Elena Buoso

Ritorno al futuro: il perimetro di sicurezza nazionale cibernetica

Abstract: L'evoluzione dei sistemi giuridici ha avuto un impatto significativo sulla funzione di sicurezza pubblica, ridefinendone i concetti e le pratiche. Le categorie tradizionali della teoria generale della sicurezza, come i principi di precauzione e prevenzione, e l'uso di concetti giuridici indeterminati per legittimare il potere esercitato, rivelano la complessità nel rispondere alle nuove sfide e la necessità di stabilire criteri per bilanciare il potere e gli interessi coinvolti. La sicurezza, considerata come un concetto olistico e multiforme, si è ampliata fino a includere la dimensione della cybersecurity, un'area sempre più centrale nelle moderne politiche di sicurezza, ampliando così anche il potere amministrativo per la protezione preventiva. Uno dei nuovi strumenti attraverso cui si esercita questa antica funzione è il Perimetro nazionale di sicurezza cibernetica. Esso rappresenta uno strumento cruciale per la tutela degli interessi strategici del Paese, individuando i soggetti ivi inclusi per imporre obblighi preventivi e successivi per la protezione delle funzioni e dei servizi essenziali dello Stato. La natura del potere esercitato in questo contesto, le peculiarità del procedimento amministrativo e gli effetti sull'attività dei soggetti inclusi sollevano importanti questioni relative alle garanzie e alle tutele necessarie a bilanciare la sicurezza nazionale con i diritti individuali e collettivi.

Keywords: Cybersecurity; Protezione preventiva; Perimetro di Sicurezza Nazionale Cibernetica; Procedimento amministrativo.

Sommario: 1. La funzione di pubblica sicurezza e l'evoluzione degli ordinamenti giuridici – 2. La teoria generale della sicurezza: i concetti giuridici indeterminati – 3. La poliedricità della sicurezza come concetto olistico e la 'nuova' cybersicurezza – 4. Il perimetro di sicurezza nazionale cibernetica: funzione e soggetti inclusi – 5. Segue: effetti dell'inserimento nel perimetro – 6. Il procedimento di inserimento nel perimetro – 7. I criteri per l'inserimento nel perimetro, la natura del potere e la questione delle garanzie e delle tutele.

1. La funzione di pubblica sicurezza e l'evoluzione degli ordinamenti giuridici

Rischio, pericolo e, di conseguenza, paura, sono elementi che caratterizzano la percezione umana del mondo e influenzano l'azione individuale e collettiva. Già nel 1986 la migliore sociologia descriveva le peculiarità della nuova "società del rischio" e dei suoi percorsi verso una nuova modernità[1].

1 Beck 1986: 1. V. anche Luhmann 1991: 9; Bauman 2006: 54.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760158

Come sempre avviene, le conquiste tecnologiche degli ultimi decenni hanno portato anche nuove minacce e negli ultimi lustri gli ordinamenti giuridici registrano un aumento degli strumenti di protezione contro pericoli inediti, sviluppando strategie di difesa non solo in ottica nazionale ma anche, vista la dimensione e le caratteristiche dei fenomeni, globale[2]. Si tratta, peraltro, di fenomeni regolatori ricorrenti, con ricaduta su diversi istituti e branche del diritto, ai quali abbiamo assistito più volte nel corso del secolo scorso per reagire al terrorismo nazionale[3] e internazionale[4], alla criminalità organizzata[5], alla violenza negli e fuori dagli stadi[6].

La reazione degli ordinamenti, e in particolare di quello italiano, ha preso anche la strada del diritto amministrativo, con strumenti tradizionali o introducendo istituti nuovi, in un complesso di misure molto varie, dai controlli e dall'inasprimento di regimi autorizzatori o di divieti, alle *black list*, alle interdittive antimafia, ai d.a.s.p.o. Il panorama è molto ampio perché la funzione legata alla sicurezza è una delle funzioni primarie dell'apparato statale, infatti la troviamo descritta e analizzata diffusamente già dai primi trattati di diritto amministrativo[7].

Curiosamente, l'interesse della dottrina amministrativistica si è successivamente spostato su altri oggetti, un po' perché nella dialettica libertà e autorità è intervenuto il diritto costituzionale[8], ma anche perché altri settori sono risultati più rilevanti per il loro impatto economico e per un concetto di diritto amministrativo come fattore di sviluppo (si pensi agli appalti)[9]; o ancora perché l'attenzione si è rivolta alla cura di interessi differenziati e sensibili, come ambiente, paesaggio, sanità[10]. La funzione di pubblica sicurezza in sé, invece, non è stata particolarmente ulteriormente indagata con contributi di portata generale[11], se non per singoli aspetti che interferiscono con quel diritto amministrativo 'dell'economia'[12]. Il disinteresse

2 V. ad es., con riferimento al terrorismo, Haubrich 2003: 3-28; con riguardo alle minacce informatiche e alla cybersicurezza si segnalano i dati pubblicati dalle Nazioni Unite al sito https://unctad.org/page/cybercrime-legislation-worldwide nonché Kipker and Pagel 2020: 1 e le analisi comparate e nazionali pubblicate dalla Rivista International Cybersecurity Law Review – Zeitschrift für Cybersicherheit und Recht; Chiti 2016: 511.

3 Spataro 2023: 1-26.

4 Braml J. 2021: 2-26; Prosperi 2016: 16 e gli altri contributi del medesimo Volume.

5 Maggio 2013: 808; Passarelli 2024: 150-173.

6 D'Arienzo 2012: 1131; Follieri 2017: 23; Garaffa 2017: 399; Bifulco 2018: 159; Di Nella 2018: 77.

7 Orlando 1904: 71, la descrive come "quella funzione che tende a prevenire il danno sociale e ad assicurare la pace e l'ordine pubblico ed esercita una influenza sui diritti individuali, limitandone la sfera di azione in maniera che si mantenga l'armonia fra essi e fra l'utilità singola e quella collettiva"; v. anche Romano 1912: 244.

8 Mortati 1975: 135; Barile 1967: 12; Cerrina Feroni e Morbidelli 2008: 31; Matteucci 2016: 20; D'Atena 2018: 6.

9 Napolitano 2014: 695.

10 Sciullo 2016: 58.

11 Con alcune eccezioni: Corso 1979; Caia 2000: 184; Tropea 2010; e con un ritrovato interesse in tempi più recenti Tonoletti 2022: 791; Ursi 2022; Buoso 2023; Raimondi 2023.

12 Come il già richiamato istituto delle interdittive antimafia, sulle quali esiste una letteratura molto abbondante. V. ad es. Sticchi Damiani e Amarelli 2016: 11; Mazzamuto 2018: 2222.

è curioso[13], considerando non solo che ci si trova di fronte a una funzione squisitamente afferente al concetto di sovranità e di interesse pubblico[14] – e quindi al ruolo tradizionale dello Stato e della pubblica amministrazione – ma anche che essa implica poteri che incidono su diritti e libertà ed è quindi rivelatrice della concezione di Stato e di pubblica amministrazione del periodo storico di volta in volta considerato.

Sicurezza e prevenzione sono elementi ricorrenti, perché necessari al mantenimento del sistema e dell'ordinamento, ma con connotazioni e implicazioni molto differenti. Oggi sono lontane le teorie dell'individuazione dell'interesse pubblico e dei poteri autoritativi della pubblica amministrazione come garanzia totalizzante del benessere sociale[15] – che tra le Due Guerre hanno portato alle distorsioni dei regimi totalitari[16] – ma alcune suggestioni in questa direzione non sono assenti dagli atti legislativi in materia di pubblica sicurezza. In questo senso può essere letta anche l'attuale definizione degli scopi dell'Unione Europea in termini di creazione di "uno spazio di libertà, sicurezza e giustizia", che fonda e legittima la pervasività della regolazione unionale (art. 3, II c., TUE).

2. La teoria generale della sicurezza: prevenzione, precauzione e concetti giuridici indeterminati

Le considerazioni di teoria generale sulla funzione di sicurezza sono state recuperate in relazione al potere di prevenzione, impostosi con sempre maggiore evidenza come principio cardine dell'azione amministrativa – assieme al successivo principio di precauzione – in molti settori critici, quali il diritto dell'ambiente e della salute pubblica[17]. Entrambi i principi, infatti, sono riferiti a poteri limitativi della sfera giuridica dei privati, anticipatori rispetto all'evento e conformati da concetti giuridici indeterminati[18]. Nel caso dei poteri di sicurezza, i concetti giuridici indeterminati trovano la loro massima applicazione; essi infatti riguardano la *ratio* del potere (sicurezza, ordine pubblico e come abbiamo sentito ieri interessi nazionali strategici), l'individuazione dei presupposti dell'agire (rischio, pericolo) e la qualificazione dell'oggetto di esso (attività pericolose, servizi essenziali).

13 Sul disinteresse della scienza del diritto amministrativo per il tema, v. Cassese 2000: 127; Raimondi 2023: 2.

14 Fisichella 2008: 65.

15 Ranelletti 1904: 269, riprendendo le note tesi di O. Mayer.

16 Con riferimento allo Stato nazionalsocialista v. Schwegel 2005: 132; in relazione allo Stato fascista, cfr. Groppali 1940: 79; Panza 1990: 3; Cassese 2010: 14.

17 De Leonardis 2005: 6; Trimarchi 2005: 1673; Barone 2006; Manfredi 2011: 28. Esemplare in questo senso la giurisprudenza in materia di contrasto della Xylella fastidiosa nella vicenda che ha riguardato gli espianti degli ulivi in Puglia per contenere il fenomeno del disseccamento (Corte giustizia UE, sez. I, 9 giugno 2016, n. 78; Consiglio di Stato, sez. III, 11 marzo 2021, n. 2096) e quella relativa all'obbligo vaccinale previsto per alcune categorie di lavoratori durante la pandemia COVID19 (*ex multis*, Consiglio di Stato, sez. III, 20 ottobre 2021, n. 7045).

18 De Pretis 1995: 11; Fraenkel-Haeberle 2005: 808.

I concetti giuridici indeterminati sono una categoria molto sviluppata nel diritto tedesco (*unbestimmte Rechtsbegriffe*), che in quell'ordinamento consentono una valutazione amministrativa pressoché pienamente sindacabile dal giudice[19]. La categoria nazionale corrispondente, ossia la discrezionalità tecnica, si presenta invece molto più problematica per le note oscillazioni e difficoltà del giudice amministrativo tra sindacato esterno e sindacato interno debole dell'agire amministrativo[20].

Ma anche a livello costituzionale, dove sono posti i primi e fondamentali limiti ai poteri di sicurezza ricorre il riferimento a tali categorie concettuali. La Costituzione, infatti, afferma la possibilità di limitare le libertà da essa espresse solo per preservare "interessi essenziali" al mantenimento di una ordinata convivenza civile[21]. Il limite non è definito precisamente nei suoi termini sostanziali, ma viene costruito con garanzie procedurali e di metodo, quali la riserva di legge, di giurisdizione e l'applicazione dei principi di ragionevolezza e proporzionalità.

3. La poliedricità della sicurezza come concetto olistico e la 'nuova' cybersicurezza

L'inerenza della funzione di sicurezza a tutta l'attività statale e pubblica ne comporta diverse declinazioni e una estrema ampiezza. Accanto alla "sicurezza nazionale", intesa come difesa degli interessi dello Stato come ordinamento di libere istituzioni e comunità (art. 117, II c., lett. d), Cost.), troviamo la sicurezza pubblica in senso materiale e individuale, come ordine pubblico (art. 117, II c., lett. h), Cost.) anche in senso economico[22].

Si tratta di poli diversi della stessa funzione, tra i quali trova spazio la nuova funzione volta a garantire la cybersicurezza, definita nel Cybersecurity Act europeo come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"[23]. La portata di questa definizione non è esigua come a prima vista appare. La rete e i sistemi informativi sono oggi irrinunciabili per il funzionamento dei sistemi statali, intesi in termini istituzionali e delle pubbliche ammi-

19 Fraenkel-Haeberle 2005: 811; Reinhardt 2019: 195.

20 Travi 2001: 9; Villata e Ramajoli 2007: 117.

21 Così Corte cost. sent. 7 aprile 1995, n. 115, in tema di riforma del TUPS; Id. sent. 30 luglio 2020, n. 177, sulla l.r. Puglia n. 14/2019 (Testo unico in materia di legalità, regolarità amministrativa e sicurezza).

22 V. Corte cost., sent. n. 6 luglio 1966, n. 87, punto 4 del *Diritto*. La sentenza, di accoglimento parziale, rigetta la questione costituzionale posta sul divieto penale di propaganda sovversiva ed antinazionale, ritenendo che la disposizione tuteli "l'ordine economico, rispetto al diritto al lavoro, alla organizzazione sindacale, alla iniziativa economica privata, alla proprietà" nonché "il mantenimento dell'ordine pubblico considerato come ordine legale costituito".

23 Art. 2, n. 1), Regolamento (UE) 2019/881 del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("Regolamento sulla cybersicurezza").

nistrazioni[24] ma anche come costruzioni economico-sociali e produttive[25]. Ed è infatti su questi fattori che nell'ultimo decennio si sono trasferite molte delle più incisive minacce alla sicurezza nazionale, delineata come concetto non solo poliedrico ma piuttosto 'olistico', comprensivo cioè di tutti gli aspetti che caratterizzano gli Stati contemporanei e la loro tendenza alla "securitizzazione" della società e dell'ordinamento, nell'ottica di prevenzione della vulnerabilità della società e degli individui per creare resilienza, secondo dinamiche che focalizzano sull'aspetto della protezione anziché su quello della libertà[26].

Così anche il recente regolamento UE sui servizi digitali, che riferisce la sicurezza sia a una dimensione individuale, sia in relazione agli effetti negativi reali o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica in senso materiale[27].

Tale evoluzione rende la cybersicurezza un presupposto di legittimazione di poteri normativi e amministrativi formidabili. Gli strumenti della cybersicurezza sono gli strumenti tradizionali del diritto amministrativo, ma in una declinazione nuova, soprattutto in relazione ai procedimenti e agli organi competenti, come si vedrà nei prossimi paragrafi.

4. Il perimetro di sicurezza nazionale cibernetica: funzione e soggetti inclusi

Il perimetro di sicurezza nazionale cibernetica comprende molti di questi strumenti che si estendono e mescolano con la dimensione economica delle attività private e dello Stato. Esso è stato delineato da un complesso sistema di interventi normativi, europei e nazionali, e provvedimenti d'urgenza nazionali[28].

24 Montessoro 2019: 783; Lauro 2021: 529.

25 Cfr. Angelini e Altri 2021: 7.

26 Buzan e Wæver e De Wilde 1998: 12; Buzzacchi 2015: 104.

27 Regolamento (Ue) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

28 A partire dalle Direttive NIS-1 (Direttiva (Ue) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione) e NIS-2 (Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148). Possono essere poi ricordati il richiamato Regolam. UE 2022/2065 sui servizi digitali; il Regolamento (Ue) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione; il d.l. 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica; il dPCM 30 luglio 2020, n. 131 sul Perimetro nazionale di sicurezza cibernetica e il d.l. 14 giugno 2021, n. 82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. Più in dettaglio Buoso 2023: 87 ss.; Rossa 2023: 115 ss.

Lo scopo di questo strumento è indicato dall'art. 1 d.l. 105/19. Il perimetro è istituito per

> assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

I richiamati interessi, assolutamente primari, giustificano poteri estremamente ampi ed effetti limitativi dell'iniziativa economica e dell'agire privato, che conseguono all'inserimento di un soggetto e di una attività nel perimetro. Tali limitazioni e conformazioni delle sfere giuridiche dei soggetti individuati, sono accompagnate da alcune peculiarità del procedimento amministrativo che riguarda l'inserimento nel perimetro.

Partendo dall'indicazione dei soggetti sottoposti a questo potere, si tratta di una platea molto ampia, definita secondo un meccanismo articolato in tre presupposti. Il primo è la natura del soggetto, che può essere pubblico (pubbliche amministrazioni e operatori pubblici in senso lato) o privato che abbia una sede nel territorio nazionale; il secondo considera l'attività svolta (tramite reti, sistemi informativi e servizi informatici)[29]. Infine, vengono indicati gli scopi e gli effetti dell'attività da proteggere: da essa, infatti, deve dipendere "una funzione essenziale dello Stato", o "la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato" quando dal loro malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa "derivare un pregiudizio per la sicurezza nazionale".

Qualche specificazione aggiuntiva deriva dal decreto attuativo della norma, ove vengono individuati come soggetti che svolgono "funzioni o servizi essenziali" quelli cui "l'ordinamento attribuisce compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia […] la funzionalità dei sistemi economico e finanziario e dei trasporti"[30]. Quanto ai soggetti che "presta[no] un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato", essi sono inseribili nel perimetro quando pongono in essere attività "strumentali all'esercizio di funzioni essenziali dello Stato; necessarie per

29 Reti e sistemi informativi sono definiti dalle direttive NIS-1 e NIS-2 e del d.lgs. 65/2018, come "qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali; i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione".

30 D.P.C.M. n. 131/2020, art. 2 c. 1, lett. a).

l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale"[31].

Le norme distinguono quindi tra "funzioni essenziali dello Stato" – concetto che richiama le "funzioni essenziali dell'ordinamento" individuate dalla giurisprudenza costituzionale come oggetto della funzione di sicurezza[32] – e prestazione di "servizi essenziali" per le attività civili, sociali ed economiche, indicazione che rinvia, anche nell'ordine espositivo, ai diritti garantiti nei primi tre Titoli della parte I della Costituzione.

L'individuazione dei soggetti richiede una operazione ermeneutica quasi heideggeriana, che mette in connessione il destinatario con lo scopo stesso del potere e con una qualificazione dei pericoli e delle minacce da scongiurare.

Guardando alle categorie sviluppate nell'ambito dei principi di precauzione e di prevenzione all'agire anticipatorio della pubblica amministrazione, possiamo chiederci se il presupposto che legittima l'attivazione del potere sia il pericolo (concreto) o il mero rischio (potenziale)[33]. Secondo i criteri di questa dogmatica, a fronte della gravità delle minacce e dell'importanza degli interessi coinvolti, è possibile ritenere sufficiente il mero rischio per attivare il potere amministrativo, con un approccio di estrema prudenza – il medesimo applicato dal legislatore europeo in materia di intelligenza artificiale[34] – decisamente ampliativo del potere. In questo senso depone anche la specificazione normativa, per la quale solo nel caso dei servizi essenziali vengono qualificati gli effetti del malfunzionamento rilevanti per l'inserimento nel perimetro, non invece per le funzioni essenziali.

Le norme italiane non si esprimono in termini di rischio o pericolo, ma il decreto n. 131/2020 sembra richiamare – con confusione di termini – il primo, laddove definisce il pregiudizio per la sicurezza nazionale in termini di

> danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale.

31 Art. 2 c. 1, lett. a), d.P.C.M. n. 131/2020.

32 Ad. es. Corte cost. 25 febbraio 1988, n. 218.

33 Tali categorie sono state sviluppate con ampia elaborazione dottrinale nel sistema tedesco e riconducono rispettivamente al principio di precauzione e a quello di prevenzione: v., per tutti, Breuer 1978: 836; Darnstadt 1983: 6 ss.

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

Un ulteriore ampliamento dei presupposti di attivazione di questo potere preventivo si ha con l'art. 1 d.l. n. 82/2021, il quale mira a garantire la "resilienza"[35] dei sistemi informativi "anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico". Non risulta peraltro chiaro rispetto a cosa questi elementi si qualifichino come ulteriori; inoltre torna alla luce il tradizionale concetto di interesse nazionale, che la riforma del Titolo V ha estromesso dalla Costituzione[36].

Già questa rapida analisi delle minacce individuate dalle norme come presupposti di esercizio del potere rende evidente come si tratti di rischi che comportano e legittimano una concentrazione di poteri al vertice politico istituzionale dell'esecutivo, perché toccano l'esistenza dello Stato e lo svolgimento delle sue funzioni essenziali. Tale accentramento in capo all'esecutivo e al suo vertice non è privo di risvolti problematici[37] ed è stato temperato rispetto alla versione originaria, che concentrava molte funzioni sul Presidente del Consiglio dei Ministri in coerenza con il suo ruolo di direzione e responsabilità per le politiche di cybersicurezza[38], compartendole con altri organi e con la novella Agenzia nazionale per la cybersicurezza[39] secondo una "geometria variabile" molto articolata[40].

5. Segue: effetti dell'inserimento nel perimetro

L'inclusione di un soggetto nel perimetro nazionale di cybersicurezza comporta obblighi e adempimenti di diversa natura.

Anzitutto scattano obblighi preventivi, che possono essere organizzati in quattro categorie: di comunicazione[41]; di adeguamento delle tecnologie e dei processi interni[42]; di formazione e consapevolezza dei dipendenti[43] e riguardanti gli approvvigionamenti e l'affidamento di forniture di beni, sistemi e servizi di ICT[44].

35 Sul concetto di cyberresilienza, v. Rossa 2023: 72 ss.

36 Barbera 1973: 25 ss.; Tosi 2002: 86.

37 Previti 2022: 65 ss.

38 Sulla strategia nazionale di cybersicurezza, v. Matassa 2022: 625.

39 Cfr. l'art. 1, c. 2 *bis*, d.l. n. 105 del 2019 e i successivi artt. 5 d.P.C.M. n. 131 del 2020 e 7, c. 1, lett. h), d.l. n. 82 del 2021, ai sensi del quale l'ACN assume tutte le funzioni attribuite alla Presidenza del Consiglio dei Ministri di cui al d.l. n. 105 del 2019.

40 Giupponi 2024: 295.

41 Che prevedono la trasmissione all'ACN di un elenco, periodicamente aggiornato, delle reti, dei sistemi informativi e dei servizi informatici: art. 1, comma 2, d.l. n. 10 del 2019. Tale comunicazione consente allo Stato una mappatura totale della struttura dei servizi.

42 Gli adeguamenti devono garantire elevati livelli di sicurezza e relativi diversi tipi di contenuti e attività, secondo uno schema già collaudato con la normativa anticorruzione. Deve inoltre essere creata una struttura organizzativa preposta alla gestione della sicurezza, individuando politiche di gestione del rischio e prevenzione degli incidenti, anche attraverso interventi sugli apparati o sui prodotti che risultino gravemente inadeguati sul piano della sicurezza. Cfr. l'art. 1, c. 3, lett. b), d.l. n. 105 del 2019.

43 Art. 1, comma 3, lett. b), n. 7, d.l. n. 105 del 2019.

44 Art. 1, comma 3, lett. b), n. 8 e c. 6, d.l. n. 105 del 2019. Le disposizioni prevendono

In secondo luogo, sul soggetto all'interno del perimetro pesano obblighi successivi. Al verificarsi di una "compromissione" – definita come perdita di sicurezza o di efficacia dello svolgimento di una funzione essenziale dello Stato o di un servizio essenziale, connessa al malfunzionamento, all'interruzione, anche parziali, ovvero all'utilizzo improprio di reti, sistemi informativi e servizi informatici – o di un "incidente" – ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici-[45] i soggetti del perimetro devono attuare le misure di mitigazione e gestione degli incidenti secondo i protocolli di intervento e notificare l'accaduto al Gruppo di intervento per la sicurezza informatica in caso di incidente istituito presso la ACN[46].

Gli obblighi sono muniti di sanzioni amministrative pecuniarie, da moderate a ingenti[47], lontane dalle soglie massime di altri apparati sanzionatori del diritto amministrativo, probabilmente per evitare che l'eccessiva deterrenza porti a fenomeni di elusione delle comunicazioni, soprattutto in materia di compromissioni e incidenti.

6. Il procedimento di inserimento nel perimetro

Il procedimento – le norme parlano significativamente di procedura[48] quasi a marcare la distanza dal procedimento amministrativo ai sensi della legge generale 7 agosto 1990, n. 241 – di inserimento nel perimetro presenta alcune interessanti peculiarità[49]. Esso si articola in tre passaggi: il primo prevede un sistema di raccolta dei profili da parte dei Ministeri, nei propri settori di attività, come individuati dall'art. 3 d.P.C.M. n. 131/20[50]. Successivamente, l'elenco risultante viene trasmesso al CISR tecnico e sottoposto al CISR "ordinario"[51]. È poi proprio quest'ultimo

sia la definizione di caratteristiche e requisiti di carattere generale, standard e limiti per le acquisizioni, sia l'obbligo di comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN) dell'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset "strategici".

45 Per queste definizioni, v. l'art. 1, c. 1, lett. g) e h), d.P.C.M. n. 131 del 2020. L'ACN definisce con propria determinazione la "*tassonomia degli incidenti*" che devono essere oggetto di notifica, come previsto dalla direttiva NIS, e di quelli che possono esserlo, ai fini di "*fornire all'ACN un quadro di valutazione della minaccia più completo*": così la determinazione ACN del 3 gennaio 2023, in G.U. n. 7 del 10 gennaio 2023.

46 Art. 1, comma 3, lett. a), d.l. n. 105 del 2019.

47 Art. 1, comma 9, d.l. n. 105 del 2019

48 Art. 4 d.P.C.M. n. 131/2020.

49 Artt. 1, c. 2, lett. a) d.l. n. 105 del 2019 e 5 d.P.C.M. n. 131/2020.

50 Tali settori sono: a) interno; b) difesa; c) spazio e aerospazio; d) energia; e) telecomunicazioni; f) economia e finanza; g) trasporti; h) servizi digitali; i) tecnologie critiche; l) enti previdenziali/lavoro.

51 Il Comitato interministeriale per la sicurezza della Repubblica è stato istituito ed è disciplinato dall'art. 5 l. 3 agosto 2007, n. 124, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto. Il Comitato è coadiuvato da un organismo tecnico

a formulare la proposta di elenco definitivo, che sarà adottato con atto del Presidente del Consiglio dei Ministri[52].

L'individuazione dei soggetti e il loro inserimento nel perimetro si sono così perfezionati, ma ancora nulla è uscito all'esterno né i soggetti inclusi ne hanno contezza. Solo entro 30 giorni dalla conclusione del procedimento il DIS (Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio dei ministri)[53], comunica – in forma non specificata dalla disposizione – l'avvenuta inclusione al soggetto, indicando la funzione essenziale o il servizio essenziale che giustifica l'inserimento[54].

Evidenti ragioni di sicurezza impediscono la pubblicazione degli atti ma è escluso anche l'accesso, con previsione che limita fortemente le possibilità di opposizione all'inserimento e che va forse differenziata, in via interpretativa, rispetto ai diversi tipi di accesso e ai soggetti richiedenti[55].

Da questo momento devono ritenersi efficaci per i soggetti inclusi nel perimetro gli obblighi sopra ricordati, ma restano poco chiari gli eventuali obblighi di comunicazione ai soggetti connessi (i fornitori etc.) nella rete.

7. I criteri per l'inserimento nel perimetro, la natura del potere e la questione delle garanzie e delle tutele

Sulla base dei presupposti che lo legittimano, degli organi coinvolti nel procedimento e della stessa procedura di compilazione degli elenchi, risulta evidente l'ampiezza delle valutazioni e conseguentemente del potere esercitato, con effetti di vincolo anche molto penetranti sull'attività inclusa nel perimetro.

Le disposizioni specificano un criterio per la formazione dell'elenco e per l'esercizio dei poteri sfavorevoli connessi: la gradualità, in base alla quale si deve tener conto "dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei si-

di supporto, il CISR tecnico (art. 4, c. 5, d.P.C.M. 3 aprile 2020, n. 2), istituito presso il DIS, presieduto dal Direttore Generale e composto dai direttori delle Agenzie e da Dirigenti apicali designati dai Ministri membri del CISR. In proposito Vigna 2007: 693; Bellandi 2013: 1.

52 Artt. 1, c. 2-bis, d.l. 105/2019. Il d.l. n. 82/2021 parrebbe però aver trasmesso anche questa competenza all'ACN.

53 Art. 4 l. 3 agosto 2007, n. 124.

54 Artt. 1, c. 2-bis d.l. 105/2019 e 5, c. 3, d.P.C.M. n. 131/2020. La disposizione regolamentare specifica una serie di ulteriori informative: l'avvenuta iscrizione è comunicata anche alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, per i soggetti pubblici e per quelli di cui all'articolo 29 del codice dell'amministrazione digitale, e al Ministero dello sviluppo economico, per quelli privati. Inoltre, l'elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica è trasmesso all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione (previsto dall'art. 7-bis d.l. 27 luglio 2005, n. 144, conv. con modif. in l. 31 luglio 2005, n. 155).

55 Art. 1, c. 2-bis, d.l. n. 105/2019.

stemi informativi e dei servizi informatici predetti"[56]. Nonostante il termine non compaia, si tratta di una descrizione del concetto di proporzionalità, inteso non come principio ma come canone di decisione amministrativa[57], declinato alla luce delle valutazioni di costi-benefici e delle regole di *risk assesment*[58].

Ci si può chiedere, pertanto, se l'applicazione del criterio di gradualità non sia già necessitata per il nostro diritto amministrativo e la sua formulazione non risulti troppo generale per costituire una linea guida ulteriore. A questo proposito sarebbe opportuna una maggiore specificazione delle categorie di attività, seguendo l'approccio *risk oriented* del Regolamento UE dei servizi digitali e del Regolamento AI, che elencano diverse categorie di rischio sistemico, mappate e valutate dai gestori, sulle quali si graduano gli obblighi.

L'atto di inserimento nel perimetro, tramite la predisposizione degli elenchi, è esercizio di un potere di prevenzione che si situa ad un crocevia tra atto di indirizzo, valutazione tecnica e scelta discrezionale, che – negli effetti – sembra avvicinabile all'imposizione di un vincolo, costitutivo, conformativo e compressivo della situazione giuridica soggettiva del soggetto inserito. La coesistenza di valutazione tecnica – espressa dal contributo alla compilazione degli elenchi fornito dai Ministeri e dal CISR tecnico – assieme a una componente di discrezionalità amministrativa pura rende necessario ma anche possibile un bilanciamento tra la tutela di interessi pubblici essenziali in gioco con quelli privati o pubblici contrastanti.

Le usuali garanzie per un corretto bilanciamento, anche in vista della tutela giurisdizionale successiva, tradizionalmente offerte nel nostro ordinamento dal procedimento, sono molto poche. Prevale, infatti, l'esigenza di sicurezza, sacrificando quelle di trasparenza e partecipazione.

La formulazione normativa consente di ipotizzare un atto di inserimento la cui motivazione si sostanzia nell'indicazione della funzione e del servizio essenziale offerto dall'operatore, quindi pressoché non sindacabile, salvo macroscopici travisamenti.

Un limite può essere offerto dai criteri sostanziali che sono alla base delle valutazioni di tipo tecnico per la formazione degli elenchi, anche in ambiti ad alta sensibilità politico-economica. Ma le formulazioni generali e la mancata applicazione del diritto di accesso, se applicata in riferimento a tutte le sue forme, compreso l'accesso documentale del soggetto incluso, può rendere molto difficile l'individuazione di queste valutazioni e la loro giustiziabilità.

La garanzia più efficace, ad oggi, sembra risiedere nell'aspetto organizzativo della architettura della cybersicurezza in Italia. Rispetto alla disciplina originaria è stato introdotto un sistema di condivisione e di gestione del potere attraverso strutture organizzative complesse e coordinate dei vari Ministeri e di altri organi, nonché dal ruolo – non ancora del tutto definito – della Agenzia nazionale.

56 Art. 1, c. 2, d.l. 105/19 e art. 3 d.P.C.M. n. 131/2020.

57 Buoso 2012: 255.

58 Su questi aspetti della proporzionalità per una obiettiva valutazione del rischio, v. Schrader-Frechette 1993: 91 ss.

Se queste garanzie siano sufficienti per bilanciare un potere non nuovo nella sua natura ma inedito nelle modalità di esercizio[59], è ancora presto per dirlo. La cifra e la gravità delle minacce giustificano le nuove forme di potere preventivo, ma è necessario vigilare perché non divengano occasione per un ritorno al passato, ai poteri di una amministrazione quasi ottocentesca con i potenziati sistemi di controllo che la tecnologia consente[60]. Il viaggio dell'ordinamento, con il bagaglio delle categorie tradizionali della sicurezza, deve invece puntare al futuro.

Bibliografia

Angelini M. e Altri 2021, *Metodologia per il cybersecurity assesment con il Framework Nazionale per la Cybersecurity e la Data Protection*, disponibile al sito *http://www.cybersecurityfracamework.it* (consultato il 18 luglio 2024).

Barbera A. 1973, *Regioni e interesse nazionale*, Milano: Giuffrè.

Barile P. 1967, "La pubblica sicurezza", in Id. (a cura di) 1967, *La pubblica sicurezza*, Vicenza: Neri Pozza.

Barone A. 2006, *Il diritto del rischio*, Milano: Giuffrè.

Bauman Z. 2006, *Liquid Fear*, Hoboken: Wiley.

Beck U. 1986, *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Frankfurt am Main: Suhrkamp.

Bellandi R. 2013, "L'affermazione del Comitato interministeriale per la Sicurezza della Repubblica (CISR) quale nuovo protagonista della politica di sicurezza nazionale", in *federalismi.it*, 24: 1-15.

Bifulco L. 2018, "La sicurezza negli stadi in Italia. Tifo, violenza, diritto e misure di contrasto", in *Sociologia del diritto*, 3: 159-185.

Braml J. 2021, "Anti-terrorism laws and powers. An inventory of the G20 States 20 years after 9/11", in *Friedrich Ebert Stiftung*. Disponibile al link https://ny.fes.de/article/anti-terrorism-laws-20-years-after-9-11.html (ult. accesso: June 30, 2024).

Breuer R. 1978, "Gefahrenabwehr und Risikovorsorge im Atomrecht", in *Deutsches Verwaltungsblatt.*, 836-852.

Buoso E. 2012, *Proporzionalità, efficienza e accordi nell'attività amministrativa*, Padova: CEDAM.

Buoso E. 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino: Giappichelli.

Buzan B., Wæver O., De Wilde J. 1998, *Security: A New Framework for Analysis*, Boulder-London: Lynne Rienner.

Buzzacchi C. 2015, "Sicurezza e securitization tra Stato, Unione europea e mercato", in Pizzolato F. e Costa P. (a cura di) 2015, *Sicurezza, Stato e mercato*, Milano: Giuffrè, 98-131.

Caia G. 2000, "L'ordine e la sicurezza pubblica", in Cassese S. (a cura di) 2000, *Trattato di diritto amministrativo*, Milano: Giuffrè.

Carotti B. 2020, "Sicurezza cibernetica e Stato-nazione", in *Giornale di Diritto Amministrativo*, 5: 629-641.

Cassese S. 2000, *Le basi del diritto amministrativo*, VI ed., Milano: Giuffrè.

Cassese S. 2010, *Lo Stato fascista*, Bologna: Il Mulino.

59 Ursi 2023: 7 ss.

60 Su questi aspetti, v. Carotti 2020: 639.

Cerrina Feroni G. e Morbidelli G. 2008, "La sicurezza: un valore superprimario", in *Percorsi costituzionali*, 1: 31-44.
Chiti E. 2016, "Le sfide alla sicurezza e gli assetti nazionali ed europei delle forze di sicurezza e di difesa", in *Diritto amministrativo*, 4: 511-547.
Corso G. 1979, Corso G., *L'ordine pubblico*, Bologna: Il Mulino.
D. de Pretis 1995, *Valutazione amministrativa e discrezionalità tecnica*, Padova: CEDAM.
D'Arienzo M. 2012, "Divieto di accesso alle manifestazioni sportive (daspo): natura, funzione e problematiche connesse alla sua applicazione", in *Diritto e processo amministrativo*, 4: 1311-1329.
D'Atena A. 2018, "Costituzionalismo e tutela dei diritti fondamentali", in Id. 2018 [2001], *Lezioni di diritto costituzionale*, Torino: Giappichelli.
Darnstadt T. 1983, *Gefahrenabwehr und Gefahrenvorsorge: eine Untersuchung über Struktur und Bedeutung der Prognose-Tatbestände im Recht der öffentlichen Sicherheit und Ordnung*, Frankfurt a. M.: Metzner.
de Leonardis F. 2005, *Il principio di precauzione nell'amministrazione di rischio*, Giuffrè: Milano.
Di Nella L. 2018, "La violenza negli stadi. L'esperienza tedesca", in *Rassegna di diritto ed economia dello sport*, 1: 77-93.
Fisichella D. 2008, *Alla ricerca della sovranità. Sicurezza e libertà in Thomas Hobbes*, Roma: Carocci.
Follieri E. 2017, "Il daspo urbano (artt. 9, 10 e 13 del D.L. 20.2.2017 n. 14)", in *GiustAmm. it*, 3: 23-49.
Fraenkel-Haeberle C. 2005, „Unbestimmte Rechtsbegriffe, technisches Ermessen und gerichtliche Nachprüfbarkeit – Eine rechtsvergleichende Analyse", in *Die Öffentliche Verwaltung*, 808-815.
Garaffa P. 2018, "Misure antiviolenza negli stadi: vecchi e nuovi contrasti, vecchie e nuove questioni, vecchi e nuovi chiarimenti", in *La Giustizia Penale*, 7: 399-448.
Giupponi T. 2024, "Il governo nazionale della cybersicurezza", in *Quaderni costituzionali*, 2: 277-303.
Groppali A. 1940, "Sul concetto di ordine pubblico", in AA.VV. 1940, *Scritti giuridici in onore di Santi Romano*, vol. II, Padova: CEDAM.
Haubrich D. 2003, "September 11, Anti-Terror Laws and Civil Liberties: Britain, France and Germany Compared", in *Government and Opposition*, 38(1): 3-28.
Kipker D-K. and Pagel P. 2020, "Editorial", in *International Cybersecurity Law Review – Zeitschrift für Cybersicherheit und Recht*, 1: 1-5.
Lauro A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", in *Quaderni del Gruppo di Pisa*, 3: 529-545.
Luhmann N. 1991, *Soziologie des Risikos*, Berlin-New York: Walter de Gruyter.
Maggio P. 2013, "La lotta alla criminalità organizzata in Europa fra strategie di contrasto e rispetto dei diritti umani", in *Cassazione penale*, 2: 808-821.
Manfredi G. 2011, "Cambiamenti climatici e principio di precauzione", in *Rivista quadrimestrale di diritto dell'ambiente*, 27-39.
Matassa M. 2022, "Una strategia nazionale a difesa del cyberspazio", in *Persona e amministrazione*, 2: 625-653.
Matteucci N. 2016, *Organizzazione del potere e libertà. Storia del costituzionalismo moderno*, Bologna: Il Mulino.
Mazzamuto M. 2018, "Le interdittive prefettizie tra prevenzione antimafia e salvataggio delle imprese", in *Giurisprudenza italiana*, 10: 2222-2230.
Montessoro P.L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti dell'amministrazione digitale", in *Istituzioni del federalismo*, 3: 783-800.

Mortati C. 1975, *Istituzioni di diritto pubblico*, vol. I, Padova: CEDAM.
Napolitano G. 2014, "Diritto amministrativo e processo economico", in *Diritto amministrativo*, 4: 695-724.
Orlando V.E. 1904, "Introduzione al Diritto amministrativo", in Id., (a cura di) 1904, *Primo trattato completo di diritto amministrativo italiano*, vol. I, Milano: Società editrice libraria.
Panza G. 1990, "Ordine pubblico, I) Teoria generale", in *Enc. giur*., XXII, Roma: Treccani.
Passarelli t. 2024, "Interdittive antimafia e prevenzione collaborativa: azioni di contrasto al crimine organizzato tra incertezze legislative e discrezionalità applicativa", in *federalismi.it*, 10: 150-173.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informativo", in *federalismi.it*, 25: 65-93.
Prosperi A. 2016, "L'esperienza della storia italiana, antica e recente", in *Terrorismo internazionale. Politiche della sicurezza. Diritti fondamentali – Speciale di Questione Giustizia*, 16-25. Disponibile al link https://www.questionegiustizia.it/speciale/2016-1 (consultato il 5 luglio 2024).
Raimondi S. 2023, *La sicurezza pubblica*, Torino: Giappichelli.
Ranelletti O. 1904, "La polizia di sicurezza", in Orlando V.E. (a cura di) 1904, *Primo trattato completo di diritto amministrativo italiano*, vol. IV, Milano: Società editrice libraria.
Reinhardt M. 2019, „Umweltschutz ist wesentlich. Verfassungsrechtliche Anforderungen an die Standardsetzung mit unbestimmten und unbestimmbaren Rechtsbegriffen", in *Neue Zeitschrift für Verwaltungsrecht*, 195-211.
Romano S. 1912 [1901], *Principii di diritto amministrativo italiano*, Milano: Società editrice libraria.
Rossa S. 2023, *Cybersicurezza e pubblica amministrazione*, Napoli: Editoriale Scientifica.
Schrader-Frechette K.S. 1993, *Valutare il rischio*, trad. it., Milano: Giuffrè.
Schwegel A. 2005, *Der Polizeibegriff im NS-Staat*, Tübingen: Mohr Siebeck.
Sciullo G. 2016, "'Interessi differenziati' e procedimento amministrativo", in *Rivista giuridica di urbanistica*,1: 58-98.
Spataro A. 2023, "Il contrasto al terrorismo", in *Sistema penale*, 1-26.
Sticchi Damiani S. e Amarelli G 2016, *Le interdittive antimafia e le altre misure di contrasto all'infiltrazione mafiosa negli appalti pubblici*, Torino; Giappichelli.
Tonoletti B. 2022, "Ordine e sicurezza pubblica", in Mattarella B.G. e Ramajoli M. (a cura di) 2022, *Funzioni amministrative – Enciclopedia del diritto. I Tematici*, III, Milano: Giuffrè, 791-816.
Tosi R. 2002, "A proposito dell'interesse nazionale", in *Quaderni costituzionali*, 86-88.
Travi A. 2001, "Circa il sindacato del giudice amministrativo sulla discrezionalità tecnica della pubblica amministrazione", in *Foro it.*, III, 9-15.
Trimarchi F. 2005, "Principio di precauzione e «qualità» dell'azione amministrativa", in *Rivista trimestrale di diritto pubblico e comunitario*, 1673-1707.
Tropea G. 2010, *Sicurezza e sussidiarietà. Premesse per uno studio sui rapporti tra sicurezza pubblica e democrazia amministrativa*, Edizioni Scientifiche Italiane: Napoli.
Ursi R. 2022, *La sicurezza pubblica,* Bologna: Il Mulino.
Ursi R. 2023, "La sicurezza cibernetica come funzione pubblica", in Id. (a cura di) 2023, *La Sicurezza nel Cyberspazio*, Milano: Franco Angeli, 7-20.
Vigna P.L. 2007, "La nuova disciplina dei servizi di sicurezza", in *La Legislazione penale*, 4(2): 693-702.
Villata R. e Ramajoli M. 2007, *Il provvedimento amministrativo*, Torino; Giappichelli.