
aracne

Classificazione Decimale Dewey:

340.0285 (23.) DIRITTO. Elaborazione dei dati

GINO **FONTANA**

SOGGETTI PRIVATI E PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

GLI ELEMENTI ESSENZIALI DELLA CYBERSICUREZZA DAI VIZI DELLA VOLONTÀ AI REATI INFORMATICI

AGGIORNATO ALLA LEGGE 28 GIUGNO 2024, N. 90

aracne

ISBN
979–12–218–1869–7

PRIMA EDIZIONE
ROMA 28 GIUGNO 2025

A mio padre uomo laborioso, tenace e visionario
il cui pensiero ha reso di me ciò che sono.
Alla mia famiglia il cui sostegno rappresenta la mia forza

INDICE

INTRODUZIONE

L'evoluzione delle minacce informatiche e la crescente digitalizzazione impongono ai governi una maggiore attenzione alla sicurezza cibernetica. In Italia, la legge del 28 giugno 2024 n. 90 ha introdotto misure specifiche e un ampliamento del cosiddetto "perimetro di sicurezza nazionale cibernetica" con l'obiettivo di rafforzare la protezione delle infrastrutture critiche e delle reti, di stabilire obblighi chiari per le aziende e individuando nuove fattispecie di reati informatici. Oltre a definire i requisiti di base per la cybersicurezza, la normativa affronta aspetti complessi come i "vizi della volontà" nelle attività digitali inaugurando, così, una nuova fase nella gestione dei rischi e delle responsabilità cibernetiche.

In risposta alla Direttiva NIS2 del 2022, che aveva aggiornato e ampliato la precedente direttiva NIS (2016) e introdotto nuovi standard e misure per garantire un livello elevato e uniforme di sicurezza delle reti e dei sistemi informativi in l'Unione Europea, alla L. n. 90/2024 fanno eco nuove leggi in materia emanate da grandi *player* internazionali come gli Stati Uniti, la Cina e la Russia. L'evoluzione del panorama normativo, tuttavia, lungi dal potersi ritenere che abbia raggiunto un punto di equilibrio, si presenta costantemente *in fieri,* di conseguenza le crescenti minacce informatiche, potenziate dall'uso dell'intelligenza artificiale, stanno spingendo i legislatori globali a introdurre normative sempre più stringenti per proteggere cittadini e istituzioni.

Secondo l'ultimo *Global Security Outlook,* pubblicato dal *World Economic Forum,* il 60% dei dirigenti ha espresso la convinzione che

adeguate normative sulla sicurezza informatica e sulla privacy possano ridurre efficacemente i rischi informatici i quali, secondo i rilevamenti di autorevoli osservatori internazionali, continuavano ad aumentare numericamente e qualitativamente anno dopo anno. I legislatori di tutto il mondo, dunque, si sono trovati nella condizione di dover emanare nuove normative, alcune delle quali hanno rafforzato le disposizioni emanate in precedenza, pensate per aumentare il livello di protezione della sicurezza informatica in modo da ostacolare efficacemente le crescenti minacce informatiche.

La cybersicurezza, dunque, rappresenta, oggi, uno dei temi più urgenti e complessi per governi, aziende e cittadini che rende necessarie norme e strategie efficaci per la protezione dei sistemi digitali. In virtù di questa consapevolezza il presente saggio si pone l'obiettivo di esplorare le principali questioni legate alla sicurezza cibernetica, offrendo un'analisi approfondita e aggiornata della normativa sia europea sia italiana, senza tralasciare qualche riflessione su quanto avviene al di fuori del confini del Vecchio Continente.

Nel Capitolo I, *Un focus sulla cybersicurezza,* viene fornita una panoramica globale della cybersicurezza, partendo dalla definizione del concetto e dai suoi elementi fondamentali; viene analizzato il quadro internazionale ed europeo, con particolare attenzione agli investimenti e alle normative dell'Unione Europea, come la *Direttiva NIS2* e l'*Atto sulla Sicurezza Cibernetica,* volte a garantire resilienza e protezione contro le minacce digitali.

Il Capitolo II, *Il quadro italiano della cybersecurity: dal perimetro nazionale della sicurezza cibernetica alla l. n. 90/2024,* si concentra sulla risposta italiana alla sfida della cybersicurezza, illustrando come il Paese abbia strutturato la propria strategia nazionale e l'applicazione di normative fondamentali; tra questi aspetti, figurano il *Perimetro di Sicurezza Nazionale Cibernetica*, l'*Autorità Nazionale per la Cybersicurezza* (ACN), e l'integrazione della nuova legge n. 90 del 2024 che è arrivata ulteriormente a consolidare il previgente quadro normativo, includendo nuovi soggetti privati nella tutela nazionale.

Infine, il Capitolo III, *Vizi della volontà e reati informatici,* esplora un aspetto cruciale del problema, ossia la connessione tra i "vizi della volontà" e i reati informatici. Dall'*hacking* al *phishing* al *ransomware*,

il capitolo esplora le principali minacce e le normative di prevenzione e repressione, evidenziando le modalità con cui si manifestano e il ruolo del dolo e dell'inganno. La riflessione si estende anche all'ambito europeo ed extraeuropeo, offrendo uno sguardo comparativo sulle diverse azioni adottate in risposta alle minacce presenti e future.

CAPITOLO I

UN FOCUS SULLA CYBERSICUREZZA

1.1. Alla ricerca di una definizione: dalla pubblica sicurezza alla sicurezza cibernetica

La sicurezza cibernetica (*cyber security)* può essere considerato l'ultimo tassello di un complesso ingranaggio che lega, oggi più che mai, in un'unica equazione 'pubblica sicurezza' e 'sicurezza nazionale' e questo in virtù del fatto che, ormai, gran parte delle infrastrutture critiche e delle attività della società del terzo millennio dipendono dal cyberspazio[1]. Il crescente utilizzo di tecnologie digitali e l'interconnessione delle infrastrutture critiche rendono il cyberspazio un dominio essenziale per la stabilità interna e la difesa nazionale[2].

Partendo dall'analisi del concetto di 'pubblica sicurezza' emerge come, nel tempo, esso si sia modificato nel tentativo di adeguarsi alle profonde trasformazioni che, via via, interessavano la società e le forme di Stato. Risulta, tuttavia, evidente anche che il suo nucleo fondante sia rimasto immutato, venendo a modificarsi aspetti più estetici e formali,

(1) R. A. Clarke, R. K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*, Penguin Press, Londra, 2019; U. Gori (a cura di), *Cyber Warfare 2017. Information, Cyber e Hybrid Warfare: contenuti, differenze, applicazioni*, Franco Angeli, Milano, 2018.

(2) A. Rotondo, *Cyber security e protezione delle infrastrutture critiche: l'efficacia del modello europeo,* in S. Marchisio, U. Montuoro (a cura di), *Lo spazio cyber e cosmico*, Giappichelli, Torino, 2019, pp. 115-136; G. Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*, Butterworth-Heinemann, Oxford, 2015.

e questo in virtù del fatto che il suo fine è rimasto sempre, e comunque, quello di assicurare l'ordine della vita sociale[3]. Obiettivo delle azioni e delle attività di 'pubblica sicurezza', infatti, resta quello di anticipare e avversare quelle attività e quei comportamenti che, potenzialmente, posso turbare la pacifica e tranquilla convivenza civile, in modo che non si traducano dalla potenza all'atto e ne scaturiscano azioni violente da parti di alcuni a scapito della cittadinanza.

Il bene che, sotto il profilo oggettivo, viene tutelato dalla 'pubblica sicurezza' è l''ordine pubblico'[4], inteso come la somma dei «principi etici e politici, la cui osservanza ed attuazione sono ritenute indispensabili all'esistenza di tale ordinamento ed al conseguimento dei suoi fini essenziali" ('ordine pubblico' c.d. "ideale")»[5] e come «il buon assetto o il regolare andamento del vivere civile, a cui corrispondono, nella collettività, l'opinione e il senso della tranquillità e della sicurezza» ('ordine pubblico' c.d. "materiale")[6].

Secondo l'orientamento elaborato dalla dottrina nell'ambito degli studi in materia di Diritto Costituzionale e Pubblico, la 'pubblica sicurezza' va intesa come l'integrità fisica dei cittadini e dei loro beni, degni, questi ultimi, di tutela nei confronti di qualunque tipologia di pericolo; nel caso in cui, infatti, tale sicurezza fosse messa in repentaglio da comportamenti lesivi, questi assumerebbe rilievo come danno per l'intera comunità (indipendentemente dal fatto che l'obiettivo fosse quello di nuocere a un singolo cittadino). La ragione di ciò affonda la propria *ratio* nel fatto che quando viene lesa l'incolumità fisica, o patrimoniale, dei privati la situazione che può venirsi a creare è tale da mettere a rischio non solo il regolare svolgersi del vivere civile, ma anche una certa tranquillità e sicurezza all'interno della opinione pubblica[7].

---

(3) G. Trombetta, *Ordine pubblico e sicurezza nell'ordinamento italiano,* in "Democrazia e Sicurezza", anno X, n. 2, 2020, pp. 45-94.

(4) F. Famiglietti, *La polizia di sicurezza (o "pubblica sicurezza"),* in F. Caringella, A. Iannuzzi, L. Levita, *Manuale di diritto di pubblica sicurezza,* Dike edizioni, Roma, 2014, p. 28.

(5) V. Guarriello, E. Macrì, S. M. Guarriello, *Cybercrime: una nuova minaccia per la Pubblica Sicurezza,* in "Democrazia e Sicurezza – Democracy and Security Review", Anno XIII, n. 1, 2022, p. 46.

(6) *Ibidem*.

(7) A. Pace, *Libertà e sicurezza. Cinquant'anni dopo,* in A. Torre (a cura di), *Costituzioni e sicurezza dello Stato,* Maggioli, Santarcangelo di Romagna, 2013, p. 558 e ss.

Con un maggiore sforzo esplicativo, adottando questa interpretazione, la 'pubblica sicurezza' può essere vista come la concreta applicazione del concetto di 'ordine pubblico', in particolare per quanto riguarda la protezione dei cittadini e dei loro diritti. In tal senso, secondo eminente dottrina, le due definizioni di 'ordine pubblico' sopra menzionate sono legate da un rapporto di strumentalità, nel senso che la salvaguardia dell''ordine pubblico' materiale serve a proteggere l''ordine pubblico' ideale[8]. In base a questo ragionamento, tuttavia, l''ordine pubblico' e la 'pubblica sicurezza' verrebbero a trovarsi su due piani distinti con significati diversi anche a livello concettuale[9].

In Italia, tuttavia, la riflessione sul tema è stata oggetto di nuovi apporti con l'entrata in vigore della Costituzione, a partire dalla quale ha cominciato a mettersi in dubbio l'ipotesi che potesse parlarsi di 'ordine pubblico' in senso ideale[10]. L'atteggiamento critico della dottrina si basava essenzialmente sul fatto che la Carta Costituzionale, con l'obiettivo di tutelare l''ordine pubblico', poneva determinati limiti ai diritti inviolabili del cittadino creando una situazione contraddittoria; l'*empasse* interpretativo, tuttavia, è stato superato dalla dottrina più moderna la quale ha ritenuto che la *Grundnorm* considerasse l''ordine pubblico' solo dal punto di vista materiale, arrivando, così, a identificare la 'pubblica sicurezza' come quell'attività volta ad assicurare una vita sociale tranquilla. A tale riguardo Angelini evidenzia che «Nell'intento di razionalizzarne la portata, la dottrina ha, […] operato una distinzione fondamentale fra "ordine pubblico materialmente inteso o amministrativo", in quanto concretamente imposto all'agire dei soggetti di un gruppo sociale, e "ordine ideale o normativo" affermato e tutelato dal diritto vigente»[11].

Verso la fine degli anni Novanta, il legislatore interno è intervenuto a confermare il suddetto orientamento con il d.lgs. n. 112/98, art. 159, comma 2, nel quale si stabiliva che l''ordine pubblico' andasse inteso

(8) F. Angelini, *Ordine pubblico e integrazione costituzionale europea. I principi fondamentali nelle relazioni inter-ordinamentali*, Cedam, Padova, 2007, p. 27.

(9) O. Caramaschi, *Dall'ordine pubblico alla sicurezza: una prospettiva di teoria costituzionale,* in "Democrazia & Sicurezza (Online), vol. 13, fasc. 1, 2023, pp. 83-132.

(10) G. Fiandaca, E. Musco, *Diritto penale, Parte speciale,* Zanichelli, Bologna, 2012, p. 474.

(11) F. Angelini, *Ordine pubblico e integrazione costituzionale europea. I principi fondamentali nelle relazioni inter-ordinamentali*, cit., p. 27.

come quel «complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, nonché alla sicurezza delle Istituzioni, dei cittadini e dei loro beni» mentre che con la locuzione 'pubblica sicurezza' dovessero intendersi le «misure preventive e repressive dirette al mantenimento dell'ordine pubblico»[12]. In seguito, intervenne in materia anche la Corte Costituzionale che consolidò l'interpretazione secondo cui per 'pubblica sicurezza' si dovesse ritenere la «funzione inerente la prevenzione dei reati o al mantenimento dell'ordine pubblico»[13]. Secondo questa operazione esegetica, 'ordine pubblico' e 'pubblica sicurezza' non si trovavano più in contraddizione l'uno con l'altra ma, anzi, andavano a formare un'endiadi e questo per il fatto di far parte dello stesso campo semantico e per essere, concettualmente, complementari.

Come avremo modo di argomentare, il concetto di 'pubblica sicurezza' si è nel tempo legato a quello di 'sicurezza informatica' (o cibernetica) soprattutto in virtù del crescente numero di reati informatici[14] che minacciano la tranquillità del vivere civile[15]. I reati informatici, caratterizzati da pervasività e invasività, non solo attentano alla quotidianità dei singoli individui ma, di riflesso, immettono nella società un senso di precarietà e d'incertezza che può anche raggiungere livelli molto elevati a seconda degli umori e della sensibilità dell'opinione pubblica. Prima di analizzare il tema della 'sicurezza informatica', tuttavia, si rende necessario un ulteriore passaggio che porta ad analizzare il concetto di 'sicurezza nazionale'.

Così come la 'pubblica sicurezza' anche il concetto di 'sicurezza Nazionale' ha stentato a trovare una definizione comunemente accettata dalla dottrina, difficoltà, questa, bene espressa da Wolfers che l'ha definita un «ambiguous symbol in political science»[16], ambiguo

(12) G. Tiani, *L'ordine pubblico: qualche considerazione sulla realtà italiana, in F. Angelini, Ordine pubblico e integrazione costituzionale europea*, Franco Angeli, Milano, 2011, p. 215 e ss.

(13) C. Cost., n. 77 del 24 marzo 1987, in "Gazz. Uff.", 1ª serie speciale, 1° aprile 1987, n. 147.

(14) Sulla difficoltà a formulare una definizione precisa di "reato informatico" si rimanda a S. Amore, V. Stanca, S. Staro, *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni,* Halley, Matelica, 2006, p. 49 e ss.

(15) Clusit, *Rapporto Clusit 2024 sulla sicurezza ICT in Italia*, 2024.

(16) A. Wolfers, *National Security as an Ambiguous Symbol,* in "Political Science Quarterly", 67, 4, 1952, pp. 481-502.

in quanto capace di rimandare a più significati senza assumerne nessuno in modo concreto. In base ai recenti orientamenti, la "sicurezza nazionale", lungi dal potersi definire solo in rapporto a minacce di natura militare, andrebbe intesa come «la protezione dello stato-nazione da minacce che mettono a repentaglio la sua indipendenza politica, l'integrità territoriale e la coesione socio-politica»[17]. In ragione di questo rapporto d'interdipendenza tra l'area politico-militare, quella energetica e quella economica, la cosiddetta "catena di sicurezza", la 'sicurezza nazionale' viene spesso tradotta graficamente come l'area dove intersecano tre o più cerchi[18].

In Italia l'intervento che maggiormente ha influito sulla normativizzazione del concetto di 'sicurezza nazionale', dopo l'art. 126 della Costituzione secondo il quale «Con decreto motivato del Presidente della Repubblica sono disposti lo scioglimento del Consiglio regionale e la rimozione del Presidente della Giunta che abbiano compiuto atti contrari alla Costituzione o gravi violazioni di legge. Lo scioglimento e la rimozione possono altresì essere disposti per ragioni di sicurezza nazionale [...]»[19], è stata la L. n. 124/07 che ha definito il sistema d'informazione per la sicurezza della Repubblica[20]. Con la Legge del 2007, infatti, la 'sicurezza nazionale' è stata definita come la somma di quelle attività il cui obiettivo è quello di difendere l'indipendenza, l'integrità e la sicurezza dello Stato strumentali «alla «protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia, nonché il compito di individuare e contrastare al di fuori del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali»[21].

Parlare di 'sicurezza nazionale', tuttavia, nonostante le facili confusioni, non significa fare riferimento né alla 'difesa nazionale', che

(17) E. Camilli, *Sicurezza nazionale: tra concetto e strategia,* 2014, p. 5.

(18) A. Pansa, *La sicurezza nazionale: innovazione e nuovi limiti, in* "Gnosis", vol. 25, fasc. 1, 2019, pp. 20-35.

(19) L. Tramontano, *Codice di procedura civile e leggi complementari,* La Tribuna, Piacenza, 2020, p. XII.

(20) I. Portelli, *Le trasformazioni e le complessità del sistema nazionale dell'ordine e della sicurezza pubblica*, in "Queste istituzioni", fasc. 144, 2007, pp. 147-167.

(21) A. Spataro, *Segreto di Stato e ricadute sulle indagini giudiziarie. Il caso Abu Omar*, in A. Torre (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli, Santarcangelo di Romagna, 2013, p. 61 nota 17.

rimanda a quelle azioni che vengono realizzate per difendere l'indipendenza dello Stato e la risposta nei confronti di minacce esterne né, tantomeno, a quello di 'pubblica sicurezza' di cui si è detto[22]. Ne consegue, tuttavia, che, così come per la 'pubblica sicurezza', anche la 'sicurezza nazionale' assume un fondamentale rilievo nel tema della *cyber security*; si pensi, infatti, il caso in cui vengono sabotate o rubate delle informazioni riguardanti infrastrutture critiche per lo Stato (ad esempio di tipo sanitario o energetico) o per altre Istituzioni strategiche e di come queste azioni possano risultare dannose di quegli interessi che rappresentano in nucleo fondante della 'sicurezza nazionale'[23].

Rileva evidenziare che, oggi, diverse azioni di natura militare trovano statuto di esistenza nel *cyberspazio,* declinate nell'inedita versione (rispetto al passato) di *cyberwar* o *cyberwarfare,* ritenuta dagli esperti del settore una nuova modalità di belligeranza figlia della terza rivoluzione industriale[24]. Parlare di guerra "cibernetica" significa, di fatto, ipotizzare scenari in cui vengono attaccate infrastrutture critiche di un Paese, intercettati dati e conversazioni strategiche per sabotare e/o intralciare strumentazioni militari o di interesse pubblico di natura informatica o satellitare; non si tratta, sempre e solo, di attacchi che si sostanziano in azioni che producono conseguenze fisiche, come la distruzione di apparati informatici, ma anche sintattiche che portano, cioè, a termine degli attacchi informatici attraverso l'uso di *malware* (come *Trojan* e *Spyware*) in grado di compromettere la sicurezza e la *privacy* di un sistema, oppure di *Denial of Service,* altre tipologie di attacchi progettati per rendere un servizio, un sito web o una rete inaccessibile agli utenti legittimi, sovraccaricandolo di richieste o causando malfunzionamenti[25]. In alcuni casi, invece, attraverso l'uso dell'ingegneria sociale vengono realizzare delle azioni (tipo il *phishing*) tramite le quali sono carpite agli avversari informazioni riservate o credenziali d'accesso a determinati

(22) T. F. Giupponi, *I rapporti tra sicurezza e difesa: differenze e profili di convergenza,* "Diritto costituzionale: rivista quadrimestrale", 1, 2022, pp. 21-47.

(23) A. Antinori, *Sicurezza nazionale in quanto 'sicurezza (cyber-)sociale',* in "Gnosis", vol. 24, fasc. 4, 2018, pp. 54-63.

(24) P. Baiocchi, *Cyberwar, la quinta dimensione,* in "Valori", 113, 2013, pp. 34-40.

(25) I. Salvadori, *I reati contro la riservatezza informatica*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime,* Utet, Torino, 2023, pp. 694-763; A. Cappellini, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in *Ivi*, pp. 810-876.

sistemi informatici rilevanti per la sicurezza del Paese, dal che ne deriva che affinché uno Stato sia in grado di tutelare la 'pubblica sicurezza' e la 'sicurezza nazionale', nel mondo del terzo Millennio, debba necessariamente dimostrarsi in grado di tutelare la 'sicurezza cibernetica'.

Definire la *cybersecurity* è un obiettivo niente affatto semplice, si tratta, infatti, di un termine ampiamente utilizzato che, tuttavia, suscita ancora un accesso dibattito in dottrina e tra gli esperti di settore. L'assenza di una definizione concisa e ampiamente accettabile che ne catturi la multidimensionalità impedisce, a livello globale, una visione univoca e ostacola l'evoluzione stessa della materia[26]. In termini approssimativi, tuttavia, la sicurezza cibernetica viene intesa come quell'attività finalizzata a proteggere i sistemi informatici e le informazioni in essi contenuti da eventuali rischi e violazioni[27].

A livello tecnico le azioni poste in essere per tutelare la sicurezza cibernetica si muovono, generalmente, su tre piani differenti: quello logico, quello fisico e quello funzionale, in modo da assicurare la fruibilità dei sistemi e dei dati solo a chi ne abbia autorizzazione (in virtù di un principio di riservatezza), per difendere l'accuratezza delle informazioni (integrità) e per garantire ai soggetti autorizzati un costante accesso e utilizzo ai dati (disponibilità)[28]. Affinché sia rispettato il principio di riservatezza, integrità e disponibilità, i *server* vengono allocati fisicamente in sedi sicure e sorvegliate e si valutano attentamente, in termini logici, i soggetti che, tramite autenticazione, possano accedervi; infine, per ogni utente ammesso si stabilisce a quali e quante informazioni può avere accesso. La protezione contro gli attacchi informatici avviene anche a livello operativo, monitorando le attività svolte all'interno dei sistemi da parte degli utenti che hanno accesso autorizzato; questo controllo è realizzato attraverso l'uso di *file* di *log* che servono a tracciare e registrare tali attività (garantendone, così, l'*accountability*)[29].

---

(26) D. Craigen, N. Diakun-Thibault, R. Purse, *Defining Cybersecurity,* in "Technology Innovation Management Review", ottobre 2014, p.13.

(27) G. Iovane, *Cyberware e Cyberspace: Aspetti Concettuali, Fasi ed Applicazione allo Scenario Nazionale d all'ambito Militare*, CeMiSS, 2008.

(28) C. Pfleeger, S. Pfleeger, *Sicurezza in informatica,* Pearson-Prentice Hall, Milano, 2004, p. 12 e ss.

(29) I. Priyadarshini, C. Cotton, *Cybersecurity: Ethics, Legal, Risks, and Policies,* CRC Press, New York, 2022, p. 34 e ss.