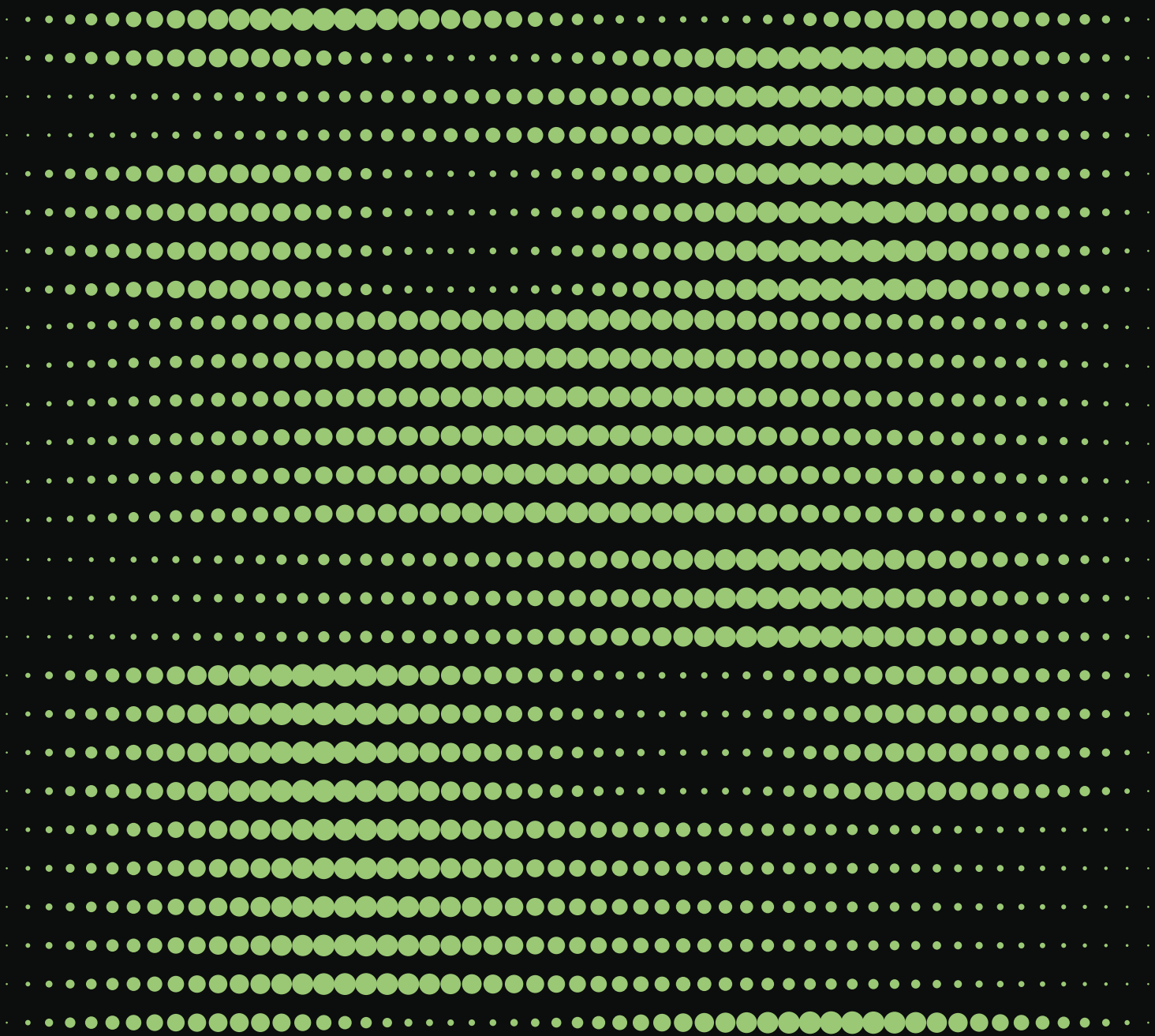
RIVISTA DELLO STATO DIGITALE

02



2025

RIVISTA DELLO **STATO DIGITALE**

02

Pubblicazione scientifica in formato digitale
su informatica e sfera pubblica
ISSN 3103-3768

Numero 2 – Anno 2025

I contributi di questa Rivista sono sottoposti alla valutazione di un revisore in forma anonima (*double blind peer review*), con la sola eccezione della rubrica "Lo Scaffale".

La Rivista si conforma alle linee guida stabilite dalla *Committee on Publication Ethics* (COPE), nel rispetto del Codice etico consultabile in: https://www.rivistastatodigitale.eu

Ogni riflessione e ogni suggerimento sono i benvenuti, nello spirito di una comunità scientifica aperta e partecipata. Per ogni informazione in merito all'invio dei contributi è possibile contattare la Rivista all'indirizzo rsd@irpa.eu

IRPA | ISTITUTO DI RICERCHE SULLA PUBBLICA AMMINISTRAZIONE
Piazza Venezia, 11 - Roma

Roma, febbraio 2026

Progetto grafico: **Nuvola Studio**

Sommario

La declinazione cibernetica della sicurezza nazionale tra vecchie ambiguità e nuove sfide

Riccardo Ursi*

Abstract

Il contributo analizza la progressiva trasformazione della sicurezza nazionale nella sua dimensione cibernetica, mettendo in luce le ambiguità strutturali di una nozione giuridica tradizionalmente priva di definizione positiva e oggi sottoposta a una profonda riconfigurazione funzionale. La sicurezza nazionale viene ricostruita come bene pubblico supremo e al contempo come categoria giuridicamente "aperta", oscillante tra nucleo essenziale di tutela dell'esistenza dello Stato e area estesa di protezione degli interessi strategici nazionali. In tale quadro, il cyberspazio emerge come dominio strategico autonomo e trasversale, caratterizzato da indeterminatezza territoriale, evoluzione tecnologica continua e ibridazione tra dimensione fisica e logica. L'articolo distingue sistematicamente tra sicurezza "nel" cyberspazio, riferita alla tutela dei dati e delle relazioni digitali, e sicurezza "del" cyberspazio, intesa quale declinazione diretta della sicurezza nazionale, volta a proteggere l'ecosistema digitale come infrastruttura critica per la vita civile, economica e istituzionale. La sicurezza cibernetica come una funzione pubblica composita, articolata in difesa, prevenzione e resilienza, sta progressivamente trasformando la sicurezza nazionale in una forma di sicurezza europea, anticipando un possibile mutamento strutturale dei tradizionali paradigmi della sovranità e della protezione statuale.

Sommario

1. Il volto ambiguo della sicurezza nazionale

Come è noto, l'ordinamento italiano, pur riconoscendo implicitamente la sicurezza nazionale come bene pubblico supremo, non ne fornisce una definizione positiva. Si riscontra una fisiologica ambiguità che ha generato un'indeterminatezza funzionale connotata da ampi margini di discrezionalità politica e amministrativa[1]. Nonostante, negli ultimi anni, si sia assistito a un processo di normativizzazione della sicurezza nazionale, il costante richiamo ope-

* Professore ordinario di diritto amministrativo nell'Università di Palermo.

1 A. Wolfers, *"National Security" as an Ambiguous Symbol*, in *Political science quarterly*, 4, 1952, p. 481-502.

rato dal legislatore non ha condotto ad una chiara individuazione dei confini della nozione, la quale continua ad appartenere alla sfera del "pre", "extra" o "meta" giuridico[2].
Per ragioni che si riconducono all'intima sussistenza del potere statuale e che assumono spesso un significato eminentemente politico, la sicurezza nazionale contrassegna una sorta di spazio residuale di sovranità, utilizzato per derogare talvolta ad un impianto regolatorio sovranazionale, talaltra a un sistema di garanzie prescritte[3]. In altri termini, attraverso l'individuazione politica dei beni e degli interessi irrinunciabili per lo Stato si denota un'area di necessario intervento repressivo, preventivo, oppure semplicemente precauzionale, teso a disinnescare una minaccia probabile ovvero a mitigare un rischio possibile a tali beni o interessi.
Dottrina e giurisprudenza hanno concordemente riconosciuto che essa costituisce un bene pubblico primario, la cui tutela è affidata alla responsabilità degli organi costituzionali e al sistema integrato di difesa e informazione per la sicurezza. Essa non coincide con la sola difesa militare: include anche la protezione delle istituzioni democratiche, dell'ordine costituzionale, dell'economia e della società civile[4].
Così, in un'ottica dinamica, la sicurezza nazionale è diventata dal punto di vista giuridico un *empty box* : gli elementi che la riempiono di contenuto funzionale coincidono a seconda dei casi con «l'indipendenza, l'integrità e la sovranità della Repubblica, la comunità di cui essa è espressione, le istituzioni democratiche poste dalla Costituzione a suo fondamento, la personalità internazionale dello Stato, le libertà fondamentali ed i diritti dei cittadini costituzionalmente garantiti nonché gli interessi politici, militari, economici, scientifici ed industriali dell'Italia»[5].
Tuttavia, questa prospettiva potrebbe rendere necessario operare una differenziazione tra il "nocciolo duro" dell'esistenza e un'area di interessenza in cui non è difficile intravedere i caratteri della ancestrale "Ragion di Stato".
Nel primo ambito si colloca il supremo interesse all'integrità territoriale, al mantenimento dell'assetto istituzionale repubblicano, ma che si può spingere sino alla tutela della coesione sociale propria della pacifica convivenza civile.
Tale nozione ristretta che coincide con la Sicurezza della Repubblica è stata efficacemente descritta dalla giurisprudenza della Corte costituzionale, la quale ha spesso collegato la sicurezza nazionale alla nozione di "interesse pubblico supremo", riconoscendole carattere preminente e insopprimibile. In particolare, nella sentenza n. 76 del 1977, la Consulta ha affermato che la sicurezza della Repubblica è un bene primario che può giustificare restrizioni anche significative di altri diritti quando in gioco vi sia l'esistenza stessa dello Stato. Come tale la sicurezza nazionale si configura come un valore di bilanciamento, legittimando misure straordinarie solo se proporzionate, temporanee

2 M. Barberis, *Non c'è sicurezza senza libertà. Il fallimento delle politiche antiterrorismo*, Bologna, Il Mulino, 2017, p. 97.

3 A. Papisca, M. Mascia, *Le relazioni internazionali nell'era dell'interdipendenza e dei diritti umani*, II ed., Padova, Cedam, 1997, p. 338-339.

4 Sul punto si veda: T.F. Giupponi, *I rapporti tra sicurezza e difesa. Differenze e profili di convergenza*, in *Dir. cost.*, 1, 2022, p. 21 ss.; G. De Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 4, 2019, p. 69; M. Valentini, *Sicurezza della repubblica e democrazia costituzionale*, Napoli, Editoriale Scientifica, 2017; P. Bonetti, *Ordinamento della difesa nazionale e costituzione italiana*, Milano, Giuffré, 2000, p. 22-23.

5 Si v. Sistema Di Informazione Per La Sicurezza Della Repubblica, *Glossario intelligence. Il linguaggio degli Organismi informativi*, 2019.

e finalizzate alla salvaguardia della Repubblica democratica. Così, essa non è un fine autoreferenziale, ma un mezzo per garantire la libertà e l'ordine costituzionale. Sulla base del principio di legalità e sulla responsabilità politica del Governo, la sicurezza nazionale si articola in una dimensione preventiva (evitare rischi per l'integrità e la continuità delle istituzioni) e repressiva (neutralizzare minacce attuali).

Nel secondo ambito si individua invece un complesso eterogeneo di attività volte a tutelare la sovranità statale attraverso il perseguimento degli interessi nazionali. Questi rappresentano gli strumenti volti «a tutelare l'indirizzo politico costituzionale, così come assunto dalle forze politiche egemoni in un determinato momento storico, non coincidente (quindi) con l'indirizzo politico delle forze di maggioranza»[6]. Sicché in tale accezione ampia si rivela il contenuto maggiormente politico della nozione di sicurezza nazionale poiché in essa si riscontra la qualificazione politico-discrezionale di un interesse pubblico ad appannaggio del governo e giustificata da una clausola aperta. Qualificazione funzionale che conduce a legittimare forme di intervento regolatorio, amministrativo e financo operativo a tutela degli interessi strategici dello Stato (energia, infrastrutture, economia, informazione), in un'ottica di sicurezza "espansa".

Questa distinzione, pur utile sul piano analitico, non è sempre netta nella prassi. Le trasformazioni del contesto globale, dalla dipendenza tecnologica alla competizione economica, hanno reso porosi i confini tra le due accezioni di sicurezza nazionale. Infatti, lo sviluppo tecnologico e la complessità del sistema di interrelazioni generate dalla rete rendono impossibile non solo una chiara definizione del legame tra bene protetto e spazio di interessenza, ma nel complesso prefigurano ambigue connotazioni della stessa sovranità statuale.

La sicurezza nazionale può essere considerata un bene collettivo complesso: la sua tutela richiede l'interazione di soggetti pubblici e privati, centrali e locali, militari e civili. Essa rappresenta una funzione sistemica, finalizzata a garantire la continuità dello Stato e la sicurezza dei cittadini in senso ampio. In questa prospettiva, la sicurezza nazionale si estende oltre la mera protezione fisica del territorio, includendo la sicurezza economica, la sicurezza tecnologica e la sicurezza informativa.

Tale ampliamento del concetto comporta un duplice effetto: da un lato, la sua politicizzazione in quanto strumento di orientamento dell'azione del governo in ambiti riservati al legislatore; dall'altro, la necessità di giuridificazione progressiva, per evitare che la sicurezza diventi categoria indeterminata e potenzialmente arbitraria.

Su questo terreno la dimensione cibernetica e l'intervento dell'Unione europea assumono un ruolo cruciale. Infatti, il cyberspazio si configura come un dominio strategico in grado di influenzare la stabilità delle istituzioni, la coesione sociale e la competitività economica, ponendo sfide inedite alla tradizionale distinzione tra sicurezza interna ed esterna, tra difesa militare e tutela civile. Proprio la sicurezza cibernetica e la sua regolazione ha mostrato l'ambiguità della nozione giuridica di sicurezza nazionale soprattutto in considerazione della sua portata di ambito di competenza esclusiva rispetto al diritto europeo. La tutela dello spazio cibernetico è infatti il terreno di confronto da una visione tradizionale di difesa dello stato e dei suoi interessi nevralgici e una regolazione europea "espansiva" tesa a invadere ogni spazio

6 Si v. T.G. Giupponi, *I rapporti tra sicurezza e difesa. Differenze e profili di convergenza*, cit., p. 47.

in virtù della natura eminentemente economica di ogni interesse minacciato. Da tale assunto deriva che la sicurezza nazionale potrebbe apparire, al contempo, – parafrasando un celebre *incipit* – "uno spettro" che si aggira nello spazio giuridico europeo ovvero un'ancella degli apparati preposti a una sicurezza cibernetica europea, nella più tradizionale prospettiva funzionalista[7].

2. La sicurezza nel cyberspazio

Il mondo interconnesso in cui viviamo dipende integralmente dalle informazioni, dall'informatica e dalle comunicazioni. L'economia nazionale e la sicurezza stessa degli Stati sono ormai indissolubilmente legati alla stabilità e alla sicurezza del cyberspazio. Come è noto, quest'ultimo viene definito come l'insieme delle reti di comunicazione, sistemi informatici, dati e infrastrutture digitali che consentono la creazione, lo scambio e l'elaborazione di informazioni. Pertanto, esso è un ambiente globale, caratterizzato dall'uso dell'elettronica e delle ICT per creare, immagazzinare, modificare, scambiare e sfruttare informazioni attraverso reti e sistemi interdipendenti. In tale ambiente gli esseri umani e le loro organizzazioni utilizzano le tecnologie per agire e produrre effetti rilevanti sia al suo interno sia nell'ambito di altri domini fisici: un nuovo dominio operativo di natura artificiale, trasversale agli altri quattro domini tradizionali (dominio terrestre, dominio aereo, dominio marittimo, dominio spaziale)[8].

La dimensione cibernetica è generata da quella rete di infrastrutture materiali di collegamento e di comunicazione che, attraverso la tecnologia informatica, mette in contatto tra loro un crescente numero di esseri umani e permette loro di attivare e controllare, da ubicazioni remote, macchine e apparati in tutto il mondo. La sua natura è pertanto ibrida: fisica (*hardware*, cavi*, server*, *data center*) e logica (*software*, algoritmi, protocolli).

Le coordinate di individuazione di una nozione giuridica del cyberspazio devono tenere conto, dunque, dei profili qualitativi e strutturali dello stesso.

Infatti, sul piano strutturale, lo spazio cibernetico si manifesta, invece, come un ecosistema complesso di tre livelli interattivi: quello fisico-infrastrutturale, rappresentato dalle macchine (le architetture delle reti, i *computer*, i *router*); quello logico-informativo rappresentato dal volume dei dati gestiti dalle macchine (*database*, *files*, *software*); quello sociale-cognitivo determinato dall'insieme delle relazioni umane e delle caratteristiche socio-cognitive che possono costituire le identità virtuali (l'indirizzo *e-mail*, il profilo nei *social network*, gli indirizzi IP delle macchine).

Invece, sul piano qualitativo, risulta agevole rilevare che sono principalmente due gli elementi che contraddistinguono lo spazio cibernetico rispetto a quello fisico. In primo luogo, esso è qualificato dall'indeterminatezza spaziale in quanto privo di confini fisici e di territorialità giuridica. Infatti, tutte le operazioni avvengono in una dimensione extraterritoriale che rende particolarmente problematici i parametri di attivazione della sovranità statale nella sua componente regolativa e coercitiva. In secondo luogo, esso si connota per essere in permanente evoluzione poiché l'innovazione tecnologica continua (*cloud*, intelligenza artificiale, *Internet*

7 Questa prospettiva è il nucleo fondante della tesi sostenuta da M. Matassa, *La sicurezza cibernetica come funzione pubblica*, Milano, FrancoAngeli, 2025.

8 L. Martino, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, 1, 2018, p. 61 ss.

of Things, *quantum computing*) produce mutamenti costanti nella morfologia del cyberspazio. Sicché in conseguenza di tale mutazione le regole giuridiche soffrono di una fisiologica rapida senescenza applicativa.
Dunque, quale un ecosistema condiviso i tentativi di regolazione richiedono cooperazione multilivello, standard tecnici condivisi e coordinamento normativo internazionale. Tuttavia, questa visione universalistica si scontra con la crescente nazionalizzazione del digitale, ossia con l'uso del cyberspazio come strumento di potere e come proiezione della sovranità statale. Attraverso il controllo delle infrastrutture, dei dati e delle piattaforme, gli Stati e le grandi imprese tecnologiche esercitano influenza politica, economica e culturale[9].
In questo senso la capacità di uno Stato di assicurare l'autonomia decisionale, la protezione dei propri dati e la continuità dei servizi critici diventano espressione di una sovranità digitale[10] che inevitabilmente diventa espressione della sicurezza nazionale. D'altra parte, la dipendenza dalle tecnologie rende gli Stati vulnerabili. La stessa rete che connette e abilita l'economia può essere strumentalizzata per attacchi, spionaggio o disinformazione. Questa duplicità — potere e vulnerabilità — costituisce il cuore del problema giuridico della sicurezza cibernetica. Il cyberspazio è, in sintesi, un dominio strategico asimmetrico, dove attori statali e non statali possono agire con costi ridotti e impatti potenzialmente devastanti.
Appare opportuno sottolineare, però, che in tale dominio la sicurezza assume un diverso connotato a seconda se la si osservi come sicurezza "nel" cyberspazio ovvero come sicurezza "del" cyberspazio.
Nella prima prospettiva la *cybersecurity* può essere intesa come quel complesso di attività volte a garantire la confidenzialità, l'integrità e la disponibilità dei dati. In particolare, l'idea della 'sicurezza nel ciberspazio' può essere ricollegata alla tutela diretta delle informazioni contenute nello spazio cibernetico possedute da utenti, aziende e organizzazioni in un'ottica strettamente correlata sia alla protezione e al trattamento dei dati, sia ai temi propri del diritto della *privacy*. In questo senso, la *cybersecurity* diventa anche tutela della persona, non solo dell'infrastruttura: la violazione di un database o di un sistema informativo può compromettere la dignità e l'autonomia degli individui. La sicurezza "nel" cyberspazio è dunque micro-sistemica poiché essa è una condizione di base, ma non esaurisce la dimensione pubblica della sicurezza. Infatti, nell'ottica analizzata il problema della sicurezza riguarda la protezione di ogni singolo nodo della rete, di ogni transazione digitale e di ogni archivio di dati.
In termini generali si può affermare che la sicurezza "nel" cyberspazio potrebbe configurarsi come una sorta di ordine pubblico digitale in cui l'azione di protezione riguarda le relazioni umane digitali e i beni digitali. L'avvento della rivoluzione digitale ha determinato il sorgere di nuovi conflitti e ha reso possibili nuovi comportamenti illeciti, che violano o minacciano gravemente sia i diritti e gli interessi tradizionali di persone, gruppi e collettività sia quelli nuovi che proprio nella dimensione cibernetica trovano il loro necessario riconoscimento. Come è stato evidenziato, «accanto alle nuove forme di prevaricazione e di soggezione, correlate a concentrazioni straordinarie di poteri e di

9 In tema si veda M. Betzu, *I baroni del digitale*, Napoli, Editoriale scientifica, 2021.

10 B. Carotti, *Uniformità e autonomia nella sicurezza cibernetica*, in *Cybersecurity e istituzioni democratiche: un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, a cura di P. Heritier, S. Rossa, in *Teoria e Critica della ragione sociale*, 2, 2024, p. 39 ss.

corrispondenti forze e capacità di intimidazione, di controllo, di condizionamento delle informazioni, della volontà e delle scelte delle singole persone e dei gruppi sociali, si sono sviluppate e si sviluppano nuove forme di aggregazione, di condivisione, di partecipazione, che utilizzano le inedite possibilità di incontro, scambio e creazione di comunità e gruppi di interessi, con obiettivi e valori comuni»[11].

In tale contesto, la criminalizzazione di tali condotte è avvenuta secondo due linee di sviluppo: da una parte, tramite l'estensione di talune fattispecie già esistenti che trovano nello spazio cibernetico un ambiente differenziato; dall'altra mediante la creazione di ipotesi specifiche, in considerazione delle peculiarità intrinseche della dimensione digitale. Ciò ha permesso la classificazione dei *cyber-crimes* a seconda che si tratti di reati comuni commessi mediante lo strumento informatico (per esempio, la diffamazione sul *blog*), ovvero si tratti di fattispecie nelle quali l'elemento informatico costituisca un elemento imprescindibile e caratterizzante della fattispecie, nel rispetto delle esigenze di tassatività delle norme incriminatrici[12].

Il tema riguarda l'attività di repressione degli illeciti e di prevenzione delle condotte lesive, che impongono una rivisitazione delle categorie tradizionali del diritto penale e spingono inevitabilmente a immaginare un ambito operativo di interrelazioni tra forze dell'ordine e autorità di sicurezza che esorbita i confini statuali. Si tratta di attività amministrative e giudiziarie espressioni di poteri sovrani, la cui efficacia risulta pregiudicata dalla collocazione territoriale dell'autore di simili illeciti, ammesso che lo si possa individuare, e dal fatto che l'intermediario privato che gestisce la rete ha la disponibilità esclusiva dei dati e dei contenuti sui quali si intende intervenire. In questa prospettiva, soggetti privati, titolari di piattaforme e *providers,* esercitano poteri preventivi e sanzionatori nei confronti dei propri utenti, spesso in maniera sommaria e senza alcuna garanzia procedurale.

Si è pertanto in presenza di un quadro complesso in cui, a fronte di una incrementale domanda di sicurezza generata dai pericoli e dalle minacce provenienti da un mondo virtuale, si registra un indebolimento delle tradizionali funzioni pubbliche statuali e una loro contaminazione forzata. E ciò in quanto il mondo socio-politico ha delegato al mondo privato-imprenditoriale il disegno e la gestione dell'architettura cibernetica, la quale integra una dimensione della sicurezza avulsa dalle categorie giuridiche di cui si è sempre nutrita, ossia la legittimazione, la polarità privato-pubblico, il nesso di spazialità-territorialità.

Nella prassi la prevenzione legata all'ordine pubblico digitale, ossia la sicurezza "nel" cyberspazio, si è concentrata prevalentemente sulla tutela della riservatezza dei dati, che si

11 Si v. L. Picotti, *Diritto penale e tecnologie informatiche: una visione di insieme*, in *Cybercrime*, diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Torino, Utet, 2019, p. 38.

12 Si tratta di condotte che da oltre un trentennio sono oggetto di normazione sovranazionale e internazionale, che ha trovato il suo suggello più importante nella Convenzione di Budapest sulla criminalità informatica del 2001, recepita in Italia con la legge 18 marzo 2008, n. 48. Obiettivo di questo trattato è quello di perseguire una politica criminale comune e promuovere la cooperazione internazionale, tenendo in considerazione i profondi cambiamenti dovuti all'evoluzione della tecnologia digitale e alla globalizzazione delle reti informatiche e coinvolgendo nella prevenzione e nell'accertamento dei reati informatici non solo gli Stati, ossia organismi pubblici, ma anche il settore privato. L'ordinamento euro-unitario ha seguito la medesima traiettoria muovendosi, dapprima, con strumenti generali di armonizzazione come le decisioni quadro e, dopo il Trattato di Lisbona del 2008, con direttive specifiche, in attuazione a quanto previsto dall'art. 83.1 TFUE, che hanno determinato importanti sentenze della Corte di giustizia come quella sul caso Google del 2014. In argomento si veda R. Flor, *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di internet*, 3, 2019, p. 457.

sostanzia nella garanzia che il trattamento dei dati sia effettuato in modo da assicurare la sovranità delle informazioni, ossia la capacità di controllare l'integrità, la disponibilità e la circolazione delle informazioni digitali[13].
La tutela dei dati è la precondizione per limitare il crimine informatico e la protezione e la responsabilizzazione del trattamento degli stessi diventa prioritario fattore di sicurezza per prevenire il fenomeno[14].
Com'è noto, l'azione preventiva, regolativa e amministrativa è dettata dalla disciplina euro-unitaria disposta dal Regolamento (UE) 679/2016 (il cd. GDPR), mentre l'azione repressiva si indirizza verso condotte criminali tese a compromettere la riservatezza dei dati, attraverso una loro esposizione al rischio di apprensione da parte di soggetti terzi, a determinare la perdita di disponibilità dei medesimi da parte del titolare, oppure a causare una menomazione della loro integrità e autenticità[15].
La sicurezza "del" ciberspazio, invece, si colloca su un livello macro-sistemico, poiché l'oggetto della tutela non è il dato o l'utente, ma la funzionalità dell'intero ecosistema digitale da cui dipende il funzionamento della società e dello Stato. Pertanto, la sicurezza "del" cyberspazio diventa una declinazione della sicurezza nazionale.
Il cyberspazio è esso stesso un bene giuridico: un'infrastruttura critica da proteggere perché il suo collasso metterebbe in pericolo la vita civile ed economica del Paese. In questo senso, la sicurezza è indirizzata non solo alla protezione delle reti e dei sistemi informativi, ma anche di tutti i beni e le persone fisiche bersagli di attacchi informatici. Sicché il *cyberspace* può essere inteso come bene giuridico tutelato dalla sicurezza informatica in via soltanto mediata e indiretta, in quanto il fine ultimo perseguito dall'attività pubblica si ravvisa nella protezione delle persone e dei beni del mondo reale messi in pericolo dalla minaccia cibernetica.
Come protezione degli interessi minacciati da condotte lesive nei confronti dei sistemi e delle reti informatiche la sicurezza del cyberspazio denota un ambito che coinvolge l'insieme delle tecnologie e delle misure di risposta e mitigazione progettate per tutelare reti, computer, programmi e dati da attacchi, danni o accessi non autorizzati, in modo da garantire riservatezza, integrità e disponibilità. Ed è proprio tramite la individuazione degli interessi primari da proteggere che la sicurezza cibernetica si presenta come una funzione pubblica, la quale muovendo da un controllo delle infrastrutture tecnologiche tenta di inibire pericoli e minacce sulle persone.
Questa prospettiva si collega al concetto di sicurezza nazionale in senso debole, ma con implicazioni di sicurezza "forte". La compromissione di reti energetiche, sanitarie, finanziarie o militari tramite attacchi informatici non produce solo danni economici, ma può minacciare la salus rei publicae.
Al riguardo, richiamando la dottrina statunitense si è parlato di *cyber-physical security*[16]: l'interdipendenza tra sistemi digitali e strutture materiali implica che un attacco nel cyberspazio può avere effetti fisici e sociali concreti (si pensi ai blackout elettri-

13 A.C. Amato Mangiameli, *Reato e reati informatici. Tra teoria generale del diritto e informatica giuridica*, in *I reati informatici. Elementi di teoria generale e principali figure criminose*, a cura di A.C. Amato Mangiameli, G. Saraceni, II ed., Torino, Giappichelli, 2019, p. 1 ss.

14 C. Bigotti, *La sicurezza informatica come bene comune implicazioni penalistiche e di politica criminale*, in *La giustizia penale nella "rete"*, a cura di R. Flor, D. Falcinelli, S. Marcolini, Milano, DIPLap Editor, 2015, p. 116.

15 V. Manes, F. Mazzacuva, *GDPR e nuove disposizioni penali del Codice privacy*, in *Dir. pen. proc.*, 2, 2019, p. 168.

16 Si v. M. Matassa, *La sicurezza cibernetica come funzione pubblica,* cit., p. 54.

ci o al blocco del traffico aereo causato da *malware*).
Quale funzione pubblica correlata alla sicurezza nazionale la sicurezza "del" cyberspazio ha trovato una regolazione multilivello che rivela alcune ambiguità sistematiche e una complessità derivante dalla sovrapposizione di ambiti di normazione funzionalmente diverse.

3. Breve ricognizione della regolazione della sicurezza cibernetica tra ordinamento europeo e diritto italiano

La regolazione della sicurezza cibernetica nasce con differenti caratteristiche funzionali in ambito europeo e in ambito nazionale. In ambito europeo con uno sviluppo ormai venticinquennale[17] lo scopo originario della regolazione è stato esclusivamente la tutela del funzionamento del mercato e quindi la protezione delle imprese e dei consumatori rispetto a minacce provenienti prevalentemente dalla criminalità informatica. A conferma di ciò risulta agevole rilevare come la dir. (UE) 2016/1148 (c.d. NIS) individui quali soggetti bisognosi di tutela gli operatori di servizi essenziali e nei fornitori di servizi digitali, non includendo tra questi gli operatori pubblici e privati operanti nel settore della pubblica amministrazione, dell'ambiente, dell'alimentare, di quello chimico e nucleare. L'Italia ha recepito la direttiva NIS con il decreto legislativo n. 65/2018.
L'ordinamento italiano, tuttavia, ha avvertito la necessità di rafforzare l'impianto normativo in un'ottica peculiare e differente, incardinando le questioni della sicurezza cibernetica prevalentemente sull'attività correlata al Sistema di Informazione e Sicurezza della Repubblica[18]. In tal senso, in presenza di una imprevista recrudescenza dei fenomeni di criminalità informatica e di minacce ai sistemi critici si è registrata, a partire dal 2013 un'embrionale regolazione (d.p.c.m. 24 gennaio 2013, cd. Decreto Monti), alla quale ha fatto seguito una produzione normativa alluvionale e multilivello, che ha visto nel decreto-legge n. 105/2019, con il quale si è creato il Perimetro informatico, e nel decreto-legge n. 82/2021, che ha istituito l'Agenzia per la Sicurezza Cibernetica, due momenti fondamentali di definizione del modello istituzionale di tutela delle reti, dei sistemi e delle comunicazioni elettroniche.
L'architettura complessiva che se ne ricava si caratterizza, da una parte, per la stretta connessione tra la nozione di sicurezza nazionale e quella di ordine e sicurezza pubblica, e dall'altra per la partecipazione attiva delle infrastrutture critiche, gestite sia da soggetti pubblici che privati, alle attività di protezione della cybersicurezza[19].
In particolare, l'istituzione del Perimetro guarda alla protezione di reti, sistemi informatici e servizi informativi necessari allo svolgimento di funzioni o alla prestazione di servizi ritenuti essenziali in quanto condizioni per garantire l'indipendenza, l'integrità e la sovranità della Repubblica[20]. Infatti, l'art. 1, comma 1, del d.l. n. 105/2019 include

17 L'avvio si registra in un documento della Commissione 2000 e poi con la istituzione dell'ENISA nel 2004, evolvendosi, poi, in diversi interventi settoriali, peraltro non particolarmente incisivi, sino all'adozione della dir. (UE) 2016/1148 (cd. NIS).

18 Per una ricostruzione al riguardo si veda T.F. Giupponi, *Il Governo nazionale della cybersicurezza, in Quad. Cost.*, 2, 2024, p. 277 ss.

19 F. Serini, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021,* in *Federalismi.it,* 12, 2022, p. 268.

20 M. Macchia, G. Sferrazzo, *Sicurezza e rischio tecnologico. La funzione di cybersecurity*, in *Dir. amm.*, 1, 2025, p. 120 ss.

all'interno del Perimetro le amministrazioni pubbliche, gli enti e gli operatori nazionali pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività ritenute fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero dal cui utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. L'innovazione più rilevante del Perimetro risiede nella sua visione integrata: esso non si limita a regolare le infrastrutture tecnologiche, ma mira a proteggere l'insieme delle funzioni vitali dello Stato. La sua logica è eminentemente funzionale, non settoriale: ciò che conta non è il tipo di soggetto, ma la rilevanza della funzione svolta per la sicurezza nazionale[21].

Si introduce un meccanismo di tutela selettiva: individua soggetti pubblici e privati che esercitano "funzioni essenziali dello Stato" o erogano "servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi nazionali". Tali soggetti devono rispettare specifici requisiti di sicurezza e notificare incidenti informatici di rilievo.

Così, di fronte ai pericoli derivanti dalle minacce informatiche all'assetto economico e sociale del Paese provenienti da minacce o attacchi informatici la risposta dell'ordinamento è stata la creazione di un "fortino digitale" all'interno del quale esercitare la sovranità statuale di difesa e sicurezza.

Tale approccio è confermato dal d.l. n. 82/2021 sebbene si attribuiscano per la prima volta funzioni amministrative attinenti alla sicurezza cibernetica a soggetti esterni al SISR[22].

L'adozione della direttiva (UE) 2022/2555 (cd. NIS 2) nonché di una serie di provvedimenti regolatori correlati o integrativi ha propiziato una complessità del sistema regolativo generato dalla sovrapposizione di ambiti e di funzioni tra il livello interno e quello europeo.

Pur mantenendo lo spirito originario, la NIS 2 estende notevolmente l'ambito soggettivo e settoriale di applicazione, introducendo una classificazione tra "soggetti essenziali" e "soggetti importanti". Essa include, per la prima volta, numerose amministrazioni pubbliche centrali, le infrastrutture *cloud*, i fornitori di servizi gestiti, le piattaforme digitali e le catene di approvvigionamento critiche.

La direttiva introduce un sistema di obblighi più stringenti: *i*) adozione di politiche di gestione del rischio basate su standard minimi europei; *ii*) obblighi di notifica più rapidi e completi; *iii*) possibilità di sanzioni significative in caso di inadempienza; *iv*) armonizzazione dei poteri di vigilanza delle autorità nazionali.

La NIS2 rappresenta un passaggio da un modello di compliance reattiva a uno di resilienza preventiva, spostandosi dalla mera protezione alla capacità di risposta e recupero improntata a un approccio *risk-based*.

Nel complesso sembra corretto ritenere che la finalità di tutela del "mercato interno" ceda il passo a una vera e propria politica di sicurezza comune sebbene nell'ottica di un concetto di sicurezza economica[23] "espansa" che - almeno formalmente - risulta coerente con la clausola di cui all'art. 4, par. 2,

21 Al riguardo si veda B. Carotti, *Sicurezza Cibernetica e Stato-nazione*, in *Giornale di diritto amministrativo*, 5, 2020, p. 629 ss.

22 M. Macchia, G. Sferrazzo, *Sicurezza e rischio tecnologico. La funzione di cybersecurity,* cit., p. 136.

23 F. Serini, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, in *MediaLaws*, 3, 2023, p. 185; S. Poli, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *I Post di AISDUE*, III, 20 dicembre 2021, p. 78-79.

del Trattato in base al quale la sicurezza nazionale rimane esclusiva competenza degli Stati membri.
In un'ottica integrata si registra una evidente ibridazione di un modello regolativo europeo in cui convivono le esigenze più tradizionali della sicurezza statuale con quelle di continuità del mercato. Ibridazione che si giustifica della stretta interrelazione tra ragioni economiche e tenuta socio-istituzionale che la pervasività della tecnologia reca con sé e che segna l'avvio di una politica di sicurezza economica europea, in cui resilienza e competitività si saldano.
A conferma di ciò si evidenziano anche due ulteriori interventi approvati contestualmente alla NIS2, ossia il Regolamento (UE) 2022/2554 (noto come *Digital Operational Resilience Act* o DORA)**,** adottato con la finalità di introdurre delle misure speciali volte a garantire un più elevato livello di sicurezza cibernetica nel settore finanziario dell'Unione; e la dir. (UE) 2022/2557 (denominata *Critical Entity Resilience* o CER), la quale va inquadrata in una prospettiva più ampia, ossia quella della tutela delle "infrastrutture critiche" indispensabili per il mantenimento delle funzioni sociali ed economiche essenziali per la vita dell'Unione e per la sicurezza dei suoi cittadini.
Il legislatore italiano ha dato attuazione alla normazione europea non perdendo tuttavia le caratteristiche del suo impianto originario. In particolare, il decreto legislativo n. 138/2024, che ha recepito la direttiva NIS 2, all'art. 2, lett. *s*) qualifica la sicurezza cibernetica come l'insieme delle attività previste dall'art. 1, comma 1 lett. *a*) del decreto legislativo n. 82/2021. Sicché tutta la regolazione introdotta dalla NIS 2 non incide su un modello di sicurezza basato sull'insieme delle «attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico».

4. Alla ricerca di un centro di gravità

Alla luce di questo quadro normativo composito non può che condividersi l'opinione di chi ritiene che la sicurezza cibernetica può essere rappresentata come una funzione pubblica multilivello composta da tre diversi cerchi concentrici: il primo racchiude quel nucleo di funzioni intangibili dello Stato rivolte alla tutela della sicurezza nazionale e della difesa (*salus rei publicae*); il secondo tutte quelle funzioni poste al crocevia tra la tutela della sicurezza nazionale e la tutela del mercato interno che possono essere sintetizzate nella comune volontà di tutelare la 'sicurezza economica' o 'l'interesse nazionale', in cui l'*enforcement* resta di competenza tendenzialmente nazionale ma gli standard risultano anche di provenienza UE (in cui la *salus rei publicae* incontra la *salus oeconomica*); il terzo, dal carattere residuale, racchiude invece tutte quelle funzioni di matrice esclusivamente comunitaria che, pur tutelando in via mediata la sicurezza degli Stati membri chiamati ad applicare la relativa disciplina, sono circoscritte alla tutela del mercato interno dell'Unione (*salus oeconomica*)[24].
Mentre il primo e il terzo livello rinviano a impianti normativi chiari nei loro contenuti fun-

24 Si v. M. Matassa, *La sicurezza cibernetica come funzione pubblica*, cit., p. 307.

zionali, organizzativi e prescrittivi. Si pensi agli attacchi informatici a infrastrutture militari o a obiettivi sensibili quali le istituzioni governative e non (tipicamente rientranti nel nocciolo duro del SISR) ovvero di minacce e pregiudizi rispetto alla sicurezza informatica o dei sistemi informativi degli attori di mercato (pienamente ascrivibili al corretto funzionamento del mercato secondo i parametri europei). Invece non pochi problemi applicativi presenta il secondo livello in cui con una ampia scala di sfumature si riscontrano le interrelazioni tra sicurezza economica e dinamica di protezione degli interessi nazionali ritenuti fondamentali ovvero connessi a infrastrutture critiche.

Correndo il rischio di semplificare una situazione di oggettiva complessità sistematica si può ritenere che, dal punto di vista regolativo, nella zona grigia l'elemento discriminante vada individuato nella collocazione del soggetto regolato all'interno del Perimetro[25].

Di fronte alla fisiologica a-territorialità dello spazio cibernetico si individua una sorta di "area di territorializzazione effettuale" dello stesso, in modo da definire un ambito di tradizionale autorità ed esercizio dei poteri correlati[26]: una funzione di tutela che si lega alla natura nazionale (e quindi direttamente o indirettamente territoriale) degli interessi tutelati.

Ciò posto, il "fortino digitale" artificialmente immaginato segna il confine tra la prevalenza del diritto europeo e la riserva di esclusività in materia di sicurezza nazionale. Tale lettura conferisce alla disciplina italiana e alle scelte amministrative correlate uno spazio operativo e derogativo del livello di tutela offerto dalla normativa europea. Occorre precisare che si tratta di una portata derogativa funzionalizzata a una maggiore protezione e al discrezionale ulteriore allargamento dell'area dei soggetti perimetrati. Sicché si potrebbe ritenere che la regolazione comunitaria costituisca il minimo di tutela ritenuto necessario e imprescindibile lasciando alle scelte governative un innalzamento ulteriore della protezione.

Alla luce di quanto detto risulta agevole rilevare che sussiste un interesse pubblico che denota una funzione statuale: quello di approstare, contestualmente, mezzi di protezione a favore dello Stato e dei suoi soggetti, relativi alla sopravvivenza, all'incolumità e all'integrità politica, alla stabilità economica e al benessere sociale derivanti dall'utilizzo dello spazio cibernetico.

La funzione amministrativa 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.

In questa prospettiva la sicurezza cibernetica si presenta come una funzione di carattere composito in cui convivono almeno tre funzioni interdipendenti: *i*) la difesa da minacce attuali o potenziali (attacchi informatici, intrusioni, sabotaggi); *ii*) la prevenzione ossia la riduzione del rischio sistemico, attraverso norme, procedure e cultura della sicurezza; e in ultimo *iii*) la resilienza, vale a dire la capacità di resistere, assorbire e ripristinare la funzionalità dei sistemi dopo un incidente. In questo senso, la sicurezza cibernetica si configura come una funzione amministrativa dinamica, orientata non solo alla difesa, ma alla governance del rischio. Sembra corretto ritenere che la disciplina europea gioca un

25 E. Buoso, *Ritorno al futuro: il perimetro di sicurezza nazionale cibernetica*, in *Cybersecurity e istituzioni democratiche: un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, a cura di P. Heritier, S. Rossa, in *Teoria e Critica della ragione sociale*, 2025, 1, p. 33 ss.

26 Sul punto si veda anche E. Longo, *Il diritto costituzionale e la cybersicurezza*, in *Rass parl.*, 66, 2024, p. 377.

ruolo solo sul piano della prevenzione e su quello della resilienza poiché la difesa rimane pienamente, almeno fino ad oggi, nello spazio di azione riservato agli Stati membri.
Orbene, sembra chiaro che l'esatta declinazione cibernetica della sicurezza nazionale rispetto al rapporto tra fonti europee e ambito interno si colloca sul crinale, non sempre agevole da tracciare, che separa la difesa e resilienza: ossia, indugiando sulla metafora, sulla distinzione dei compiti tra chi presidia il fortino e chi provvede alla solidità delle sue mura. La difesa dei "bastioni digitali" si configura quale espressione di una funzione tradizionale in chiave digitale: difendere le istituzioni, le infrastrutture, la parte più intima e vitale dei gangli sociali ed economici da attacchi o minacce probabili provenienti *extra-moenia*. Si tratta di un'attività, la *cyber-defence* che riguarda il modo con cui fronteggiare i nuovi conflitti cibernetici e nella quali si misura la capacità dello Stato di proteggere sé stesso, le proprie istituzioni e le strutture economico-sociali ritenute essenziali, contro minacce, spionaggio, sabotaggio, terrorismo ecc.
Al riguardo è stato evidenziato che la difesa cibernetica ha una sua specificità e importanza da tre punti di vista.
Il dominio cibernetico può essere considerato un terreno di scontro ad alta intensità nel quale non è mai stato finora dichiarato un conflitto, ma in cui gli attacchi sono numerosi, vengono attuati da una pluralità di attori statali o non, e possono portare all'attivazione della clausola di difesa collettiva della Nato, con ripercussioni anche nel "mondo reale".
La prevenzione e la resilienza con le quali si manutengono le strutture e si assorbono i colpi subiti puntellando e rafforzando le "mura" è attività complessa e variegata. In particolare la resilienza in ambiente digitale si configura come un'azione sostanzialmente cooperativa, comprensiva di interventi di ripristino, di assistenza e di prevenzione destinata a integrare responsabilità pubbliche e responsabilità private e, soprattutto, ad assicurare un coordinamento per fare funzionare al meglio l'obiettivo comune, quello di non pregiudicare il funzionamento di servizi essenziali o la disponibilità e la interoperabilità dei dati che a essi si riferiscono e che sono il presupposto stesso per la comune vita civile.
In senso digitale la resilienza si ricollega alla capacità stessa delle infrastrutture, delle reti e dei sistemi informatici di resistere, di adattarsi e di recuperare dopo possibili eventi critici, siano essi attacchi informatici, ma anche eventi critici che possano insorgere sul piano tecnico. Tale concetto presuppone così, e comprende, una serie di interventi cooperativi estesi tra enti pubblici e privati[27], volti proprio a garantire la continuità operativa e la sicurezza dei servizi essenziali.
La resilienza digitale implica, cioè, essenzialmente l'adozione di misure preventive, la rapidità nella risposta agli incidenti come alle criticità e infine la capacità di ripristinare rapidamente tutte le funzionalità compromesse, per mantenere inalterata la fiducia degli utenti e la protezione e l'affidabilità e insieme la disponibilità dei dati indispensabili per le relazioni individuali, economiche[28].
Risulta agevole rilevare che questa attività,

27 Al riguardo, si veda L. Previti, *Convergenze e deviazioni in materia di cybersicurezza: implicazioni sistematiche e nuovi interrogativi*, in *Cybersecurity e istituzioni democratiche: un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale,* a cura di P. Heritier, S. Rossa, cit., p. 109 ss.; S. Rossa, *Cybersicurezza e Pubblica amministrazione*, Torino, Giappichelli, 2023, p. 167 ss.

28 In tema si veda M. A. Rizzi, F. Serini, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano,* in *Rivista italiana di informatica e diritto*, 2, 2024, p. 125 ss.

pressoché integralmente governata dalle fonti europee sia il presupposto fondativo dell'incidenza della protezione offerta dalla *cyber defence*, sicché appare ragionevole ritenere che questa ultima – l'*hard core* del potere statuale – si caratterizzi vieppiù da spazi regolativi europei, i quali, inevitabilmente stanno superando i pretestuosi e fantomatici argini della sicurezza economica. Insomma, si può concludere che si sta assistendo a una trasformazione che potrebbe essere epocale, ossia una sicurezza nazionale che in ambito cibernetico comincia a declinarsi come sicurezza europea. In questo settore si sta forse raggiungendo un risultato al quale non si è arrivati con le politiche di difesa e sicurezza comuni nel mondo fisico.

The cyber dimension of national security between old ambiguities and new challenges

Abstract:

The article examines the transformation of national security in its cyber dimension, highlighting the structural ambiguities of a legal notion traditionally lacking a positive definition and now undergoing a profound functional reconfiguration. National security is reconstructed both as a supreme public good and as an "open" legal category, oscillating between a core sphere of State survival and a broader area of protection of strategic national interests. Within this framework, cyberspace emerges as an autonomous and transversal strategic domain, characterised by territorial indeterminacy, continuous technological evolution and the hybridisation of physical and logical dimensions. The article systematically distinguishes between security "in" cyberspace, concerning the protection of data and digital relationships, and security "of" cyberspace, conceived as a direct expression of national security aimed at safeguarding the digital ecosystem as a critical infrastructure for civil, economic and institutional life. Cybersecurity, conceived as a composite public function structured around defence, prevention and resilience, is progressively transforming national security into a form of European security, foreshadowing a possible structural shift in the traditional paradigms of sovereignty and state protection.

Parole chiave: Sicurezza nazionale – Sicurezza cibernetica – Cyberspazio

Keywords: *National security – Cybersecurity – Cyberspace*