Luigi Previti

Convergenze e deviazioni in materia di cybersicurezza: implicazioni sistematiche e nuovi interrogativi

Abstract: Il lavoro si propone di evidenziare come le politiche italiane ed europee sulla cybersecurity, dopo una prima fase di disallineamento, stiano iniziando a convergere verso una visione unitaria dei rischi di cybersecurity e delle relative azioni da intraprendere, tra cui, in particolare, un più diretto e strutturato coinvolgimento del settore privato, al fine di raggiungere effettivamente un soddisfacente livello di cyber resilienza e cyber difesa. Tuttavia, l'attuazione delle linee strategiche definite a livello europeo, in parte recepite nella recente strategia italiana 2022-2026, solleva nuovi interrogativi teorici e questioni operative, che il contributo cerca di individuare, a partire da un ripensamento generale del ruolo dello Stato in questo delicato settore.

Keywords: Cybersecurity; Strategia europea; Strategia italiana; Partenariato pubblico-privato; Regolazione di mercato.

1. Premessa

Negli ultimi anni il sistema italiano di tutela della sicurezza cibernetica sta attraversando un importante processo di trasformazione e adeguamento.

La sua articolazione originaria, che faceva capo, principalmente, alle diverse strutture amministrative attive nel c.d. "Sistema di informazione per la sicurezza della Repubblica"[1], è stata incisivamente modificata, com'è noto, a seguito dell'entrata in vigore di due significativi interventi normativi.

Il primo è rappresentato dal d.l. 21 settembre 2019, n. 105, conv. dalla l. 18 novembre 2019, n 133, che ha introdotto il Perimetro di Sicurezza Nazionale Cibernetica (di seguito, anche PSNC) al fine di garantire un livello elevato di sicurezza delle reti, dei dispositivi e dei servizi *online* utilizzati dai soggetti (pub-

1 Al riguardo, si vedano la l. 3 agosto 2007, n. 124, come modificata dalla l. 7 agosto 2012, n. 133, nonché i successivi DPCM del 24 gennaio 2013 e del 17 febbraio 2017, entrambi rubricati "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". Sul sistema delineato dalla l. n. 124/2007, cfr. Franchini 2010: 431 ss.

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: 10.7413/197054760163

bliche amministrazioni ed enti privati) che esercitano una funzione o un servizio "essenziale" dello Stato[2].

Il secondo è costituito, invece, dall'introduzione, ad opera del d.l. 14 giugno 2021, n. 82, conv. dalla l. 4 agosto 2021, n. 109, dell'Agenzia per la cybersicurezza nazionale (di seguito, ACN), quale punto di riferimento fondamentale per tutti i soggetti inseriti all'interno del Perimetro, "punto di contatto unico" transfrontaliero e principale centro di attuazione della politica nazionale in materia[3].

In particolare, spetta all'Agenzia esercitare un coacervo di rilevanti compiti istituzionali, che ricomprende, tra gli altri, la predisposizione e l'aggiornamento della strategia nazionale di cybersicurezza[4], l'ispezione, l'accertamento e l'irrogazione delle sanzioni prescritte in caso di violazioni della normativa di riferimento[5], il coordinamento e la direzione del sistema di certificazione, qualificazione e valutazione della cybersicurezza dei prodotti, servizi e processi ICT[6], il rafforzamento delle capacità e delle conoscenze nel settore[7], la gestione delle crisi informatiche e il monitoraggio del verificarsi di attacchi e incidenti *cyber*[8], la promozione di attività e progetti rivolti alla formazione e alla sensibilizzazione collettiva[9].

2 In particolare, tali soggetti sono tenuti ad adottare particolari precauzioni organizzative e tecniche, più consistenti rispetto a quelle adottate da altri enti, tra i quali rientrano: *i*) l'obbligo di aggiornare, con cadenza annuale, gli elenchi delle reti, dei sistemi e dei servizi informatici; *ii*) l'obbligo di compiere analisi di valutazione del rischio di eventuali interruzioni o danneggiamenti dei sistemi e delle reti usati per la propria attività; *iii*) l'obbligo di comunicare al Centro di Valutazione e Certificazione nazionale (CVCN) istituito presso l'ACN la volontà di acquistare beni e sistemi tecnologici sul mercato, in modo tale da accertarne l'affidabilità; *iv*) l'obbligo di rispettare gli oneri di segnalazione al CSIRT Italia, in caso di incidenti o di attacchi aventi un impatto rilevante. Sull'istituzione del PSNC, si vedano, tra gli altri, Carotti 2020: 629 ss.; Mele 2020: 186 ss.; Renzi 2021: 538 ss.

3 Sui peculiari caratteri strutturali e funzionali dell'ACN, cfr. Parona 2021: 713 ss.; Serini 2022: 241 ss.; Forgione 2022: 1113 ss.

4 Il testo della suddetta strategia nazionale, adottata per il quinquennio 2022-2026, è reperibile al sito www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza.

5 Funzioni che vengono ulteriormente potenziate e coordinate, da ultimo, a seguito dell'entrata in vigore della l. 28 giugno 2024, n. 90, rubricata "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", specie con riferimento agli obblighi di notifica degli incidenti *cyber*.

6 In quanto "Autorità nazionale di certificazione della cybersicurezza" ai sensi dell'art. 58 del regolamento UE 2019/881 del 17 aprile 2019, c.d. *Cybersecurity Act*, con il compito di attuare un controllo preventivo sulla sicurezza di tuti gli acquisti di beni e sistemi ICT che supportano la fornitura di servizi e funzioni essenziali a livello nazionale.

7 In quanto "Centro nazionale di coordinamento" ai sensi dell'art. 6 del regolamento UE 2021/887 del 20 maggio 2021, con il compito di supportare il Centro europeo di competenza per la cybersicurezza nell'attività di rafforzamento delle capacità, delle conoscenze e della competitività dell'Unione nel settore.

8 Presso l'ACN opera, infatti, lo CSIRT Italia, con il compito di ricevere le segnalazioni di eventuali incidenti o attacchi cibernetici, emettere allarmi e allerte, nonché offrire assistenza operativa in situazioni di crisi.

9 Tali attività vengono espletate anche tramite il coinvolgimento di università, enti di ricerca, imprese e altre istituzioni pubbliche.

I recenti assestamenti strutturali paiono aver conferito all'architettura italiana una forma maggiormente compatta e coordinata a livello funzionale, che risulta essere sempre più orientata a soddisfare le crescenti esigenze di celerità ed efficienza dell'azione di contrasto.

Tuttavia, se si rivolge attentamente lo sguardo alle caratteristiche e alla portata delle minacce della dimensione cibernetica[10], in cui anche l'utente medio o la piccola impresa possono rappresentare *target* appetibili per i criminali informatici[11], appare opportuno continuare a interrogarsi in merito all'adeguatezza e all'effettività delle misure e degli strumenti che connotano il complessivo sistema nazionale, in gran parte rivolti nei confronti dei gestori delle infrastrutture e dei servizi digitali di maggiore importanza per la vita del Paese[12].

La presente riflessione mira ad evidenziare il valore strategico del contributo svolto dal settore privato-imprenditoriale nel delicato contesto in esame. Nello specifico, dopo aver sottolineato le principali modalità attraverso le quali, sulla falsariga delle indicazioni europee, la preziosa cooperazione tra autorità istituzionali e imprese che operano nell'ambito delle *Information and Communication Technologies* (ICT) e della *cybersecurity* può concretamente esplicarsi, verranno illustrate le più recenti iniziative avviate in tal senso a livello nazionale. Tale disamina consentirà di svolgere, in seguito, alcune considerazioni di sintesi in merito alle implicazioni sistematiche e agli interrogativi teorici che la concreta attuazione dei citati indirizzi strategici non può che suscitare, a partire dal ripensamento del ruolo finora riservato ai poteri statali nell'affrontare le nuove sfide poste dalla sicurezza informatica.

2. Il contributo degli operatori economici privati nella visione europea di cyberspazio

Nonostante il tema della sicurezza informatica sia conosciuto e discusso da tempo[13], i primi tentativi di dettare una risposta uniforme a livello sovranazionale si

10 Si pensi, ad esempio, alla diffusione a livello internazionale di quei dispositivi che appartengono al vasto insieme dell'*Internet of Things,* quale fenomeno che sta determinando, rispetto al passato, un vertiginoso aumento delle superfici di attacco e del numero dei *target* colpiti. Si pensi, ancora, alla crescente espansione della c.d. economia cybercriminale, che ha visto fiorire nel tempo un vero e proprio mercato *online* (solitamente, nel *dark web)* di prodotti e servizi volti a consumare pericolosi attacchi informatici e offerti, a costi contenuti, anche a soggetti non particolarmente esperti nell'uso delle tecnologie, in aderenza al concetto del "*Crime as a Service*". In merito al concetto del "*Crime as a Service*", si veda Paganini 2022: 67 ss. Sulla criminalità informatica e sulle connesse problematiche di diritto penale, si rinvia, per tutti, ad Amato Mangiameli, Saraceni 2019.

11 Si pensi, al riguardo, ai sempre più frequenti attacchi informatici alla *supply chain*, rivolti nei confronti di imprese di piccole e medie dimensioni con il precipuo intento di colpire imprese di grandi dimensioni di cui sono fornitori. Sull'esigenza di intervenire per migliorare il livello di alfabetizzazione digitale e di consapevolezza degli utenti della rete, cfr. Montessoro 2019: 783 ss.; Ziccardi 2019: 210.

12 Al riguardo, cfr. anche Brighi, Chiara 2021: 20 ss.

13 Cfr., tra gli altri, la comunicazione della Commissione europea del 6 giugno 2001, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, COM

rintracciano soltanto di recente, segnatamente nell'ambito delle diverse iniziative dedicate alla realizzazione del *Digital Single Market*[14].

Con questi atti l'Unione ha inteso affermare, in particolare, una propria visione strategica del cyberspazio, quale luogo virtuale aperto e sicuro per lo svolgimento delle attività economiche e sociali dei cittadini europei, improntato alla protezione e all'affidabilità dei dati, delle reti e dei prodotti informatici presenti al suo interno. Un ambito dai confini indefiniti[15], del quale si intende garantire un elevato livello di resilienza tramite l'applicazione di politiche e misure omogenee, nonché tramite un efficiente meccanismo di segnalazione degli incidenti e degli attacchi più rilevanti[16].

Nei più recenti atti di indirizzo adottati in materia, che si occupano spesso di rimarcare come la sicurezza informatica costituisca il risultato dell'intervento attivo di diversi attori (pubblici e privati)[17], pare possibile notare lo sforzo delle istituzioni dell'Unione di promuovere un più diretto e articolato coinvolgimento del settore imprenditoriale all'interno dei sistemi di prevenzione e difesa elaborati dagli Stati membri.

Sotto questa prospettiva va notato, in primo luogo, come le imprese che producono, offrono o importano prodotti tecnologici nell'Unione siano chiamate ad assumere un impegno giuridicamente vincolante, fin dal momento della progettazione, all'interno del mercato unico.

(2001) 298; nonché la comunicazione della Commissione europea del 26 settembre 2003, *Il ruolo dell'e-Government per il futuro dell'Europa*, COM (2003) 567.

14 In materia, cfr. la comunicazione della Commissione europea del 6 maggio 2015, *Strategia per il mercato unico digitale in Europa*, COM (2015) 192 final, spec. par. 3.4; la direttiva UE 2016/1148 del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, c.d. direttiva NIS 1, modificata, da ultimo, dalla direttiva UE 2022/2555 del 14 dicembre 2022, c.d. direttiva NIS 2; le comunicazioni congiunte della Commissione europea e dell'Alto rappresentante dell'Unione, rispettivamente, del 7 febbraio 2013, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN (2013) 1 final, del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte dell'UE*, JOIN (2017) 450 final, e del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN (2020) 18 final; il regolamento UE 2019/881 del 17 aprile 2019, c.d. *Cybersecurity Act.*

15 Cfr. Rodotà 2014: 3, il quale ha definito il cyberspazio come "il più grande spazio pubblico che l'umanità abbia conosciuto".

16 Sulla visione strategica dell'Unione relativa allo spazio cibernetico, si vedano Contaldo, Mula 2020: 57 ss.; Kohler 2020: 7 ss.; Bassini 2021: 319 ss.; Baroni 2022: 373 ss.

17 Si vedano, ad esempio, la comunicazione della Commissione europea del 16 dicembre 2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, par. 3.2, ove si afferma che: "La natura interconnessa del ciberspazio richiede che tutti i portatori di interessi si scambino informazioni e si assumano le proprie responsabilità specifiche, per mantenere un ciberspazio globale, aperto, stabile e sicuro", nonché la comunicazione della Commissione europea del 24 luglio 2020, *La strategia dell'UE per l'Unione della sicurezza*, COM (2020) 605 final, par. 3, ove si afferma che: "[…] la cooperazione con il settore privato è fondamentale, tanto più che l'industria possiede una parte importante dell'infrastruttura digitale e non digitale indispensabile per lottare efficacemente contro la criminalità e il terrorismo. Anche i singoli individui possono apportare il loro contributo, ad esempio creando competenze e consapevolezza per combattere la criminalità informatica o la disinformazione".

In tal senso, tali soggetti vengono obbligati, da un lato, a mettere in commercio esclusivamente beni e servizi che possiedono determinati requisiti di sicurezza contro il rischio di incidenti e di attacchi cibernetici (principio di *cybersecurity by design*); dall'altro, gli stessi sono chiamati a mantenere, nei confronti degli utenti, il ruolo di interlocutori principali durante l'intero ciclo di vita dei prodotti, collaborando con il settore pubblico nell'esercizio delle attività di controllo degli *standard* di sicurezza e assumendosi, di conseguenza, le relative responsabilità[18].

Da qui la previsione di una serie di peculiari oneri e adempimenti (verifiche *ex ante*, aggiornamenti costanti, revisioni periodiche, azioni mirate, interventi a tutela dei dati personali), tanto più stringenti quanto più elevati sono i rischi di manomissione delle applicazioni e dei dispositivi tecnologici offerti dalle imprese[19].

L'obiettivo di costruire un ecosistema *cyber* più efficiente e aperto si traduce, in secondo luogo, nella definizione di modalità più stabili e durature di cooperazione tra autorità pubbliche e settore privato, in grado di sfruttare adeguatamente le conoscenze e le capacità di analisi di quest'ultimo, "*that rival those of the world's most sophisticated intelligence agencies, including in the notoriously difficult task of attack attribution*"[20].

È sotto questa prospettiva che può essere compresa l'istituzione di alcune sedi privilegiate di raccordo di matrice europea, tra le quali: il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cybersicurezza, che intende sviluppare le risorse e le competenze dell'Unione e ridurre la sua dipendenza da Paesi terzi, impegnando le energie dei Centri nazionali di coordinamento (in Italia, l'ACN), del mondo dell'industria e delle università[21]; l'Unità congiunta per il cyberspazio (*Joint Cyber Unit*), quale piattaforma finalizzata a promuovere lo scambio di informazioni, buone pratiche e conoscenze, nonché la cooperazione tra le forze dell'ordine e della difesa, le autorità civili e diplomatiche e i privati interessati in caso di gravi attacchi o incidenti di natura transfrontaliera[22]; la rete dei Centri operativi di sicurezza (c.d. SOC, *Security Operations Center*), quale

18 In materia, cfr. anche Taddeo 2019: 351-352.

19 Il potenziamento degli obblighi e dei requisiti di sicurezza esigibili da parte dei produttori, importatori e distributori di prodotti digitali, già auspicato dalle comunicazioni congiunte del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'UE*, par. 2.2, e del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, par. 1.5., viene espressamente previsto dalla recente proposta di regolamento UE 2022/272 del 15 settembre 2022, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, COM (2022) 454 final, c.d. *Cyber Resilience Act*, approvato dal Parlamento europeo a marzo 2024. I principali obiettivi della proposta sono tre: *i)* creare le condizioni per lo sviluppo di prodotti digitali sicuri, garantendo che siano immessi sul mercato *hardware* e *software* con il minor numero di vulnerabilità; *ii)* accrescere la responsabilità degli operatori economici privati, obbligandoli ad assicurare la necessaria attività di supporto e aggiornamento dei prodotti; *iii)* migliorare il livello delle informazioni rese agli utenti in merito alla sicurezza dei beni e dei servizi da loro acquistati. Sul punto, cfr. Chiara 2023: 143 ss.

20 Così, Sales 2018: 632.

21 Cfr. il regolamento UE 2021/887 del 20 maggio 2021.

22 Cfr. la comunicazione congiunta del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, par. 2.1.

network finalizzato ad assicurare un monitoraggio costante, diffuso e in tempo reale delle intrusioni e delle anomalie informatiche nelle reti e nei sistemi di diversi portatori di interesse, anche attraverso il coinvolgimento delle PMI dell'Unione e l'utilizzo di tecnologie avanzate di intelligenza artificiale[23]. Grazie a questa rete, pensata per coordinare i diversi SOC nazionali dislocati su tutto il territorio europeo, vengono potenziate, in particolare, le capacità di rilevamento, di analisi e di condivisione dei dati relativi agli attacchi *cyber* più pericolosi, consentendo ad autorità pubbliche e soggetti privati di segnalare tempestivamente, tramite canali condivisi, minacce potenziali e in corso, prima che queste abbiano causato danni irreparabili su larga scala[24].

Già da questi esempi è possibile ricavare come, nella visione prospettica adottata in sede europea, la gestione del rischio cibernetico richieda la sperimentazione di modelli relazionali diversi rispetto a quelli tradizionali, basati non tanto (o non solo) sulla logica della difesa del "fortino" sperimentata nell'ambito della protezione della sicurezza nazionale[25], quanto su una più strutturata cooperazione tra pubblico e privato.

Tuttavia, se è evidente che la realizzazione del nuovo paradigma non può essere lasciata alla mera adesione volontaria dei soggetti interessati (specie nel breve-medio periodo), risulta necessario stabilire con quali modalità, con quali incentivi ed entro quali limiti la suddetta collaborazione deve avvenire.

In altri termini, la concreta attuazione delle ricordate linee strategiche definite in sede sovranazionale richiede la conclusione di appositi accordi contrattuali tra le parti coinvolte, volti a chiarire, tra gli altri, gli incentivi economici, la ripartizione dei rischi, le condizioni di riservatezza e le clausole di esonero da responsabilità per le imprese del settore[26].

23 Cfr. la comunicazione congiunta del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, par. 1.2.

24 Lo sfruttamento di questo *network* pubblico-privato permetterà di creare quello che viene definito in termini di "scudo europeo di sicurezza informatica" dalla recente proposta di regolamento UE del 18 aprile 2023, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza e di preparazione e risposta agli stessi, COM (2023) 209 final, c.d. *Cyber Solidarity Act*.

25 Cfr. Ursi 2022: 18 ss., il quale osserva che, nei Paesi a democrazia liberale, è il settore privato che detiene la stragrande maggioranza delle reti e delle infrastrutture digitali; in tal senso, gli obblighi introdotti dal nostro legislatore nei confronti dei soggetti ricompresi all'interno del Perimetro nazionale costituirebbero una moderna espressione del dovere di difesa della patria di cui all'art. 52, comma 1, Cost.

26 Sull'importanza dei suddetti accordi contrattuali, cfr. Bossong, Wagner 2017: 284: "*In the area of cybersecurity, other forms of risks and responsibilities beyond timely construction or reliable service provision have to be considered. Governments are also increasingly able to exert pressure to obtain 'voluntary' cooperation from business […]. But when dealing with new or advanced cyber threats, public actors often enter these partnerships as the weaker partner, reliant on specialised IT companies to define the level of vulnerability and appropriate countermeasures*", nonchè Pupillo 2018: 3, secondo il quale "*it is thus clear that new conceptual approaches to cybersecurity are required to make the behaviour of all players in this market more incentive-compatible*"; Taddeo 2019: 351.

Al riguardo occorre rilevare come l'Agenzia dell'Unione europea per la cybersicurezza (*European Union Agency for Network and Information Security*, di seguito ENISA) abbia stimolato più volte gli Stati membri ad agire in questa direzione, identificando, segnatamente, quattro principali paradigmi già presenti in Europa[27]: *i*) l'*Institutional PPP*, finalizzato ad assicurare la protezione di istituzioni e infrastrutture critiche attraverso una cooperazione di lungo periodo tra gli interessati, che si esplica, ad esempio, nello svolgimento di attività di supporto operativo, di analisi dei dati, di elaborazione di buone pratiche, di controllo degli *standard* di sicurezza e di altri servizi[28]; *ii*) il *Goal-oriented PPP*, volto a promuovere la cultura della sicurezza informatica negli Stati membri attraverso la costituzione di centri e di gruppi di scambio di conoscenze e di soluzioni pratiche su specifici argomenti[29]; *iii*) il *Service outsourcing PPP*, utile a rappresentare alle autorità pubbliche competenti le problematiche *cyber* più sentite all'interno di uno specifico contesto imprenditoriale ed a suggerire, di conseguenza, gli opportuni atti normativi e di indirizzo da adottare per risolverle[30]; *iv*) l'*Hybrid PPP*, che costituisce una combinazione del primo e del terzo modello, spesso utilizzato per affidare a qualificati enti privati funzioni e compiti che le stesse istituzioni nazionali non sono in grado di esercitare, come quelli inerenti alle attività di segnalazione e di risposta in caso di attacchi cibernetici[31].

La scelta del modello di partenariato da implementare viene lasciata, invero, ai singoli Stati membri, dal momento che "*there is no universal, simple solution that applies to all the nations for creating and developing PPP. It is rather a national issue, connected with the culture and the way how the whole political and economic system works*"[32].

Dalle richiamate proposte di partenariato è possibile ricavare, a ben vedere, gli ulteriori, rilevanti benefici derivanti dall'instaurazione di una duratura interlocuzione tra autorità pubbliche e mondo imprenditoriale, che non si apprezzano solo con riferimento allo scambio di conoscenze specialistiche e di soluzioni operative[33], ma anche in sede di elaborazione e di aggiornamento delle politiche, delle

27 Cfr. ENISA, *Public Private Partnerships (PPP). Cooperative models*, novembre 2017, par. 3 ss., reperibile in www.enisa.europa.eu.

28 Si tratta del modello diffuso in Estonia e Polonia.

29 Si tratta del modello presente in Spagna, Regno Unito, Lussemburgo, Olanda, Austria, Slovacchia.

30 Si tratta del modello che si trova in Germania e Austria.

31 Modello presente, ad esempio, in Repubblica Ceca.

32 Cfr. ENISA, *Public Private Partnerships (PPP)*, par. 3.

33 Un contributo che non va, tuttavia, sminuito, ma che risulta essere, in ogni caso, prezioso nel contesto in esame, caratterizzato da evidenti asimmetrie informative. Infatti, se, da un lato, la capillarità delle minacce *cyber* e la complessità della tecnologia in commercio rendono le imprese del settore i soggetti più qualificati a comprendere le tattiche d'attacco degli *hackers*, a individuare le principali vulnerabilità nascoste nei *software* e a suggerire alle autorità competenti le contromisure più opportune; dall'altro, la realizzazione di un circuito di sorveglianza e di allerta distribuito (c.d. *distributed surveillance*), che si basa (anche) sulla continua attività di vigilanza svolta dagli operatori economici, può ridurre notevolmente le inefficienze e i costi amministrativi sopportati dagli Stati membri per la tutela della sicurezza cibernetica nazionale. Al riguardo, cfr. Clarke, Knake 2010: 162.

linee guida, dei protocolli e degli *standard* di sicurezza[34], specie nell'ambito della protezione delle infrastrutture e dei servizi considerati "critici", gestiti nella maggior parte dei casi da soggetti privati.

In particolare, l'intervento di questi ultimi nel processo di determinazione delle politiche e delle misure vincolanti per tutti gli *stakeholders* offrirebbe certamente alle autorità competenti un valido supporto tecnico[35]; tale forma di collaborazione consentirebbe, inoltre, di evitare il rischio di perseguire ambiziosi obiettivi di resilienza attraverso l'introduzione di oneri e requisiti inidonei o eccessivi, non compatibili con il principio di proporzionalità e con la prospettiva liberale da preservare in materia[36].

Come è evidente, infatti, aziende ed enti differenti affrontano minacce, vulnerabilità e conseguenze diverse; pertanto, un'effettiva inclusione di tali soggetti nelle sedi decisionali e consultive non potrebbe che favorire la definizione di strumenti parametrati al concreto livello di rischio informatico, adeguati ai particolari contesti in cui operano le imprese e aggiornati rispetto alle innovazioni tecnologiche sopravvenute.

In altri termini, la promozione di nuove forme di cooperazione tra attori pubblici e privati nel settore in esame consentirebbe non solo una maggiore condivisione di informazioni, abilità e buone pratiche, ma anche un'auspicabile partecipazione "dal basso" al processo regolatorio, limitando il tradizionale approccio "*command and control*" per favorire forme di "*enforced self-regulation*"[37].

3. Prove di convergenza nella recente strategia nazionale in materia di cybersicurezza

L'analisi delle recenti indicazioni formulate a livello europeo consente adesso di svolgere alcune considerazioni in merito alle caratteristiche dell'attuale architettura italiana in materia di cybersicurezza.

Al riguardo è possibile rilevare che, al pari dell'originario assetto istituzionale, anche l'ecosistema nazionale ridefinito negli ultimi anni continua a caratterizzarsi, in gran parte, per un chiaro *deficit* di partecipazione degli operatori economici[38]. Una conclusione che trova fondamento nella circostanza per la quale il principale coinvolgimento del settore privato finora sperimentato ha riguardato la fase di pro-

34 Sul punto, cfr. anche Farrand, Carrapico 2018: 197 ss.

35 Cappelletti, Martino 2021: spec. 7 ss.

36 Raffiotta 2022: 13-14, il quale contrappone, all'approccio, per certi versi, "dirigista" del legislatore europeo, il modello liberale adottato dagli Stati Uniti d'America. Secondo l'A., infatti, il paradigma americano, che opera a livello federale attraverso la *Cybersecurity and Infrastructure Security Agency* (CISA), si caratterizza per "*a voluntary approach, within which there is a synergy between a 'light government touch' and a strong empowerment of private entities, including – above all – Big Techs corporations*".

37 Il punto è evidenziato, in particolare, dalla numerosa letteratura internazionale in argomento. Al riguardo, si vedano, quantomeno, Sales 2013: 1554 ss.; Tropina 2015: 9 ss.; Rosenzweig 2012.

38 Su questi profili, cfr. anche Previti 2022: 81 ss.

gettazione e di sviluppo di tecnologie e infrastrutture digitali e non anche, come invece sarebbe stato auspicabile[39], l'implementazione di forme di co-regolamentazione, specie con riferimento al processo di definizione delle regole tecniche e dei requisiti minimi di sicurezza.

Si tratta di una scelta legislativa che suscita, a ben vedere, numerose perplessità, anche in considerazione della nota dipendenza delle nostre pubbliche amministrazioni dalle capacità e dalle esperienze in ambito tecnologico-informatico possedute dalle imprese del settore, che ha rappresentato, e rappresenta ancora, una delle principali cause dei ritardi registrati dal nostro Paese nel complessivo processo di transizione digitale[40].

Le criticità evidenziate conducono ad accogliere con particolare favore le interessanti proposte contenute nella strategia italiana sulla cybersicurezza 2022-2026 – e nel relativo piano di implementazione, che contiene, nel complesso, 82 misure specifiche per le tre macro componenti delineate dalla strategia (Protezione, Risposta, Sviluppo) – adottata nel maggio 2022, quale documento programmatico di primaria rilevanza per la definizione delle priorità di intervento e delle principali sfide da affrontare nel prossimo quinquennio[41].

Oltre che per i necessari interventi nella componente "Sviluppo"[42], i documenti in esame meritano di essere apprezzati per l'introduzione di alcuni importanti assestamenti finalizzati a sfruttare le risorse conoscitive e operative degli operatori privati nell'ecosistema nazionale *cyber*. E ciò sia in relazione agli obiettivi della componente "Protezione" che in relazione agli obiettivi della componente "Risposta"[43].

Nello specifico, con riferimento al primo obiettivo, la strategia mira a potenziare il sistema di certificazione, che fa capo al Centro di Valutazione e Certificazione Nazionale (CVCN) istituito presso l'ACN e, negli ambiti di competenza, ai Centri di Valutazione del Ministero dell'Interno e della Difesa. A tal fine, viene prevista l'introduzione di una rete dei laboratori accreditati di prova (c.d. LAP), quali soggetti, pubblici e privati, chiamati a supportare le procedure di certificazione della qualità degli *asset* tecnologici utilizzati dai soggetti inclusi nel PSNC e a individuare le relative vulnerabilità[44].

39 Lauro 2021: 537 ss.; Cusenza 2023: 130 ss.

40 In merito si rinvia, *ex multis*, a Sgueo 2022.

41 Per un'analisi della nuova strategia nazionale, cfr. Matassa 2022: 625 ss.

42 Al riguardo è interessante notare che, tra le misure indicate nel citato piano di implementazione, reperibile al sito www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza, vengono ricomprese la realizzazione di un "parco nazionale della cybersicurezza" (misura 49), finalizzato allo svolgimento di attività di ricerca e sviluppo nell'ambito della *cybersecurity* e delle tecnologie digitali tramite il coinvolgimento di competenze e risorse provenienti dal settore pubblico, imprenditoriale e accademico, nonché l'implementazione di un "piano per l'industria *cyber* nazionale" (misura 51), volto a sostenere imprese e *startup* per la progettazione e la realizzazione di prodotti e servizi ad alta affidabilità.

43 Nel complesso, gli operatori privati risultano coinvolti nella realizzazione di ben 27 misure.

44 Con riferimento alla funzione di certificazione in ambito *cyber*, cfr. Bruno 2020: 11 ss.;

Allo stesso tempo, con riferimento al secondo obiettivo, viene espressamente sottolineata la necessità di sfruttare le capacità nazionali di identificazione e di risposta in caso di attacchi *cyber*, prevedendo due peculiari forme di collaborazione tra gli operatori economici e l'ACN.

La prima, di natura strutturale, riguarda l'istituzione di una rete di centri settoriali di analisi e di condivisione di informazioni rilevanti (*Information Sharing and Analysis Center*, c.d. ISAC), chiamata a supportare gli uffici dell'ACN nel predisporre e nel diffondere buone pratiche, linee guida, avvisi di sicurezza e raccomandazioni all'interno del Paese.

La seconda, di natura occasionale, contempla il coinvolgimento diretto di aziende qualificate in materia di *incident response,* a supporto delle funzioni istituzionali dello CSIRT Italia, nel caso in cui dovesse verificarsi 'una moltitudine di incidenti *cyber* di natura sistemica'.

Attraverso tali misure, l'Italia mostra dunque di voler utilizzare non solo adeguate strategie di resilienza, ma anche efficaci tattiche di difesa attiva (*active difense*), con l'intento di sviluppare, avvalendosi di una molteplicità di sorgenti di dati rilevanti e di attori responsabili, forme partecipate e tempestive di gestione delle crisi e di contrattacco[45]: una circostanza che assume contorni affatto singolari, come è evidente, nel caso in cui l'attacco informatico abbia assunto una rilevanza tale da mettere in pericolo la stessa sicurezza nazionale[46].

4. Implicazioni sistematiche e nuovi interrogativi

Le considerazioni sopra effettuate consentono adesso di trarre le implicazioni sistematiche derivanti dal progressivo processo di avvicinamento delle linee strategiche italiane in materia di cybersicurezza alle direttrici fissate negli ultimi anni a livello sovranazionale.

Da quanto si è detto è emerso come gli operatori del settore possano occupare un vero e proprio ruolo da co-protagonista all'interno del sistema multilivello di tutela della sicurezza cibernetica.

Volendo riassumere di seguito gli ambiti di effettiva implementazione della menzionata cooperazione pubblico-privato, è possibile notare come le funzioni e i processi coinvolti da tale operazione riguardino, quantomeno: *i)* la progettazione, la produzione e la fornitura di beni e servizi *online*; *ii)* lo studio, l'analisi e la conoscenza delle vulnerabilità e delle minacce informatiche; *iii)* la condivisione e lo scambio di informazioni, esperienze, buone pratiche e soluzioni operative; *iv)* la certificazione e la verifica del possesso di determinati *standard* qualitativi; *v)* il monitoraggio, il rilevamento e la gestione di crisi cibernetiche; *vi)* la regolazione normativa e tecnica, inclusi l'elaborazione e l'aggiornamento di protocolli, linee

Serini 2023: 41 ss.

45 Su punto, cfr. Gori 2019: 17 ss.

46 Sulle caratteristiche specifiche della c.d. *cyber defence*, cfr. Ursi 2023: 13 ss.

guida, codici di condotta, misure e requisiti minimi di sicurezza; *vii)* lo sfruttamento di competenze tecniche specialistiche e la formazione e l'aggiornamento del personale delle pubbliche amministrazioni.

Si tratta, con evidenza, di un coinvolgimento potenzialmente molto esteso, che abbraccia ambiti particolarmente ampi e importanti, come quello, più tradizionale e sperimentato, dello sviluppo tecnologico, quello, più delicato e operativo, della gestione e della difesa, nonché quello, più strategico e complesso, della prevenzione e della resilienza.

Orbene, se quella appena delineata rappresenta la direzione verso la quale le politiche europee e nazionali in materia di cybersicurezza stanno lentamente convergendo, l'attuale processo di assestamento dell'architettura italiana pare poter costituire l'occasione per affrontare alcuni rilevanti interrogativi di fondo.

Il primo interrogativo riguarda la possibilità di continuare a gestire le peculiari problematiche connesse alla salvaguardia della pubblica sicurezza nel cyberspazio tramite moduli operativi e organizzativi ispirati, seppur in maniera ridotta rispetto alla disciplina previgente, a logiche e principi tipici del settore della sicurezza nazionale[47].

Al contrario, anche alla luce delle richiamate indicazioni di matrice europea, sembra ragionevole sostenere come nel contesto in esame il raggiungimento di un soddisfacente livello di resilienza e difesa richieda l'adozione di schemi e misure tipici di un settore aperto e multipartecipato, che assume sempre più le sembianze di un vero e proprio mercato di beni e servizi, rispetto al quale è necessario assicurare certezza giuridica e preservare la fiducia degli utilizzatori e degli utenti[48].

A tale considerazione si aggiunga che l'integrazione di attori privati nell'articolato sistema di sicurezza cibernetica rappresenta, nel nostro ordinamento, più un'esigenza strutturale, specie nel breve-medio periodo, che una libera presa di posizione; e ciò in considerazione della nota condizione di debolezza tecnologica e informatica in cui versa la gran parte delle pubbliche amministrazioni italiane e, di conseguenza, del frequente ricorso allo strumento dell'esternalizzazione.

Il secondo interrogativo, strettamente connesso al primo, attiene, invece, al possibile ripensamento del ruolo finora attribuito allo Stato all'interno del nuovo contesto istituzionale[49].

47 Si pensi, in tal senso, alla perdurante centralità delle attribuzioni affidate al Presidente del Consiglio dei ministri dal d.l. n. 82/2021, alla segretezza dell'elenco dei soggetti inseriti all'interno del PSNC ai sensi del d.l. n. 105/2019, all'operazione di centralizzazione delle funzioni istituzionali realizzata con l'istituzione dell'ACN, continuata, invero, anche dalle recenti modifiche introdotte dalla citata l. n. 90/2024.

48 Si pensi, in tal senso, alle politiche di *risk management* e di *risk regulation* mutuate dall'ambito privatistico, così come alla normativa multilivello in materia di certificazioni. Al riguardo, cfr. anche Serini 2023: 46, secondo il quale la stessa disciplina europea suggerisce che l'infrastruttura logica e materiale del cyberspazio può essere interpretata come "un agglomerato di prodotti, processi e servizi che attengono alle tecnologie dell'informazione e della comunicazione che circolano nel mercato globale".

49 In materia, si vedano anche le recenti e interessanti considerazioni di Casini 2020; Torchia 2023.

Al riguardo, se è, da un lato, comprensibile una certa difficoltà nel pronunciare quella "confessione di fallimento"[50] nel gestire e assicurare, con autonomia di decisioni e risorse, la sicurezza pubblica nel cyberspazio, occorre domandarsi, dall'altro, quale compito possa essere riservato alle autorità nazionali laddove le caratteristiche del fenomeno implicano, come si è visto, l'attuazione di politiche e di meccanismi di redistribuzione e condivisione del rischio tra tutti i soggetti coinvolti nel processo di sicurezza (dalla progettazione del dispositivo tecnologico fino alla difesa in caso di attacchi).

Si tratta, a ben vedere, di un interrogativo di particolare complessità, in relazione al quale, probabilmente, non è dato rinvenire una soluzione soddisfacente *a priori*, potendosi unicamente escludere il ritorno a un ambiente "incontaminato", caratterizzato dall'assenza di regole e vincoli giuridici da parte degli Stati[51].

In prima battuta, si sarebbe tentati di rispondere al quesito invocando l'attuazione del modello, dominante in Italia nell'ultimo trentennio, dello "Stato regolatore", che si riserva un ruolo di garante del funzionamento dei settori economici e di vigilanza sulla corretta applicazione delle regole (in questo caso, di sicurezza) dettate per i singoli mercati, limitando, se non necessario, il proprio intervento proattivo nei processi produttivi[52].

Eppure, una delle più celebri elaborazioni dottrinali che ha indagato il rapporto tra potere statale e sviluppo tecnologico non esita ad assegnare allo Stato il ruolo di protagonista dell'innovazione (c.d. "Stato innovatore"), dal momento che quest'ultimo rappresenterebbe l'unico soggetto in grado di assumersi, per primo, il rischio di impresa (*i.e.* l'incertezza del successo) e di investire ingenti risorse a lungo termine, nell'ottica del perseguimento di importanti benefici per la collettività. Secondo tale teoria, infatti, è l'autorità nazionale a dover intervenire, in prima persona, per coinvolgere e stimolare le imprese interessate a sviluppare nuova tecnologia, stabilendo chiaramente, in primo luogo, gli obiettivi strategici da raggiungere e socializzando, poi, i costi e i ricavi dell'operazione promossa[53].

Applicando la menzionata impostazione al settore della cybersicurezza, parte della dottrina ha così sostenuto che l'intervento statale, lungi dall'assumere il ruolo di arbitro e di mero regolatore delle dinamiche di mercato, dovrebbe tendere a implementare forme e meccanismi di c.d. "collaborazione orientata", ossia indirizzata al perseguimento degli indirizzi di lungo periodo predefiniti dalle istituzioni pubbliche[54].

50 Monti 2020: 75. Sulle inevitabili difficoltà che i pubblici poteri incontrano nel regolare le relazioni e i rapporti umani che hanno luogo nello spazio virtuale, si vedano, da ultimo, Mannoni, Stazi 2021; Betzu 2022.

51 Cfr. Pollicino 2023: 415, il quale sottolinea, al contrario, la recente tendenza degli Stati a "iper-regolare" il cyberspazio.

52 Cfr. La Spina, Majone 2000; D'Alberti, Tesauro 2000; Police 2007.

53 In tal senso, Mazzucato 2020 [2013]: spec. 15 ss.

54 Cfr. Rossa 2023: spec. 207 ss., secondo il quale, per assicurare la cybersicurezza delle reti e delle infrastrutture digitali utilizzate a fini pubblici, uno degli strumenti più adeguati sarebbe rappresentato dagli appalti innovativi (e, in particolare, dal partenariato per l'innovazione), che consentirebbe alle stazioni appaltanti e agli operatori privati fornitori di tecnologia di co-

In tal senso, spetterebbe allo Stato esercitare un'importante funzione pianificatoria, che si traduce nella fissazione delle priorità di intervento, degli obiettivi di interesse generale, degli strumenti, dell'orizzonte temporale e delle risorse economiche necessari, evitando così di venire "catturato" dagli interessi particolari di cui è portatore il produttore o il fornitore del bene o del servizio tecnologico.

In ogni caso, a prescindere dalle scelte di politica economica e finanziaria compiute dall'ordinamento[55], rimane ferma la necessità di definire, tra i diversi soggetti coinvolti nel sistema di sicurezza cibernetica, un equilibrato assetto di interessi, che assegna agli attori istituzionali l'individuazione delle linee strategiche e che, al contempo, ingloba gli operatori privati, secondo modalità variegate, nel processo di attuazione.

Questo passaggio appare, in definitiva, l'unica alternativa possibile per raggiungere, nel lungo periodo, una stabile e consolidata "sovranità tecnologica" a livello nazionale ed europeo, che non dipenderà solamente dall'ammontare e dalla destinazione degli investimenti finanziari dei prossimi anni, ma anche dalla sapiente inclusione delle risorse e delle competenze esistenti nell'attuale tessuto sociale.

Bibliografia

Amato Mangiameli A.C., Saraceni G. (a cura di) 2019, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino: Giappichelli.

Baroni M. 2022, "Intelligenza artificiale e cybersicurezza in una prospettiva costituzionale", in G. Cerrina Feroni, C. Fontana, E.C. Raffiotta (a cura di), *AI Anthology*, Bologna: Il Mulino: 373 ss.

Bassanini F., Napolitano G., Torchia L. 2021, *Lo Stato innovatore. Come cambia l'intervento pubblico nell'economia*, Bologna: Il Mulino: spec. 231 ss.

Bassini M. 2021, "Cybersecurity", in M.T. Paracampo (a cura di), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino: Giappichelli: 319 ss.

Betzu M. 2022, *I baroni del digitale*, Napoli: Editoriale scientifica.

Bossong R., Wagner B. 2017, "A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union", in *Crime, Law and Social Change*, 67 (3): 284.

Brighi R., Chiara P.G. 2021, "La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea", in *Federalismi.it*, (21): 20 ss.

Bruno B. 2020, "Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali", in *Federalismi.it*, (14): 11 ss.

creare il bene o il servizio necessario, dotato di caratteristiche *cybersafe by design*, evitando al contempo il verificarsi delle conseguenze negative legate alla produzione del c.d. effetto *lock-in*.

55 Si tratta di politiche che sono spesso legate alle contingenze temporali e alle diverse caratteristiche (storiche, politiche, culturali, ecc.) dei singoli Paesi. Per una disamina della recente evoluzione delle politiche italiane di promozione dell'iniziativa economica privata, anche con riferimento al settore dell'innovazione tecnologica, cfr. Bassanini, Napolitano, Torchia 2021: spec. 231 ss.

Cappelletti F., Martino L. 2021, "Achieving robust European cybersecurity through public-private partnerships: approaches and developments", in *Elf discussion paper*, (4): spec. 7 ss.
Carotti B. 2020, "Sicurezza cibernetica e Stato nazione", in *Giornale di diritto amministrativo*, (5): 629 ss.
Casini L. 2020, *Lo Stato nell'era di Google. Frontiere e sfide globali*, Milano: Mondadori.
Chiara P.G. 2023, "Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali", in *Rivista italiana di informatica e diritto*, (1): 143 ss.
Clarke A., Knake R.K. 2010, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: HarperCollins Publishers: 162.
Contaldo A., Mula D. (a cura di) 2020, *Cybersecurity Law*, Pisa: Pacini: 57 ss.
Cusenza G. 2023, "I poteri dell'Agenzia per la Cybersicurezza Nazionale: una nuova regolazione del mercato cibernetico", in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 130 ss.
D'Alberti M., Tesauro G. (a cura di) 2000, *Regolazione e concorrenza*, Bologna: Il Mulino.
Farrand B., Carrapico H. 2018, "Blurring public and private: cybersecurity in the age of regulatory capitalism", in O. Bures, H. Carrapico (editors), *Security Privatization. How non-security-related Private Businesses Shape Security Governance*, Cham: Springer: 197 ss.
Forgione I. 2022, "Il ruolo strategico dell'Agenzia nazionale per la cybersicurezza nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna", in *Diritto amministrativo*, (4): 1113 ss.
Franchini M. 2010, "Il sistema nazionale delle informazioni per la sicurezza e l'autorità delegata", in *Giornale di diritto amministrativo*, (4): 431 ss.
Gori U. 2019, "Nuovi approcci alla sicurezza cibernetica: la diplomazia preventiva come strumento di difesa attiva", in U. Gori (a cura di), *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Milano: Franco Angeli: 17 ss.
Kohler C. 2020, "The EU Cybersecurity Act and European standard: an introduction to the role of European standardization", in *International Cybersecurity Law Review*, (1): 7 ss.
La Spina A., Majone G. 2000, *Lo Stato regolatore*, Bologna: Il Mulino.
Lauro A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", in *La Rivista Gruppo di Pisa*, (3): spec. 537.
Mannoni S., Stazi G. 2021, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli: Editoriale scientifica.
Matassa M. 2022, "Una strategia nazionale a difesa del cyberspazio", in *P.A. Persona e amministrazione*, (2): 625 ss.
Mazzucato M. 2020 [2013], *Lo Stato Innovatore. Sfatare il mito del pubblico contro il privato,* trad. it. a cura di F. Galimberti, Roma-Bari: Laterza: spec. 15 ss.
Mele S. 2020, "Il Perimento di sicurezza nazionale cibernetica e il nuovo 'golden power'", in G. Cassano, S. Previti (a cura di), *Il diritto di internet nell'era digitale*, Milano: Giuffrè: 186 ss.
Montessoro P.L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Istituzioni del Federalismo*, (3): 783 ss.
Monti A. 2020, "Internet e ordine pubblico", in G. Cassano, S. Previti (a cura di), *Il diritto di internet nell'era digitale*, Milano: Giuffrè: 75.

Paganini P. 2022, "Cybercrime-as-a-Service: EU Perspectives", in L. Martino, N. Gamal (a cura di), *European Cybersecurity in Context. A Policy-Oriented Comparative Analysis*, Elf study: 67 ss.
Parona L. 2021, "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale di diritto amministrativo*, (6): 713 ss.
Police A. 2007, *Tutela della concorrenza e pubblici poteri*, Torino: Giappichelli.
Pollicino O. 2023, voce "Potere digitale", in *Enciclopedia del diritto. Potere e Costituzione*, V, Milano: Giuffrè: 415.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi.it*, (25): 81 ss.
Pupillo L. 2018, "EU Cybersecurity and the Paradox of Progress", in *CEPS policy insights*, (6): 3.
Raffiotta E.C. 2022, "Cybersecurity regulation in the European Union and the issues of Constitutional Law", in *Rivista AIC*, (4): 13-14.
Renzi A. 2021, "La sicurezza cibernetica: lo stato dell'arte", in *Giornale di diritto amministrativo*, (4): 538 ss.
Rodotà S. 2014, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari: Laterza: 3.
Rosenzweig P. 2012, *Cyber Warfare: How Conflict in Cyberspace is Challenging America and Changing the World*, Westport: Praeger Press.
Rossa S. 2023, *Cybersicurezza e pubblica amministrazione*, Napoli: Editoriale Scientifica: spec. 207 ss.
Sales N.A. 2013, "Regulating Cyber-Security", in *Northwestern University Law Review,* 107 (4): 1554 ss.
Sales N.A. 2018, "Privatizing Cybersecurity", in *UCLA Law Review,* 65 (3): 632.
Serini F. 2022, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", in *Federalismi.it*, (12): 241 ss.
Serini F. 2023, "La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana", in *Rivista italiana di informatica e diritto*, (2): 41 ss.
Sgueo G. 2022, *Il divario. I servizi pubblici digitali tra aspettative e realtà*, Milano: Egea.
Taddeo M. 2019, "Is Cybersecurity a Public Good?", in *Minds & Machines*, (29): 351-352.
Torchia L. 2023, *Lo Stato digitale. Una introduzione*, Bologna: Il Mulino.
Tropina T. 2015, "Public-private collaboration: Cybercrime, cybersecurity and nationals security", in T. Tropina, C. Callanan (eds.), *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*, Cham: Springer: 9 ss.
Ursi R. 2022, "La difesa: tradizione e innovazione", in *Diritto Costituzionale*, (1): 18 ss.
Ursi R. 2023, "La sicurezza cibernetica come funzione pubblica", in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 13 ss.
Ziccardi G. 2019, "La cybersecurity nel quadro tecnologico (e politico) attuale", in G. Ziccardi, P. Perri (a cura di), *Tecnologia e diritto*, III, Milano: Giuffrè: 210.