Simona Terracciano

La dimensione collaborativa tra soggetti pubblici e tra soggetti pubblici e privati nel contesto della cybersicurezza

Abstract: Considering the increase in hostile cyber activities targeting the digital infrastructures of public entities, it is necessary and urgent to establish an institutional framework capable of intercepting cyber threats preventively and intervening effectively to prevent or mitigate the damage from cybersecurity incidents and cyberattacks that affect fundamental public and private interests and the regular provision of public services. In this regard, the contribution analyzes some aspects of the collaboration between public entities and between public and private entities in the field of cybersecurity, focusing on recent regulatory interventions in the Italian legal system to verify if and how the Italian legislator intends to promote collaboration both in organizational and procedural terms, and through a fruitful collaboration with private entities in the procurement of ICT goods and services by public administrations.

Keywords: Cybersecurity, Cultura cyber, Cyber resilience, Collaborazione, Sanzioni.

1. Il contesto di riferimento: tra attività ostili nello spazio cibernetico, vulnerabilità delle istituzioni pubbliche e salvaguardia di interessi pubblici e privati

La Relazione annuale 2023 sulla politica d'informazione per la sicurezza, presentata al Parlamento dal Sistema di informazione per la sicurezza della Repubblica, rileva che le attività ostili nello spazio cibernetico nazionale interessano in modo crescente (e prevalente rispetto ai target privati) le infrastrutture digitali dei soggetti pubblici e, in particolare, quelle riferibili alle Amministrazioni centrali dello Stato e agli Istituti e Agenzie Nazionali[1].

1 In particolare, dalla Relazione Annuale 2023 sulla politica dell'informazione per la sicurezza (del 24 febbraio 2024) emerge che le operazioni cibernetiche condotte in danno al nostro paese hanno coinvolto, nel 2022, per il 56% target privati e per il 43% target pubblici,

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: 10.7413/197054760167

In particolare, l'Agenzia per la cybersicurezza nazionale (ACN), nel corso del 2023[2], ha gestito 422 eventi cyber[3] ai danni di istituzioni pubbliche nazionali, in sensibile aumento rispetto ai 160 del 2022 e, di questi eventi, 85 sono stati classificati come incidenti[4] (nel 2022 furono 57), generando un malfunzionamento dei sistemi con conseguenti blocchi o rallentamenti nella erogazione dei servizi.

L'incremento delle offensive digitali nelle filiere delle infrastrutture digitali/servizi IT, dell'energia e dei trasporti impone la necessità di predisporre un apparato istituzionale in grado di intercettare, in un'ottica preventiva, le minacce cibernetiche e di intervenire in modo efficace per evitare o limitare i danni di incidenti di sicurezza informatica e di attacchi informatici che incidono su interessi fondamentali pubblici e privati[5].

Sebbene, infatti, la consapevolezza circa i rischi, soprattutto a livello statale, stia senz'altro aumentando negli ultimi anni[6], la vulnerabilità delle istituzioni pubbliche nel contesto della cybersicurezza rimane elevata[7] in ragione, oltre di aspetti più strettamente tecnici legati alle infrastrutture e ai sistemi, anche della mancanza di adeguate competenze specifiche all'interno delle amministrazioni[8] nonché, in generale, di una insufficiente cultura della sicurezza cyber[9]. Cultura, peraltro, che

mentre nel 2023, per il 40% target privati e per il 40% target pubblici. Nell'ambito dei target pubblici, il 65% sono Amministrazioni statali (62% nel 2022), il 2% sono strutture sanitarie pubbliche (11% nel 2022), il 22% sono Istituti e Agenzie nazionali (9% nel 2022) e il 3% sono Enti regionali, provinciali e comunali (9% nel 2022).

2 Si veda la Relazione Annuale al Parlamento 2023 dell'Agenzia per la cybersicurezza nazionale.

3 Nella Relazione Annuale al Parlamento 2023 dell'Agenzia per la cybersicurezza nazionale del 2023, per evento cyber si intende un "case con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, il CSIRT Italia dirama alert e/o supporta, eventualmente anche in loco, i soggetti colpiti".

4 Nella definizione contenuta nella Relazione Annuale per "*incidente*" si intende "un evento cyber con impatto su confidenzialità, integrità o disponibilità delle informazioni confermato dalla vittima".

5 Se vogliamo, in larga parte già predisposto visto che l'architettura nazionale di cybersicurezza è stata strutturata dal d.l. n. 82/2021 in quattro pilastri di competenze diversificate ma complementari, che devono agire, per l'appunto, in sinergica collaborazione: il pilastro dell'informazione per la sicurezza nel dominio cyber, affidato ai Servizi; il pilastro della protezione militare, affidato al Ministero della Difesa; il pilastro della prevenzione e repressione criminale, affidato all'A.G. e alle forze di polizia di sicurezza e, infine, il pilastro della vigilanza e regolazione amministrativa affidato all'ACN.

6 Previti 2022: 67, osserva che l'accelerazione del processo di transizione digitale e le dinamiche sociali ed economico pandemiche, prima, e l'aumento esponenziale degli attacchi cibernetici riconducibili al conflitto russo-ucraino, poi, abbiano determinato un concreto manifestarsi negli ultimi anni di un reale interessamento delle istituzioni pubbliche per le rilevanti questioni problematiche poste dalla tutela della cybersicurezza.

7 Al riguardo, parlano di sistema amministrativo sotto assedio dal punto di vista digitale, Borriello & Fristachi, 2022:157

8 Rossa 2023b: 161.

9 Rossa 2023a: 220-221, "L'azione pubblica volta all'incremento delle competenze digitali e di cybersicurezza fra i dipendenti pubblici è funzionale alla diffusione di progetti e iniziative volte a promuovere una più ampia cultura della cybersicurezza, in grado di abbracciare anche

appare diffusa in modo molto diversificato tra i diversi livelli di governo territoriale laddove si consideri che le Amministrazioni locali con processi codificati di gestione degli eventi di sicurezza informatica (incidenti, allarmi di sicurezza o tentativi di attacco) sono appena il 29,2% (di cui 95,5% delle Regioni)[10].

La menzionata vulnerabilità si inserisce, d'altra parte, in un contesto di progressivo consolidamento dell'utilizzo di infrastrutture ICT e dei servizi digitali offerti sia a livello centrale sia a livello locale[11], che determina un aumento quantitativo e trasversale delle aree a rischio e fa emergere, dunque, la necessità di rafforzare la sicurezza e la resilienza informatica.

Tale esigenza risulta ancora più urgente considerando che la maggior parte degli attacchi alle istituzioni pubbliche nel 2023 ha riguardato eventi di natura *DDoS* (*Distributed Denial of Service*), ossia attacchi che mirano a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria con l'effetto di rendere indisponibili i siti e i servizi colpiti[12].

i cittadini e le imprese. Iniziative, vale a dire, dirette non tanto a coloro i quali si occupano professionalmente di cybersecurity, quanto invece a chi può imbattersi indirettamente in attacchi e incidenti cyber nell'uso quotidiani della tecnologia, da un lato sensibilizzando sui rischi esistenti e possibili e, dall'altro, educando a prevenire questi ultimi evitando di porre in essere azioni o comportamenti potenzialmente pericolosi".

10 Nel Report Pubblica Amministrazione Locale e ICT anno 2022 curato dall'Istituto Nazionale di Statistica e pubblicato il 23 febbraio 2024, si evidenzia che "Il miglioramento delle dotazioni ICT, della gestione in rete e dell'offerta online pone un accento ancor maggiore sulla necessità di valutare la sicurezza informatica delle PA locali. Il 15,1% delle PA locali ha nominato un Responsabile per la sicurezza al proprio interno (54,5% delle Regioni) o in gestione associata; invece, il 21,9% ha affidato la sicurezza ICT all'esterno, tipicamente a un fornitore di servizi (22,7% delle Regioni). Inoltre, le Amministrazioni locali con processi codificati di gestione degli eventi di sicurezza informatica (incidenti, allarmi di sicurezza o tentativi di attacco) sono appena il 29,2% (95,5% delle Regioni). Nel triennio 2020-2022 le PA locali hanno messo in campo azioni legate alla sicurezza informatica e in particolare il 79,8% ha acquistato o aggiornato software di sicurezza, il 51,2% ha preferito affidarsi a incarichi di consulenza a esperti esterni, il 36,0% ha elaborato o modificato protocolli di difesa e/o prevenzione, il 27,2% ha investito in formazione aggiuntiva al personale sulla sicurezza informatica, il 2,7% ha potuto assumere personale dedicato alla sicurezza informatica, e un'ultima parte ha indicato il disaster recovery come ulteriore area di azione".

11 Report *Pubblica amministrazione locale e ICT*, curato dall'Istituto Nazionale di Statistica, 23 febbraio 2024, in *https://www.istat.it/it/files//2024/02/Report_Ict_AP_LOCALI.pdf*, ove si legge che "Nel 2022 l'86,4% delle Regioni e il 70,4% dei Comuni consente di svolgere online l'intero iter, dall'avvio alla conclusione, di almeno un servizio pubblico locale. È in forte aumento, dal 34,3% del 2018 al 54,2%, l'utilizzo di servizi di cloud computing da parte delle PA locali. Sette amministrazioni locali su dieci non hanno una gestione codificata degli eventi di sicurezza ICT. Il 74,0% delle PA locali accede a Internet tramite connessioni veloci (almeno 30 Mbps, Megabit per secondo), mentre raddoppia (35,8%) rispetto al 2018 (17,4%) la diffusione di quelle ultraveloci (almeno 100 Mbps). Il 5,1% delle PA locali (l'81,8% delle Regioni) ha investito in intelligenza artificiale o analisi dei big data o ha pianificato di farlo nel triennio 2022-2024".

12 Cfr. Relazione Annuale al Parlamento 2023 dell'Agenzia per la cybersicurezza nazionale, pubblicata su *https://www.acn.gov.it/portale/documents/20119/446882/ACN_Relazione_2023.pdf*, par. 1.2.3, pp. 23-24.

2. La transizione digitale cyber resiliente e la (necessaria) promozione della dimensione collaborativa

Considerata l'espansione e la trasversalità del fenomeno e gli interessi pubblici e privati a rischio, risulta condivisibile l'impostazione metodologica che enfatizza come, ormai, la cybersicurezza "rileva in quanto elemento imprescindibile per il corretto funzionamento della Pubblica Amministrazione nel suo complesso, sempre più digitalizzata, senza il bisogno di relegare lo studio delle tematiche cyber a ragioni particolari quali la sicurezza dello Stato e la sicurezza pubblica"[13].

A fronte di una minaccia cyber generalizzata, in quanto indirizzata verso soggetti pubblici e privati, nonché diffusa e trasversale, dal momento che incide su molteplici aree dell'azione amministrativa e dei settori produttivi dell'economia nazionale, e considerati gli interessi fondamentali pubblici e privati suscettibili di essere pregiudicati, la garanzia di un elevato livello di sicurezza informatica e la fiducia nelle tecnologie divengono, dunque, un presupposto indispensabile per il complessivo successo della trasformazione digitale della Nazione e dell'Unione Europea.

Tale consapevolezza emerge anche dalla Strategia Nazionale Cybersicurezza 2022-2026[14], ove è previsto che la cybersicurezza "deve porsi a fondamento del processo di digitalizzazione del Paese, quale elemento imprescindibile della trasformazione digitale, anche nell'ottica di conseguire l'autonomia strategica nel settore", promuovendo, in sostanza, una *transizione digitale cyber resiliente* per il settore pubblico e per il tessuto produttivo[15].

La portata del fenomeno richiede, dunque, azioni pubbliche di prevenzione e gestione delle minacce e degli attacchi cyber che siano tempestive ed efficaci, garantendo la maggior tutela degli interessi pubblici e privati incisi.

Ebbene, tali attività e la necessità di protezione non paiono poter essere adeguatamente assicurate mediante interventi meramente settoriali e frammentari da parte di un unico soggetto isolato nel contesto nazionale e ciò in considerazione della estensione del fenomeno e delle "dimensioni mondiali della tecnica e dell'economia"[16].

13 Rossa 2023a: 28. In questo senso già Previti 2022: 82, secondo il quale "L'estensione indiscriminata, al settore della cybersicurezza, dei principi e dei caratteri che connotano l'attività amministrativa svolta dagli organismi inseriti nel Sistema (i.e., riservatezza delle comunicazioni, centralizzazione delle funzioni e unilateralità dei processi decisionali) non sembrerebbe rappresentare l'impostazione metodologica più idonea a superare le sfide per la pubblica sicurezza lanciate dalla diffusione del cyberspazio".

14 Strategia Nazionale di Cybersicurezza 2022-2026, disponibile sul sito istituzionale dell'ACN.

15 Per una analisi del quadro normativo in materia e del ruolo dell'ACN v. Chiappini 2022: 301-344; Ricotta 2023a: 356 e ss.; Ricotta 2023b: 97 e ss.

16 B. Carotti 2020: 633-634, nel commentare il d.l. 105/2019, afferma che esso "si cala sulle esigenze primarie dell'apparato, purché connesso allo svolgimento di funzioni essenziali legate agli interessi della nazione. È lo Stato-nazione ad essere protetto dal "peri-

Piuttosto, l'efficacia delle azioni appare inevitabilmente condizionata dallo sforzo collaborativo tra soggetti pubblici, anche in una dimensione multilivello, e tra soggetti pubblici e privati[17], mediante la condivisione di dati, informazioni, esperienze, conoscenze e soluzioni tecniche[18].

Lo sforzo collaborativo appare, infatti, fondamentale sia a monte, in una fase preventiva e fisiologica, per identificare e analizzare eventuali vulnerabilità e minacce e rischi in chiave previsionale e programmatica, sia a valle nella fase di gestione della crisi cibernetica, per garantire una risposta consapevole e tempestiva in base allo specifico scenario di riferimento.

Al contempo, la collaborazione tra pubblico e privato risulta nodale in un'ottica di sviluppo e innovazione, considerato che lo spazio cibernetico è costituito da prodotti e servizi ICT realizzati o erogati principalmente da soggetti privati[19].

metro", allorché si intreccia inscindibilmente con l'utilizzo di apparati quali reti, sistemi e servizi. (…) Se il decreto (…) tende verso una concezione fortemente nazionale dello Stato (…) i rischi di una lettura rigida e parcellizzata delle disposizioni divengono più elevati. In questo risiede la forte problematica che l'intervento solleva, laddove occorrerebbe un approccio maggiormente aperto, favorendo una lettura più moderna – in linea con quanto la giuspubblicistica ha insegnato ampiamente da decenni. Lo Stato, nel settore in esame, può essere tutelato benissimo anche in una dimensione più collaborativa, che è proprio quella richiesta dalla disciplina europea, secondo un disegno attuale, che sappia coniugare l'offerta di garanzie alla cittadinanza ai tempi e alle dimensioni mondiali della tecnica e dell'economia".

17 La collaborazione tra pubblico e privato quale dinamica che permea il procedimento amministrativo e la ricostruzione del procedimento amministrativo come rapporto giuridico collaborativo è stata messa in luce da autorevoli studiosi. Di recente, anche per la corposa bibliografia, si rimanda agli scritti di Chirulli 2023: 399-411; Spasiano 2021: 25-54; Bonetti 2022: 30. Parlava di "rivoluzione" Benvenuti 1994: 23, riferendosi al "capovolgimento della concezione e del posto e della funzione che spetta ai cittadini nell'ambito di uno Stato che voglia essere ispirato non più ai principii di monocrazia ma a principii di demo-crazia, i quali non possono ridursi al riconoscimento di posizioni giuridiche passive dei cittadini nei confronti dello Stato e quindi alla loro tutela, ma deve evolversi nel senso del riconoscimento di posizioni giuridiche attive nell'ambito delle funzioni, ciò che va sotto il nome di partecipazione" e di "partecipazione come libertà dei post-moderni" riferendosi al superamento "del momento tradizionale della democrazia ottocentesca basata sul riconoscimento della libertà del singolo e sulla loto protezione e, si apre al riconoscimento della libertà attiva fatta di partecipazione, e cioè della demarchia del futuro". Un contributo decisivo alla valorizzazione della partecipazione procedimentale è da attribuire agli studi di Scoca 1990: 24 e all'inquadramento dell'interesse legittimo come posizione sostanziale che dialoga con l'autorità lungo tutto il processo di formazione del procedimento. Si richiamano anche gli importanti scritti di Nigro 1980: 231 ss.; Ledda 1993: 133-172; Zito 1996: *passim* sulla natura giuridica delle pretese partecipative; Manganaro 1995; Cognetti 2000; Tarullo 2008: 354.

18 In modo approfondito nel settore della cybersicurezza, Rossa 2021: 145; Rossa 2023a: 107; Previti 2022: 82.

19 Nella Strategia Nazionale di Cybersicurezza 2022-2026, spec. p. 26, la Partnership Pubblico-Privato (PPP) è qualificata come trasversale agli obiettivi di protezione risposta e sviluppo, nonché ai fattori abilitanti (ossia formazione, promozione della cultura della sicurezza cibernetica e cooperazione).

D'altronde, la dimensione collaborativa è enfatizzata nei principali atti normativi e regolatori sovranazionali[20] e nazionali[21] in materia di cybersicurezza, nonché più in generale nell'approccio seguito dal regolatore europeo riguardo ai mercati

20 Regolamento (UE, Euratom) 2023/2841 del Parlamento Europeo e del Consiglio del 13 dicembre 2023 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione, *Considerando* n. 3, ove si legge che "Gli ambienti TIC dei soggetti dell'Unione sono interdipendenti, utilizzano flussi di dati integrati e sono caratterizzati da una stretta collaborazione fra i loro utenti. Tale interconnessione significa che qualsiasi perturbazione, anche se inizialmente limitata a un solo soggetto dell'Unione, può avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata su altri soggetti dell'Unione. Inoltre, alcuni ambienti TIC dei soggetti dell'Unione sono connessi con gli ambienti TIC degli Stati membri, e un incidente in un soggetto dell'Unione può rappresentare un rischio per la cibersicurezza degli ambienti TIC degli Stati membri e viceversa. La condivisione di informazioni specifiche su un incidente può facilitare il rilevamento di minacce informatiche o incidenti analoghi che interessano gli Stati membri". Anche la Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), evidenzia in più punti la necessità di collaborazione tra Stati membri e UE e prevede, tra l'altro, all'art. 7, par. 1, lett. e), che la Strategia nazionale cibersicurezza di ciascuno Stato membro comprenda "l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato" e, all'art. 29, gli accordi di condivisione delle informazioni sulla cibersicurezza tra soggetti inclusi e non inclusi nell'ambito di applicazione della direttiva, al fine di prevenire o rilevare gli incidenti, a riprendersi dagli stessi o ad attenuarne l'impatto e di aumentare il livello di cibersicurezza, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento, contenimento e prevenzione delle minacce, strategie di attenuazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati. Al riguardo, rileva anche il Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 e, in particolare, gli articoli da 45 a 49.

21 Si vedano il D.lgs. 18 maggio 2018, n. 65 di attuazione della Direttiva NIS, che promuove la collaborazione tra pubblico e privato (art. 6), tra soggetti pubblici come ACN, MEF e Autorità di Vigilanza e Garante Privacy (art. 7 e 9); Anche il d.l. 14 giugno 2021, n. 82, convertito in l. n. 109/2021, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", istituisce il Comitato interministeriale per la cybersicurezza attribuendogli il compito di promuovere "l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza" (art. 4, co. 1, lett. c), nonché, tra le funzioni dell'Agenzia per la cybersicurezza nazionale prevede, lo sviluppo di capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici (art. 7). Inoltre, la Strategia nazionale di cybersicurezza 2022-2026 esplicita l'approccio "*whole-of-society*" che, oltre degli attori istituzionali con competenze in materia cyber, vede coinvolti anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza.

e ai servizi digitali (Digital Markets Act[22], Digital Services Act[23], AI Act[24])[25], che complessivamente delineano una visione strategica fondata sulla cooperazione e condivisione multilivello di informazioni e su una sinergia tra i settori pubblico, privato e la società civile[26].

3. Alcune prospettive della dimensione collaborativa nelle recenti tendenze normative: la pianificazione e la procedimentalizzazione delle attività

Le coordinate di sistema, pur sinteticamente descritte, consentono all'interprete di analizzare le *prospettive* della dimensione collaborativa nel contesto cyber alla luce delle più recenti tendenze normative, tra le quali anche la recente legge in materia di rafforzamento della cybersicurezza nazionale e di reati informativi[27], il cui rapido iter di approvazione è stato avviato con un disegno di legge presentato dal Consiglio dei Ministri il 16 febbraio 2024[28], approvato dalla Camera dei Deputati il 15 maggio 2024[29] e approvato in via definitiva dal Senato della Repubblica in data 19 giugno 2024[30].

Tra i recenti interventi stimolati dalla intensificazione e della crescente sofisticazione delle minacce informatiche nel contesto geo-politico, con particolare riferimento alla grave crisi internazionale in atto in Ucraina, è possibile ricordare una

22 Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

23 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).

24 Al riguardo, al Summit di Seoul del 21 maggio 2024, i leader di Australia, Canada, UE, Francia, Germania, Italia, Giappone, Repubblica di Corea, Repubblica di Singapore, Regno Unito e Stati Uniti d'America, hanno sancito nella Dichiarazione di Seoul per una IA sicura, innovativa e inclusiva (punto 7) "the importance of active multi-stakeholder collaboration, including governments, the private sector, academia, and civil society to cultivate safe, innovative and inclusive Al ecosystems, and the importance of cross-border and cross-disciplinary collaboration. Recognizing that all states will be affected by the benefits and risks of AI, we will actively include a wide range of international stakeholders in conversations around AI governance".

25 In merito al DSA e DMA, Bolognini, Pelino & Scialdone (a cura di) 2023; Torchia, 2023.

26 Al riguardo, Forgione 2022: 1141.

27 Legge 28 giugno 2024, n. 90, pubblicata in G.U. n. 153 del 2 luglio 2024, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici".

28 Disegno di legge del 16 febbraio 2024, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (A.C. 1717), consultabile sul sito *https://www.camera.it/leg19/126?leg=19&idDocumento=1717*.

29 Al riguardo si veda per l'analisi del testo emendato a seguito dell'esame in Commissione riunite Affari Costituzionali e Giustizia della Camera, si veda il Dossier n. 257/1 del Servizio Studi del 13 maggio 2024 contenente gli elementi per l'esame in Assemblea, pubblicato al disponibile al seguente link: *https://documenti.camera.it/leg19/dossier/pdf/AC0225a.pdf*.

30 Si rimanda al Dossier n. 257/2 del Servizio Studi del Senato del 22 maggio 2024, disponibile al link: *https://www.senato.it/service/PDF/PDFServer/BGT/01418663.pdf*.

prima direttiva del 6 luglio 2023 del Presidente del Consiglio dei Ministri rivolta alle amministrazioni pubbliche di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, volta a promuovere la gestione adeguata e coordinata delle minacce informatiche degli incidenti e delle situazioni di crisi di natura cibernetica con il supporto all'ACN, mediante "la più ampia collaborazione da parte dei soggetti impattati, nel loro stesso interesse e in quello, più generale, della resilienza cibernetica del Paese".

Tale Direttiva si è tradotta nel mese di ottobre 2023, in sede di conversione del d.l. n. 105/2023, nella introduzione della lettera *n-bis)*, all'art. 7, co. 1, del d.l. n. 82/2021[31], che ha attribuito all'ACN, nell'ambito delle funzioni di prevenzione e gestione degli incidenti e degli attacchi informatici, il potere di svolgere "ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informativa o attacchi informatici" estendendo, ai soggetti inclusi nel perimetro di sicurezza nazionale[32], ai soggetti NIS[33] (operatori di servizi essenziali e fornitori di servizi digitali) e ai soggetti Tel.co[34] (ossia le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica) in caso di mancata collaborazione, le sanzioni amministrative pecuniarie e accessorie previste dall'articolo 1, commi 10 e 14, del decreto-legge "Perimetro", nonché qualificando la mancata collaborazione come causa di responsabilità disciplinare e amministrativo-contabile.

A tale modifica normativa – che valorizza il momento collaborativo tra Agenzia e tutti i soggetti pubblici e privati impattati – ha fatto seguito un'ulteriore Direttiva del Presidente del Consiglio dei Ministri nel dicembre 2023 che, nel fornire gli indirizzi di attuazione e di coordinamento, prescrive l'adozione di atti di intesa tra ACN e Ministeri volti a procedimentalizzare il *modus operandi* delle parti in caso di attacco informatico e di misure specifiche volte nel complesso a dotare ciascun Ministero di un piano di gestione delle vulnerabilità e di reazione ove si individuino chiaramente e in via preventiva i ruoli, le responsabilità e le attività concrete per fronteggiare efficacemente l'incidente cibernetico.

Sotto un primo profilo, sembra da accogliere positivamente l'impulso alla procedimentalizzazione delle attività di gestione dei rischi e delle risposte in caso di incidenti o attacchi informatici.

Invero, la predisposizione e la adozione di tali piani in una fase fisiologica dell'azione amministrativa presuppone, a monte, un'attività di ricognizione e di analisi da parte della Amministrazione che si rivela funzionale alla comprensione dei concreti rischi potenzialmente fronteggiabili e, in generale, alla diffusione di un'effettiva cultura della cybersicurezza.

31 Cfr. Art. 7, co. 1, lett. n-bis, del d.l. n. 82/2021.

32 Art. 1, co. 2-*bis*, del d.l. n. 105/2019.

33 Art. 3, co 1, lett. g) e i), del decreto legislativo n. 65/2018.

34 Art. 40, co. 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259.

La pianificazione – nella accezione gianniniana di *attività di durata proiettata nel futuro*[35] – richiede a monte, in altri termini, una concreta presa di coscienza sul "livello di maturità della cybersicurezza"[36] da parte di ciascuna Amministrazione per garantire la adozione di misure realmente efficaci nel contesto di riferimento.

Sotto ulteriore profilo, la procedimentalizzazione consente di avere un chiaro piano di azione laddove la minaccia informatica si concretizzi, facilitando l'adozione delle azioni di risposta e, auspicabilmente, riducendo i tempi di reazione e, di conseguenza, gli eventuali effetti espansivi dell'attacco che incidono significativamente sull'Amministrazione stessa e sulle comunità di soggetti interessati.

Inoltre, il rafforzamento della dimensione collaborativa tra soggetti pubblici attraverso la procedimentalizzazione delle attività di gestione degli attacchi informatici, mostra quell'aspetto della collaborazione amministrativa intesa come il "concorso doveroso di più soggetti pubblici, tra loro distinti e separati, alla realizzazione di un fine prescritto dalla legge", ove la collaborazione non assume un carattere spontaneo, occasionale o volontaristico, ma piuttosto, essendo formalizzata, ha valore cogente, è obbligatoria e doverosa, proprio in quanto espressamente richiesta dalla legge, che impone a più soggetti pubblici di interagire all'interno di un procedimento complesso e trasversale[37].

Al riguardo, occorre rilevare che la nozione teorica di collaborazione è stata oggetto di autorevoli riflessioni, tra loro divergenti, nella scienza giuridica italiana nel corso del tempo, essendo stata qualificata, da alcuni, come espressione di tante e variate fattispecie inidonee, tuttavia, a esprimere un concetto giuridico definito[38],

35 Giannini 1983: 629, qualifica la pianificazione come "la determinazione: a) dell'ordinata temporale o di quella spaziale o di ambedue; b) dell'oggetto; c) dell'obiettivo. La pianificazione richiede sempre che si elabori un progetto, che lo si verifichi quanto alla realizzabilità, indi che si stabiliscano risorse, tempi, spazi, eventuali modi, per la realizzazione".

36 Espressione utilizzata da Longo 2024: 4.

37 Sulla *collaborazione* come "combinazione di soggetti nell'attuazione di compiti collegati, di «attività di interesse comune»; come realizzazione di un solo interesse (o fine) pubblico grazie all'apporto, necessario per legge, di più centri di potere che ne sono titolari" e sulla elaborazione della *collaborazione procedimentale* come relazione organizzativa nell'amministrazione complessa da collocare nel procedimento amministrativo e che agisce lungo tutto l'arco di determinazione della funzione e di concretizzazione dei relativi effetti, si veda D'Angelo 2022a: 190 ss. Nella stessa prospettiva, parlava di "concorso di figure che potrebbero apparire separate dalla personalità giuridica, alla produzione di una medesima attività rivolta a realizzare l'interesse dell'ordinamento" Bazoli, 1964:72. Già, Nigro 1966: 123-124 sosteneva che "Organizzazione e attività sono invece, come sappiamo, due facce della stessa moneta, due profili (due modi di essere) dello stesso sistema di istituzione e di regolazione di strumenti e di rapporti idonei a consentire il raggiungimento di determinati fini (…). [L]a collaborazione degli uffici si si esprime nella comune partecipazione all'attività amministrativa, ed a quella dell'organizzazione perché la combinazione degli uffici è solo la manifestazione della combinazione dell'azione degli stessi uffici e dei loro interessi, che è quanto soprattutto l'ordinamento vuole attuare. Il procedimento amministrativo, da una parte, è attività, o forma di attività, dall'altra ed insieme è coordinazione (azione coordinata) di uffici (cioè, di competenze, d'interessi), quindi organizzazione".

38 Si pensi alle parole di Giannini 1973: 197 che, nel trattare della "collaborazione" sostiene che essa sia un vocabolo il quale non esprime alcun concetto giuridico definito, e che

al punto, secondo altre voci, da non avere dignità teorica[39] e, da altri autori, quale concetto dotato di una propria autonomia concettuale e un significato giuridicamente rilevante e ciò anche in ragione del suo utilizzo da parte del legislatore nei testi normativi[40]. Della collaborazione è stato valorizzato, ancora, il carattere di spontaneità e l'elemento volontaristico quale espressione dell'autonomia organizzativa dei soggetti coinvolti[41], ove la collaborazione sarebbe un mero fatto, un "impegno spontaneo, volontario di soggetti diversi di concorrere, secondo le rispettive possibilità, al conseguimento di un determinato risultato"[42]. Nella molteplicità delle autorevoli ricostruzioni, appare convincente la ricostruzione della collaborazione tra autorità amministrative come "una regola normativa di azione che governa lo svolgimento delle funzioni comuni dove più soggetti, dotati di competenze distinte ma legati da relazioni organizzative procedimentali, curano un solo interesse pubblico che ad essi è cointestato; collaborando le autorità procedenti compartecipano all'esercizio del potere determinante, al potere cioè di definire il disegno legale degli effetti della funzione"[43].

In questo senso, la sicurezza e la resilienza cibernetica divengono quegli interessi propri di ciascun ente e al contempo generali, quei fini unici la cui realizzazione non può che essere condizionata dall'apporto, richiesto per legge, ai diversi soggetti pubblici che cooperano nel modo voluto dalla legge, lasciando emergere quello spirito sotteso alla collaborazione che si sostanzia nella "l'esigenza di instaurare una relazione costruttiva tra forze attive di realtà distinte"[44].

viene usato, in diritto privato, in diritto processuale, in diritto internazionale, per descrivere istituti giuridici o rapporti eterogenei, i quali richiedono poi ulteriori più precise definizioni o quantomeno determinazioni, aventi in comune un solo elemento metagiuridico, di un concorso subparitario di attività di più operatori. Tale posizione era già stata espressa dal Giannini in occasione del V Convegno di Studi di Scienza dell'Amministrazione di Varenna del 1959, in Giannini 1961: 115, ove affermava che "Io non sono riuscito a trovare né nella scienza del diritto né nella scienza dell'amministrazione un concetto di collaborazione (…) Ma per quello che io conosco attraverso i miei studi, collaborazione è un vocabolo che sta a significare semplicemente un concorso subparitario di attività (..). Qui collaborazione significa accordo di attività esecutiva, deliberativa, ecc., in cui v'è una figura soggettiva, il collaborato, che si avvale di opere di altri. Ma questo non dà luogo a ad alcuna figura giuridica, ad alcuna figura di scienza dell'amministrazione; vorrei dire che è un risultato, non è una formula organizzatoria o un rapporto. In altre parole la collaborazione, essendo una risultanza, può derivare da tante fattispecie giuridiche estremamente variate".

39 Cavallo, 2005: 368.

40 Arcidiacono 1974, 108; D'Angelo 2022b: 185.

41 Travi, 1996: 679.

42 Giovenco, 1961: 280.

43 Così, D'Angelo 2022b, al quale si rimanda per i ricchi riferimenti bibliografici. Già in D'Angelo 2022a: 203-204., l'Autore sostiene che "il contributo delle amministrazioni cooperanti si rivela decisivo per realizzare le condizioni di legittimità della funzione e degli atti cui essa mette capo. È la fattispecie precettiva che impone infatti di agire tramite quello schema di collegamento, espressione di un disegno più ampio. Ne viene che, sul piano teoretico, la collaborazione designa una regola giuridica diretta a imporre un certo assetto dell'agire amministrativo".

44 Police 2021: 72.

4. (Segue)…la legge sul rafforzamento della cybersicurezza tra collaborazione e sanzione

Nel panorama normativo più recente sul tema si inserisce anche la richiamata legge in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

L'intervento normativo si compone di 24 articoli suddivisi in due Capi – dedicati, rispettivamente alle "Disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario, di personale e funzionamento dell'agenzia per la cybersicurezza nazionale e degli organismi di informazione per la sicurezza nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici" (artt. 1-15) e alle "Disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari" (artt. 16-24) – e si propone di rispondere alla crescente offensività delle aggressioni realizzate con mezzi telematici e informatici e alla conseguente esigenza di realizzare una più intensa tutela della sicurezza cibernetica.

Limitando l'analisi ad alcune disposizioni relative al primo capo[45], la promozione della logica collaborativa sembra emergere, anzitutto, dalla previsione che amplia soggettivamente l'obbligo di notifica di incidenti rilevanti per la cybersicurezza a soggetti ulteriori rispetto a quelli già ricompresi nel perimetro di sicurezza nazionale cibernetica[46].

Al riguardo, in reazione – con ogni probabilità – al menzionato incremento delle attività ostili a scapito di target pubblici, l'obbligo di segnalazione e notifica di incidenti[47] viene coerentemente esteso alle pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni; alle regioni e province autonome di Trento e di Bolzano; alle città metropolitane; ai comuni con popolazione superiore a 100.000 abitanti e comunque ai comuni capoluoghi di regione; alle società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti; alle società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane; alle aziende sanitarie locali; alle società in house degli enti menzionati, attive in alcuni specifici settori (servizi informatici, servizi di trasporto, raccolta, smaltimento e trattamento di acque reflue e gestione dei rifiuti).

45 Per una analisi dei principali temi presenti nell'originario disegno di legge, si rimanda alla sezione monografica curata da Fiornelli & Giannelli 2024.

46 Per un commento alla normativa in materia di Perimetro di sicurezza nazionale cibernetica, di cui al d.l. n. 195/2019, conv. in l. n. 133/2019, cfr. Carotti 2020: 629-641.

47 L'art. 1, co. 1, della l. n.90/2024 specifica che gli incidenti da segnalare sono quelli indicati nella tassonomia di cui all'articolo 1, comma 3-*bis*, del decreto-legge n. 105 del 2019 che, a sua volta, richiama gli incidenti di cui all'articolo 1, comma 1, lettera h) del regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici adottato con il DPCM n. 81 del 2021 e cioè "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".

L'obbligo di notifica viene dunque esteso ad ulteriori soggetti pubblici e privati, oltre i confini soggettivi e oggettivi del Perimetro, individuabili attraverso l'utilizzo di una tecnica normativa redazionale tradizionale (e meno ambigua rispetto a quella utilizzata nel Perimetro)[48], mediante il rimando ad altre normative (*i.e.* elenco ISTAT) o alla indicazione di limiti numerici[49].

Tale obbligo di segnalazione e, poi, di notifica completa è soggetto a tempistiche stringenti e ciò, senz'altro, graverà le amministrazioni coinvolte di un onere organizzativo in termini di risorse umane, strumentali e finanziarie per assicurare una gestione adeguata del flusso informativo.

Sotto altro profilo, la circostanza che la reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica comporti una sanzione amministrativa pecuniaria da un minimo di 25.000 a un massimo di 125.000 euro a carico dei soggetti indicati al comma 1 dell'art. 1 della legge potrebbe essere letta come una intenzione del legislatore di dare autonoma rilevanza all'interesse *procedimentale* comunicativo e allo scambio di informazioni tra pubbliche amministrazioni in aggiunta alla tutela degli interessi *sostanziali* o *finali* rappresentati dalla sicurezza e resilienza cibernetica suscettibili di essere lesi in caso di attacco cibernetico.

In questo senso, il potere sanzionatorio, da esercitare anche nei confronti di altre amministrazioni pubbliche, pare connotarsi non tanto (o non solo) per essere espressione di una logica autoritativa e punitiva, quanto, piuttosto, per essere uno strumento a disposizione dell'amministrazione volto a sollecitare la doverosa collaborazione tra amministrazioni e a garantire l'effettività della stessa, a tutela del buon andamento dell'azione amministrativa[50].

In altri termini, così come avviene in numerosi settori dell'azione amministrativa, l'efficacia, l'effettività, l'efficienza, la tempestività, la trasparenza e il buon andamento dell'azione amministrativa, oltre ad essere fini verso i quali deve tendere l'azione amministrativa, rappresentano interessi pubblici procedimentali trasversali da preservare affinché le funzioni di amministrazione attiva, di vigilanza, di regolazione e di controllo in ciascun settore possano essere svolte in modo adeguato. Tali interessi sono concretamente perseguiti dalla pubblica amministrazione anche attraverso la sanzione amministrativa pecuniaria nella misura in cui quest'ultima è lo strumento individuato dal legislatore a garanzia della effettività degli obblighi procedimentali e collaborativi posti in capo ai soggetti pubblici e ai soggetti privati.

La stessa logica volta a promuovere l'effettività dell'obbligo di collaborazione pare permeare sia la disposizione dell'articolo 2 – ove si commina una sanzione pecuniaria nei casi di ritardata o mancata adozione degli interventi risolutivi proposti dall'ACN circa specifiche vulnerabilità alle quali risultino potenzialmente esposti le amministrazioni e gli enti pubblici e gli altri soggettivi indicati dall'ar-

48 Mette in luce le criticità definitorie del d.l. n. 105/2019, Carotti 2020: 640.

49 Un possibile profilo di criticità, a livello definitorio, potrebbe risultare dalla sovrapposizione di tali categorie con quelle di soggetti *essenziali* e *importanti* previste dalla Direttiva NIS II (art. 3 della Dir. UE 2022/2555), che dovrà essere recepita dagli Stati Membri entro il 14 ottobre 2024. Tale criticità è stata segnalata anche da Longo 2024: 3.

50 Sia consentito il richiamo a Terracciano 2023: *passim*.

ticolo, ivi inclusi i soggetti inclusi nel Perimetro, i soggetti NIS e Tel.Co– sia l'articolo 3 della legge che, nel prevedere norme di raccordo con il d.l. n. 105/2019, introduce un obbligo di segnalazione e notifica in capo ai soggetti inclusi nel Perimetro relativo a incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (di loro pertinenza), sanzionando la mancata collaborazione.

Al riguardo, la circostanza che il potere sanzionatorio amministrativo di tipo pecuniario dell'ACN sia esercitato nei confronti di altri soggetti pubblici per reagire alla mancata (doverosa) collaborazione o a comportamenti ostruzionistici sembra rendere recessivo il profilo punitivo-afflittivo dello strumento sanzionatorio e sembra, piuttosto, valorizzare la sanzione come strumento sollecitatorio e di stimolo alla collaborazione pubblica a garanzia dell'effettività delle funzioni svolte dall'Agenzia e, in generale, del buon andamento dell'azione amministrativa.

Ferma restando, dunque, la possibilità di ricavare nella dinamica obbligo-violazione-sanzione uno spazio di stimolo alla collaborazione, soprattutto quando il potere è esercitato nei confronti di un soggetto pubblico, si possono comunque segnalare alcuni aspetti critici riguardo al complessivo impianto sanzionatorio promosso dall'intervento normativo, con specifico riferimento al primo capo.

Sotto un primo profilo, la forbice edittale (tra i 25 e i 125 mila euro) per i soggetti privati appare estremamente bassa e tale da mettere in dubbio la reale capacità dissuasiva della sanzione, soprattutto laddove si consideri che in altri settori – come, ad esempio, per la violazione degli obblighi di segnalazione previsti dalla Direttiva NIS II[51] – il legislatore europeo ha previsto massimi edittali milionari o comunque parametrati ad una percentuale del totale del fatturato annuo mondiale della società.

Ulteriore profilo di rilievo appare essere quello legato alla destinazione delle sanzioni pecuniarie, in quanto l'art. 24 della legge si limita a prevedere che i proventi delle sanzioni siano destinati alle entrate dell'ACN mentre, in un'ottica di promozione virtuosa della collaborazione, sarebbe forse stato più opportuno prevedere un vincolo di destinazione dei proventi a progetti di formazione, di ricerca e sviluppo di prodotti e tecnologie, in modo da valorizzare l'azione dell'ACN quale attore istituzionalmente deputato a promuovere e supportare il processo di diffusione della cultura della cybersicurezza[52].

In linea più generale, ci si potrebbe poi domandare se la finalità di *rafforzamento della cybersicurezza* che la legge intende perseguire sia più efficacemente

51 Si veda l'art. 34 della Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (Direttiva NIS II).

52 Si condivide il pensiero di Rossa 2022a: 165, secondo cui "il fine ultimo della politica pubblica di cybersicurezza: non (sol)tanto proteggere le infrastrutture digitali, ma giungere a un contesto istituzionale di cyber resilienza in cui tutti gli attori coinvolti interagendo e collaborando fra loro in vista del raggiungimento di un obiettivo comune stabilito dallo Stato, diventino consci dei rischi cyber. Come intuibile, nel far ciò il ruolo dello Stato appare imprescindibile".

raggiungibile attraverso l'imposizione di nuove prescrizioni, obblighi informativi e di sanzioni in caso di inosservanza, ovvero mediante un cospicuo investimento, in termini di risorse umane e strumentali, per rafforzare la capacità di prevenzione e gestione degli eventi e degli attacchi cyber e la resilienza informatica complessiva.

Non pare ragionevole propendere in senso netto verso l'una o l'altra alternativa, ma piuttosto si ritiene che l'approccio autoritativo dovrebbe integrarsi con quello di promozione della collaborazione, della cultura della cybersicurezza e della acquisizione e diffusione delle competenze all'interno degli enti di ridotte dimensioni e in favore delle comunità di riferimento, al fine di evitare che la sanzione comminata a fronte dei mancati obblighi collaborativi finisca per essere la conseguenza di criticità organizzative radicate e di sistema, probabilmente non dipendenti (e, dunque, non imputabili) al singolo funzionario o alla singola amministrazione di riferimento.

In questo senso, come peraltro da tempo sostengono autorevoli voci, si condivide l'idea secondo la quale "il principale fattore di miglioramento dei rendimenti amministrativi dovrebbe proprio essere il suo capitale umano, per evitare di incorrere nell'errore di considerare il processo riformatore normativo più importante del cambiamento delle persone"[53]. La diffusione delle competenze nel settore pubblico e il cambiamento dell'ambiente culturale rispetto a queste tematiche appaiono essere, come emerge dai dati richiamati, l'oggetto di un processo lento e non ancora del tutto compreso, soprattutto nelle realtà territoriali più piccole, che, tuttavia, mal si concilia con l'urgenza regolatoria del settore generata dal frequente mutamento e dalla rapida espansione del fenomeno, nonché dalla complessità dello stesso.

Al riguardo, al fine di integrare l'approccio autoritativo e quello collaborativo, sarebbe forse stato opportuno prevedere un periodo transitorio, prima di rendere efficace l'apparato sanzionatorio previsto, durante il quale svolgere corsi di formazione specifica delle risorse umane, simulazioni ed esercitazioni per testare la capacità di preparazione e reazione ad incidenti o ad attacchi informatici, sul modello di quanto effettuato nel 2023 in favore delle amministrazioni del Nucleo per la cybersicurezza e dei soggetti pubblici inseriti nel Perimetro di sicurezza nazionale cibernetica[54].

Nell'analizzare le *prospettive* della collaborazione nel contesto della cybersicurezza, un ultimo breve cenno merita il tema della collaborazione pubblico-privato nella fase di approvvigionamento di beni e servizi ICT da parte delle istituzioni pubbliche[55].

Al riguardo, occorre notare che la prima versione del disegno di legge prevedeva di assegnare all'ACN un nuovo potere di promozione e di sviluppo di ogni iniziativa, anche di partenariato tra soggetti pubblici e privati, volta a valorizzare l'intel-

53 Ramajoli 2021: 451; Battini 2021, 11-14.

54 Nella Relazione Annuale al Parlamento 2023 dell'Agenzia per la cybersicurezza nazionale si legge che, al fine di rafforzare la capacità di gestione strategico-procedurale delle amministrazioni del Nucleo per la cybersicurezza e dei soggetti pubblici inseriti nel Perimetro di sicurezza nazionale cibernetica, sono state condotte 6 esercitazioni di tipo *table-top* a favore di tali organizzazioni, nonché 2 esercitazioni di carattere tecnico a favore del CSIRT Italia, che ha previsto anche l'impiego di un cyber range, ossia di ambienti virtuali nei quali possono essere simulati, a livello tecnico, reti e sistemi informativi oggetto di attacchi.

55 Al riguardo, in modo approfondito, Rossa 2022a: 167 e ss.

ligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale, anche al fine di favorire un uso etico e corretto dei sistemi basati su tale tecnologia.

Tale previsione – che è stata espunta dal testo nel corso dei lavori parlamentari e, allo stato, è stata riproposta nella più adeguata sede del disegno di legge sull'intelligenza artificiale in discussione al Senato[56] – ha il pregio di assegnare all'ACN la promozione di ogni iniziativa anche di *partenariato pubblico privato*, aprendo la via ad una più ampia collaborazione tra pubblico e privato nel contesto dei contratti pubblici anche al fine di consentire alle amministrazioni di rivolgersi al mercato, come già evidenziato in dottrina[57], per l'approvvigionamento non solo di servizi o prodotti già esistenti sul mercato ma anche per soddisfare l'esigenza di sviluppare *ex novo* prodotti, servizi o lavori innovativi di servizi innovativi, valorizzando istituti come il partenariato per l'innovazione di cui all'art. 75 del d.lgs. n. 36/2023[58].

Nel contesto della cybersicurezza, considerate la debolezza strutturale della PA nell'approvvigionamento dei beni e dei servizi e la trasversalità e l'aumento costante della minaccia e degli incidenti cyber, la riflessione sull'utilizzo dei contratti pubblici come "strumenti creatori di innovazioni" [59], già ampiamente sviluppata in dottrina[60], non sembra ancora essere stata colta pienamente dal legislatore nazionale.

5. Cenni conclusivi

A fronte di una realtà nella quale la minaccia cibernetica cresce, come visto, in termini quantitativi ed è suscettibile di impattare sul complessivo apparato amministrativo, la promozione di forme di collaborazione tra pubbliche amministrazio-

56 Si fa riferimento al disegno di legge A.S. 1146, presentato dal Governo in data 20 maggio 2024 e, al 13 giugno 2024, in corso di esame in commissione. Si veda anche il Dossier n. 289 del Servizio Studi dell'11 giugno 2024, disponibile al link *https://www.senato.it/japp/bgt/showdoc/19/DOSSIER/0/1419908/index.html*.

57 Al riguardo, Rossa 2022a: 205, rileva che uno dei vantaggi derivanti dall'utilizzo degli appalti innovativi – tra i quali il partenariato per l'innovazione ai sensi dell'art. 75 del d.lgs. n. 36/2023, è "la possibilità di soddisfare i fabbisogni pubblici in modo sartoriale, prescindendo da un bene o un servizio già esistente ma potendo invece crearne uno che risponda esattamente alle specifiche esigenze del caso particolare. Infatti, come accennato in precedenza, non sempre la soluzione che offre il mercato è la migliore o quella che serve nel caso specifico: tuttavia, ricorrere a quello che offre il mercato è tendenzialmente la scelta obbligata. Ma non se si ha la possibilità di avvalersi di appalti innovativi come il partenariato per l'innovazione. Il progettare *ab initio* una soluzione o un bene sulle reali esigenze e fabbisogni del soggetto pubblico sarebbe in modo evidente funzionale alle esigenze che possono derivare dal contesto cybersecurity pubblica, sempre in continua evoluzione134. In tal senso, gli appalti innovativi, partenariato per l'innovazione in particolare, potrebbero essere utili per sviluppare prodotti e servizi digitali cybersafe by design, ovvero rispettosi di standard di cybersicurezza già dalla loro progettazione". Condivide tale soluzione anche Longo 2024: 5.

58 Per un approfondimento di tale procedura di scelta del contraente, cfr. Senzani 2024: 413-415.

59 Auby 2022,133.

60 Kondu, James, Rigby 2022: 490-502; Licata 2019: 1 e ss.; Racca 2017:192 e ss.; Racca & Yukins 2019: 113 e ss.; Laimer, Pagliarin & Perathoner 2021: *passim.*

ni e tra privati e amministrazioni e la diffusione di una cultura della cybersicurezza appaiono necessarie per assicurare un più elevato livello di sicurezza. Esse determinano, infatti, un maggiore scambio di conoscenze, di strategie e di soluzioni tecniche, nonché una maggiore sensibilizzazione e responsabilizzazione del capitale umano all'interno delle amministrazioni e della collettività, contribuendo a ridurre la vulnerabilità dell'apparato amministrativo e le conseguenze pregiudizievoli sia per interessi pubblici sia per quelli privati.

Dalla breve analisi condotta su alcune delle più recenti tendenze normative in materia, emerge una progressiva presa di consapevolezza, da valutare con favore, circa la necessità di rafforzare l'organizzazione delle strutture e del sistema amministrativo nei diversi livelli di governo e in molteplici settori e, al contempo, promuovere una procedimentalizzazione delle attività amministrative al fine di prevenire e gestire i rischi e gli incidenti cyber, mediante l'individuazione di ruoli, responsabilità e piani di azione.

Se gli obiettivi sono senz'altro ambiziosi e condivisibili, oltre che imprescindibili per la transizione digitale, non altrettanto condivisibile e piuttosto insoddisfacente è la scelta del legislatore di pretendere di perseguire tali finalità senza nuovi o maggiori oneri a carico della finanza pubblica, come emerge dall'art. 24 della legge n. 90/2024.

Peraltro tale prassi, stigmatizzata anche rispetto ad altri interventi dalla Consulta[61], lascia in ombra quanto già espresso in più occasioni dalla Corte dei conti, ossia che la mera apposizione di clausole di neutralità non costituisce garanzia dell'assenza di nuovi o maggiori oneri e ciò, in quanto, "La mancata previsione, infatti, di costi aggiuntivi non esclude che possano effettivamente derivare dalle norme, in futuro, maggiori esigenze a legislazione vigente, con copertura a carico dei tendenziali e dunque aggravando il saldo, soprattutto a fronte di oneri di carattere obbligatorio. Tutto ciò a meno di non ritenere che le disponibilità di bilancio a legislazione vigente siano quantificate in modo da presentare già margini per la copertura di eventuali incrementi di oneri conseguenti all'implementazione delle nuove normative previste: in tal caso si determinerebbe, però, una scarsa coerenza con il principio della legislazione vigente, che, anche nel nuovo sistema contabile, costituisce il criterio per la costruzione delle previsioni di bilancio al netto della manovra, come attesta la presenza, nella legge di bilancio, della Sezione II, dedicata, appunto, alla legislazione vigente"[62].

61 Al riguardo, di recente, Corte cost., 2 maggio 2023, n. 82, ove la Corte ha ribadito, peraltro, che "la clausola di invarianza finanziaria non può tradursi in una mera clausola di stile e che, «[o]ve la nuova spesa si ritenga sostenibile senza ricorrere alla individuazione di ulteriori risorse, per effetto di una più efficiente e sinergica utilizzazione delle somme allocate nella stessa partita di bilancio per promiscue finalità, la pretesa autosufficienza non può comunque essere affermata apoditticamente, ma va corredata da adeguata dimostrazione economica e contabile» (sentenza n. 115 del 2012), consistente nell'esatta quantificazione delle risorse disponibili e della loro eventuale eccedenza utilizzabile per la nuova o maggiore spesa, i cui oneri devono essere specificamente quantificati per dimostrare l'attendibilità della copertura".

62 Corte dei conti, SS.RR. in sede di controllo, Relazione quadrimestrale sulla tipologia

Al riguardo, ci si limita ad osservare che, considerato l'apparato sanzionatorio previsto dal nuovo testo normativo, non pare potersi escludere che molte delle previsioni introdotte rappresentino oneri di carattere obbligatorio per le amministrazioni coinvolte, richiedendo alle stesse, a titolo esemplificativo, di adeguare le dotazioni *hardware* e *software* in conseguenza di eventuali segnalazioni dell'ACN di rischi di vulnerabilità informatica ovvero di svolgere nuovi compiti, come la raccolta, la elaborazione e la classificazione dei dati relativi alle notifiche di incidenti informatici in capo all'ACN, ovvero di rendere operativo il Centro nazionale di crittografia e di individuare una struttura referente per la cybersicurezza con risorse dotate di specifiche e comprovate professionalità e competenze in materia di cybersicurezza.

In conclusione, appare chiaro che l'ambizioso piano avrebbe richiesto un ingente investimento in termini di risorse finanziarie che, seppur sollecitato da più parti nel corso dei lavori parlamentari, non è stato purtroppo previsto e ciò potrebbe compromettere la sostenibilità amministrativa dell'intervento e la effettiva possibilità di realizzare il fine ultimo dello stesso, ossia il rafforzamento della cybersicurezza nazionale.

Bibliografia

Arcidiacono L. 1974, *Organizzazione pluralistica e strumenti di collegamento. Profili dogmatici*, Milano: Giuffrè.

Auby J.B. 2022, "Conclusioni", in R.C. Perin, M. Lipari & G.M. Racca (a cura di), *Contratti pubblici e innovazioni per l'attuazione della legge delega*, Napoli: Jovene: 133.

Battini, S. 2021, "Premessa", *Formare la PA. Rapporto SNA 2017-2020*, Roma: Miligraf Edizioni: 11-14.

Bazoli, G. 1964, *La collaborazione nell'attività amministrativa*, Padova: Cedam.

Benvenuti F. 1994, *Il nuovo cittadino. Tra libertà garantita e libertà attiva*, Venezia: Marsilio.

Bolognini L., Pelino E. & Scialdone M. 2023 (a cura di), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Milano: Giuffrè.

Bonetti T. 2022, *La partecipazione strumentale*, Bologna: Bologna University Press.

Borriello G. & Fristachi G. 2022, "Stato (d'assedio) digitale e strategia italiana di cybersicurezza", *Rivista di Digital Politics*, vol. II, 1-2: 157-178.

Carotti B. 2020, "Sicurezza cibernetica e Stato-nazione", *Giorn. Dir. amm.*, 629-642.

Chiappini A. 2022, "Quadro normativo in materia di sicurezza informativa e ruolo dell'Agenzia per la cybersicurezza nazionale", in G. Dalia e M. Panebianco (a cura di) 2022, *Il segreto di Stato. Una indagine multidisciplinare sull'equo bilanciamento di ragioni politiche e giuridiche*, Torino: Giappichelli Editore: 301-334.

Chirulli P. 2023 [2015], La partecipazione a procedimento, in M.A. Sandulli (a cura di), *Principi e regole dell'azione amministrativa*, Milano: Giuffrè: 399-411.

Cognetti S. 2000, *"Quantità" e "qualità" della partecipazione, Tutela procedimentale e processuale*, Milano: Giuffrè.

delle coperture e sulle tecniche di quantificazione degli oneri nel quadrimestre, maggio-agosto 2023, Delibera n. 32/2023, pp. 3 e ss.

D'Angelo F. 2022a, *Pluralismo degli enti pubblici e collaborazione procedimentale. Per una rilettura delle relazioni organizzative nell'amministrazione complessa*, Torino: Giappichelli.
D'Angelo F. 2022b, "La collaborazione amministrativa nella funzione di vigilanza (bancaria). Profili di giurisdizione e procedimentali (nota a Cass SU 20 aprile 2021, n. 10355)", *Dir. e proc. amm.*:1.
Fiornelli G. & Giannelli M. 2024, "Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2", *Rivista italiana di informatica e diritto*, 1.
Forgione I. 2022, "Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna", *Dir. Amm.*, 4, 1141.
Giannini M.S. 1983, *Pianificazione* (voce), *Enc. Dir.*, XXXIII: 629.
Giannini M.S. 1973, "Enti locali territoriali e programmazione", *Rivista Trimestrale di Diritto Pubblico*, 1: 193-218.
Giannini M.S. 1961, "Intervento", in *Coordinamento e collaborazione nella vita degli enti locali. Atti del V° Convegno di Studi di Scienza dell'Amministrazione*, Milano: Giuffrè: 114-119.
Giovenco L. 1961, "Profilo giuridico strutturale del «coordinamento» nella vita degli enti locali, in *Coordinamento e collaborazione nella vita degli enti locali. Atti del V° Convegno di Studi di Scienza dell'Amministrazione*, Milano: Giuffrè: 280-286.
Kondu O., James A. & Rigby J. 2020, "Public Procurement and innovation: a systematic literature review", *Science and Public Policy*, 47(4): 490-502.
Laimer S., Pagliarin C., Perathoner C. 2021, *Contratti pubblici e innovazione, Una strategia per far ripartire l'Europa*, Milano: Giuffrè.
Ledda F. 1993, "Problema amministrativo e partecipazione al procedimento", *Dir. Amm.*, 2: 133-172.
Licata G.F. 2019, "Contratti pubblici e innovazione", Convegno Associazione Italiana dei Professori di Diritto Amministrativo. Disponibile in *www.aipda.it*, Paper.pdf (accesso il 18 giugno 2024).
Longo E. 2024, "*Audizione informale per il disegno di legge in materia di "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717), Camera dei Deputati, Commissioni riunite I e II – Roma 28 marzo 2024*", *Riv. Italiana di Informatica e diritto*, 1: 4.
Manganaro F. 1995, *Principio di buona fede e attività delle amministrazioni pubbliche*, Napoli: Edizioni Scientifiche Italiane.
Nigro M. 1966, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano: Giuffrè.
Nigro M. 1980, "Il nodo della partecipazione", *Riv. trim. dir. proc. civ.*: 231 ss.
Police A. 2021, "Enti pubblici di Ricerca ed università: le persistenti ragioni di una differenziazione e le indifferibili esigenze di uno sforzo comune, *Nuove Autonomie*, 1: 65-79.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", *Federalismi.it*, 25: 65-93.
Racca G.M. 2017, "La contrattazione pubblica come strumento di politica industriale", in C. Marzuoli e S. Torricelli (a cura di), *La dimensione sociale della contrattazione pubblica. Disciplina dei contratti ed esternalizzazioni sostenibili*, Napoli: Editoriale Scientifica: 192 e ss.
Racca G.M. & Yukins C. (editors) 2019, "Joint Public Procurement and Innovation: Lessons Across Borders", *Droit Administratif/Administrative Law Collection*, 27, Bruxelles: Bruylant.
Ramajoli, M. 2021, "La Scuola Nazionale dell'Amministrazione agente interno dell'innovazione amministrativa", *Giornale di diritto amministrativo*, 4, 451-456.

Ricotta F.N. 2023a, "L'architettura di sicurezza cibernetica e l'Agenzia per la cybersicurezza nazionale, in G. Colaiacovo (a cura di) 2023, *Sicurezza, informazioni e giustizia penale*, Pisa: Pacini Giuridica: 356 ss.

Ricotta F.N. 2023b, "Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria", *Dir. pen. Cont. – Rivista trimestrale*, 1, 97 ss.

Rossa S. 2023a, *Cybersicurezza e pubblica amministrazione*, Napoli: Editoriale Scientifica.

Rossa S. 2023b, "Cyber attacchi e incidenti nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario", *Vergentis. Revista de Investigación de la Cátedra Internacional Conjunta Inocencio III*, 17: 161-175.

Rossa S. 2021, *Contributo allo studio delle funzioni amministrative digitali. Il processo di digitalizzazione della Pubblica Amministrazione e il ruolo dei dati aperti*, Milano: Wolters Kluwer-CEDAM.

Scoca F.G. 1990, *Contributo sulla figura dell'interesse legittimo*, Milano: Giuffrè.

Senzani D. 2024, "Il procedimento ad evidenza pubblica e le procedure di scelta del contraente", in F. Mastragostino e G. Piperata (a cura di), *Diritto dei contratti pubblici. Assetto e dinamiche evolutive alla luce del decreto legislativo n. 36/2023*, IV ed., Torino: Giappichelli: 413-415.

Spasiano M.R. 2021, "Nuovi approdi della partecipazione procedimentale nel prisma del novellato preavviso di rigetto", *Il diritto dell'economia*, 67, 105, 2: 25-54.

Tarullo S. 2008, *Il principio di collaborazione procedimentale. Solidarietà e correttezza nella dinamica del potere amministrativo*, Torino: Giappichelli.

Terracciano S. 2023, *Le sanzioni amministrative a tutela degli interessi pubblici procedimentali*, Napoli: Editoriale scientifica.

Torchia L. 2023, *Lo Stato digitale*, Bologna: Il Mulino.

Travi A. 1996, "Le forme di cooperazione interlocale, *Dir. Amm.*, 4: 673 ss.

Zito A. 1996, *Le pretese partecipative del privato nel procedimento amministrativo*, Milano: Giuffrè.