La cybersicurezza nell'ottica dell'interesse pubblico

Piergiacomo Mastellone
(Dottore magistrale in Giurisprudenza – Università degli Studi di Napoli Federico II)

Abstract

La sempre maggiore pervasività con cui le tecnologie digitali irrompono nel funzionamento del sistema Paese, rende sempre più attuale l'equazione secondo cui una prosperità economico-sociale è direttamente proporzionale ad un adeguato livello di robustezza e sicurezza delle infrastrutture digitali e ad alta intensità tecnologica, che ne consentono il funzionamento. Il presente contributo intende, in primo luogo, offrire una analisi dell'attuale architettura nazionale di sicurezza cibernetica, partendo da una ricostruzione storica dei principali interventi comunitari e nazionali che ne hanno ispirato le fondamenta fino ad arrivare ai più recenti e rilevanti cambiamenti. In secondo luogo, prendendo spunto da un analogo dibattito dottrinale già sorto negli Stati Uniti, si sostiene la necessità di riconnettere la cybersicurezza alla nozione di bene pubblico, attraverso una individuazione di responsabilità condivise tra pubblico e privato e grazie ad una lettura universale di tale concetto. La recente Strategia Nazionale per la Cybersecurity 2022-2026, infatti, offre un interessante appiglio a tale tipo di considerazione, evocando il ruolo essenziale a cui tutti – apparati statali, mondo delle imprese, università, cittadinanza – sono chiamati a rivestire nel preservare le infrastrutture cibernetiche del nostro Paese.

The ever-increasing pervasiveness with which digital technologies are breaking into the functioning of the country's system makes the equation that an economic-social prosperity is directly proportional to an adequate level of robustness and security of the digital and technology-intensive infrastructures, that enable its operation increasingly relevant. This contribution intends, first, to offer an analysis of the current national cybersecurity architecture, starting with a historical reconstruction of the main EU and national interventions that inspired its foundations up to the most recent and relevant changes. Second, taking a cue from a similar doctrinal debate that has already arisen in the United States, it argues for the need to reconnect cybersecurity to the notion of a public good, through an identification of shared public-private responsibilities and through

a universal reading of this concept. The recent National Cybersecurity Strategy 2022-2026, in fact, offers an interesting foothold for such a consideration, evoking the essential role that everyone - state apparatuses, the business world, academia, citizenship - is called upon to play in preserving our country's cyber infrastructure.

Sommario: 1. Il complesso intreccio tra tecnica e diritto **2.** Le nuove esigenze di tutela: la cybersicurezza **3.** Il percorso normativo: dalla direttiva "NIS" al d.l. 82/2021 **3.1.** La Direttiva "NIS" e l'impatto del suo recepimento sul sistema italiano di sicurezza cibernetica **3.2** Il d.l. 105/2019 e il ruolo del *golden power* **3.3** Il d.l. 82/2021 e i più recenti interventi in Italia **4.** L'Agenzia nazionale per la *cybersecurity*: natura, poteri e funzioni **5.** Una infrastruttura cibernetica sicura è un bene pubblico?

1. Il complesso intreccio tra tecnica e diritto

Tra le tante questioni che da sempre animano il dibattito dottrinale, quella sul rapporto tra diritto e tecnica riscuote certamente un particolare interesse[1] e, alla luce delle più recenti e rapide evoluzioni sociali e tecnologiche, una importanza vitale[2]. Se posto nell'orbita del diritto amministrativo, tale complesso intreccio può essere analizzato in due diverse prospettive: la prima è quella relativa al peso che la tecnica ha sulla definizione dell'indirizzo politico e sul contenuto dell'azione amministrativa in sede di emanazione del provvedimento, incidendo sulle modalità concrete con cui questa soddisfa gli interessi alla cui tutela è preposta; la seconda, invece, è relativa all'effetto dirompente che può aversi sulla dimensione organizzativa degli apparati pubblici e sul loro *modus operandi*, andando incontro a quella tanto invocata esigenza di digitalizzazione della P.A, ancora ben lungi dall'essere realizzata[3]. Nell'ambito della prima questione, conducendo una analisi di carattere generale su quanto avviene "a

---

[1] Si veda, tra i tanti, N. Irti, E. Severino, *Dialogo su diritto e tecnica*, Bari, 2001. Tale lavoro mette a confronto due diverse concezioni nei rapporti di prevalenza tra diritto e tecnica. In estrema sintesi, secondo Severino, è la tecnica la forza che guida ed anima il mondo ed è dunque capace di offrire una propria "normatività"; mentre secondo Irti, invece, il diritto mantiene la sua capacità di condizionamento sui fenomeni del mondo ed è quindi capace di orientarne i destini.
Per una considerazione filosofica generale sul ruolo della tecnica nella società e del suo rapporto con l'uomo ed il diritto si veda U. Galimberti, *Psiche e techne, l'uomo nell'età della tecnica,* Milano, 2000.

[2] Sempre sul rapporto tra diritto e tecnica si veda G. Finocchiaro, *Riflessioni su diritto e tecnica*, in *Dir. inf. inform.*, 2012, 4, 831, la quale ritiene che "*il diritto (o la politica, in taluni casi) debba stabilire gli obiettivi (se non addirittura i valori) e che la tecnica debba essere il mezzo per raggiungerli. La tecnica deve essere etero-diretta o quanto meno dall'esterno controllata*".

[3] Sui rilievi critici mossi in tal senso si veda F. Caio, *Lo Stato del digitale*, Padova, 2014. L'autore, infatti, ben descrive lo stato attuale delle politiche di digitalizzazione della P.A. nel nostro paese, affermando che il fenomeno riformatore rischia di trasformarsi in una mera *"digitalizzazione di facciata che ha semplicemente trasferito fogli di carta dentro i computer"*. Sul tema si veda anche E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale,* in *Dir. pubbl.*, 2019, 2.

monte" – ossia in sede di definizione dell'indirizzo politico – non si può certo negare che "*la tecnica e le sottese conoscenze scientifiche non sono, né possono essere, estranee all'atto politico, in quanto ne forniscono la necessaria base cognitiva ed operativa, che costituisce il fondamento per la costruzione di efficaci e coerenti politiche pubbliche*"[4]. Le sempre maggiori esigenze di specializzazione, a fronte di un amplificarsi della complessità dei problemi che emergono dalla realtà[5], impongono un serrato confronto tra il decisore pubblico e chi è detentore di saperi tecnici e specialistici, con la conseguenza inevitabile che quella conoscenza "esterna" confluisce nella definizione dell'indirizzo politico che i vertici amministrativi adottano nell'orientare l'attività burocratica di loro competenza[6]. Venendo a quanto avviene "a valle" – con ciò riferendosi alla decisione amministrativa vera e propria che si estrinseca nel provvedimento – il ricorso alla tecnica si affianca alla complessa attività di ponderazione degli interessi cui è propriamente chiamata l'amministrazione. Anche nell'esercizio di una discrezionalità "pura" è spesso necessario l'ausilio di determinati ambiti della conoscenza (scientifici, ingegneristici, informatici etc.) per addivenire alla scelta "preferibile", posta l'inesattezza e l'incertezza che avvolge la tutela dell'interesse concreto. La tecnica, dunque, diviene indispensabile per vedere assolto quel dovere di completezza dell'istruttoria che rappresenta una delle applicazioni concrete del principio di buon andamento di cui all'art. 97 della Costituzione[7]. Il complesso intreccio tra tecnica e attività amministrativa si coglie nella controversa nozione di "discrezionalità tecnica"[8]. Questo con-

---

[4] W. Giulietti, *Tecnica e politica nelle decisioni amministrative composte,* in *Concorrenza e mercato*, 2017, 2.

[5] Sul tema del governo della complessità e del rischio connesso ad un inadeguato bilanciamento con le esigenze di semplificazione si veda R. Spagnuolo vigorita, *Amministrare la complessità, complessità da amministrare. Una introduzione* in S. Tuccillo, (a cura di), *Semplificare e liberalizzare. Amministrazione e cittadini dopo la legge 124 del 2015,* Napoli, 2016.

[6] Sul tema della "guida" tecnica nella definizione dell'indirizzo politico si veda si veda S. Civitarese Matteucci, L. Torchia, *La tecnificazione dell'amministrazione,* in L. Ferrara, D. Sorace (a cura di), *A 150 anni dall'unificazione amministrativa italiana,* Firenze, 2016, 5.

[7] Per un'ampia disamina in tal senso si veda V. Bachelet, *L'attività tecnica della Pubblica Amministrazione*, Milano, 1967.

[8] Sullo stesso conio dell'espressione non poche sono state le oscillazioni sia legislative, vista l'espressione *"valutazioni tecniche"* utilizzata in prima battuta dalla l. 241/90 e modificata nel 2005 con l'attuale formula "*discrezionalità tecnica"*, sia giurisprudenziali, si vedano Cons. Stato, Sez. IV, 11 novembre 2010, n. 8023, e Cons. Stato, Sez. V, 04 dicembre 2012, n. 6219. Per una disamina accurata dell'evoluzione del concetto si veda-

cetto fa riferimento ad un'attività della pubblica amministrazione che non riguarda una scelta fatta in nome dell'interesse pubblico a seguito di un contemperamento dei vari interessi contrapposti, ma un giudizio a mezzo di criteri tecnico-scientifici, non giuridici[9]. Tale attività valutativa lascia ampio margine di opinabilità in assenza di una certezza all'interno della relativa comunità scientifica e professionale e che solo indirettamente produce una ricaduta sull'interesse pubblico[10]. Tali tipi di scelte sono fatte *"non considerando e ponderando i diversi interessi in gioco ma soltanto in vista della soluzione tecnicamente preferibile"*[11]. L'evoluzione giurisprudenziale sui limiti e sui criteri di sindacabilità degli atti frutto di tali processi decisionali ha contribuito a definire il perimetro della definizione. La giurisprudenza amministrativa, infatti, dapprima ha sposato un regime di controllo di legittimità basato sul mero *iter* logico della decisone in termini di ragionevolezza (cd. "controllo debole"); successivamente, tale potere si è esteso anche alla attendibilità e correttezza del criterio tecnico utilizzato (cd. "controllo forte")[12]. Da questo punto di vista, appare

---

no A. Giusti, *Contributo allo studio di un concetto ancora indeterminato. La discrezionalità tecnica della pubblica amministrazione,* Napoli, 2007; F. Merloni, *Le attività conoscitive e tecniche delle amministrazioni pubbliche. Profili organizzativi,* in *Diritto pubblico*, 2013, 2, 481.

[9] Per un magistrale inquadramento della materia si veda M. S. Giannini, *Il potere discrezionale della pubblica amministrazione. Concetto e problemi*, Milano, 1939, 77; sullo specifico tema della discrezionalità tecnica, l'Autore, sostenendo che la ponderazione tra interessi costituisce il nucleo principale della funzione amministrativa, definisce la discrezionalità tecnica come "*pseudodiscrezionalità*", denunciando la mancanza in quest'ultima del momento volitivo proprio della discrezionalità amministrativa quale è il contemperamento degli interessi in gioco ai fini del soddisfacimento dell'interesse pubblico.
In tema di discrezionalità tecnica si veda, ancora, F. Cammeo, *La competenza di legittimità della IV Sezione e l'apprezzamento dei fatti valutabili secondo criteri tecnici*, in *Giur. it*., 1902, 3, 277; E. Presutti, *Discrezionalità pura e discrezionalità tecnica*, in *Giur. it*., 1910, 4, 17; O. Ranelletti, *Attività amministrativa e attività tecnica della pubblica amministrazione*, in *Scritti giuridici scelti*, Napoli, 1992, 3; F. Salvia, *Attività amministrativa e discrezionalità tecnica* in *Scritti in onore di Pietro Virga,* Milano, 1994, 1; D. De Petris, *Valutazione amministrativa e discrezionalità tecnica,* Padova, 1995; C. Videtta, *L'amministrazione della tecnica. La tecnica fra procedimento e processo amministrativo,* Napoli, 2008; F. Liguori, *La discrezionalità tecnica nel pensiero di Errico Presutti: una categoria «a tempo»,* in *Nomos*, 2022, 1.

[10] Sulla differenza tra discrezionalità tecnica e discrezionalità pura si veda G. Tropea, *Il vincolo etnoantropologico tra discrezionalità tecnica e principio di proporzionalità: "relazione pericolosa" o attrazione fatale?* in *Dir. proc. amm*. 2012, 2, 717.

[11] D. Sorace, *Il diritto delle amministrazioni pubbliche,* Bologna, 2021, 327.

[12] Si vedano, tra le altre: Cons. Stato, Sez. V, 13 febbraio 2006, n. 829; Cons. Stato, Sez. IV, 5 marzo 2010, n. 1274 per la tesi del "controllo debole"; mentre un'apertura verso il "controllo forte" la vediamo in Cons. Stato, Sez. VI, 11 giugno 2018, n. 3526 e, su tutte,

emblematica l'attività svolta dalle Autorità amministrative indipendenti, le quali, agendo in posizione di neutralità in quanto non attributarie di un interesse pubblico specifico e concreto, esercitano un potere di regolazione di un determinato settore economico proprio attraverso norme di discrezionalità tecnica[13].

Da quanto emerso dalla breve ricostruzione appena sopra tratteggiata, il rapporto tra diritto e tecnica si palesa fondamentale tanto nella definizione dell'indirizzo politico quanto nel concreto atteggiarsi del contenuto della decisione amministrativa. La tecnica, però, è capace di incidere anche sull' organizzazione amministrativa, essendo quest'ultima una parte essenziale del modo di essere delle amministrazioni pubbliche e il cui funzionamento incide in concreto sul grado di soddisfazione dell'interesse pubblico. Le *In-*

Cons. Stato, Sez. un. , 20 gennaio 2014, n. 1013. Sugli ultimi approdi giurisprudenziali in materia si vedano: Cons. Stato, Sez. VI, 25 febbraio 2019, n.13212; Cons. Stato, Sez. VI, 19 luglio 2019, n. 4990; per un'analisi condotta su di esse si veda A. Giusti, *Tramonto o attualità della discrezionalità tecnica? Riflessioni a margine di un' "attenta riconsiderazione" giurisprudenziale,* in *Dir. proc. amm.*, 2021, 2, 335 e V. Giuffrida, *Sul trattamento giurisdizionale della discrezionalità tecnica,* in *Foro amm.,* 2021, 10, 1478. In quest'ultima opera, in particolare, viene riproposta anche una interessante sentenza del Consiglio di Giustizia amministrativa per la Regione Siciliana, la n. 406 del 7 maggio 2021, la quale identifica la discrezionalità tecnica come "*manifestazione di giudizio, consistente in una attività diretta alla valutazione ed all'accertamento di fatti*" in cui "*l'Amministrazione applica concetti non esatti, ma opinabili, con la conseguenza, già evidenziata, che può ritenersi illegittima solo la valutazione che, con riguardo alla concreta situazione, possa ritenersi manifestamente illogica, vale a dire che non sia nemmeno plausibile*".

Sul tema si veda anche V. Ottaviano, *Giudice ordinario e giudice amministrativo di fronte agli apprezzamenti tecnici dell'amministrazione,* in *Studi in memoria di Vittorio Bachelet*, Milano, 1987, 2, 405; M. Della Scala, *L'evoluzione del sindacato del giudice amministrativo sulle valutazioni tecnico-discrezionali* in V. Cerulli Irelli, L. De Lucia (a cura di) *L'invalidità amministrativa,* Torino, 2009, 263; M. Allena, *Il sindacato del giudice amministrativo sulle valutazioni tecniche complesse: orientamenti tradizionali versus obblighi internazionali,* in *Dir. proc. amm.* , 2012, 1, 1602; F. Volpe, *Il sindacato sulla discrezionalità tecnica tra vecchio e nuovo rito (considerazioni a margine della sentenza Cass. SS.UU., 17 febbraio 2012, n. 2312),* in *Giustamm. it*, 28 febbraio 2012; L. Torchia, *Il giudice amministrativo e l'amministrazione: controllo, guida, interferenza*, in *Riv. trim. dir. pubbl.*, 2019, 1, 190; S. Vaccari, *Il Consiglio di Stato e la 'riduzione progressiva della discrezionalità'. Verso un giudicato a 'spettanza stabilizzata?*, *Dir. proc. amm.*, 2019, 4, 1172.

[13] Tra la sconfinata letteratura in materia, si cita S. Cassese, *Le autorità indipendenti: origini storiche e problemi odierni*, in S. Cassese, C. Franchini (a cura di), *I garanti delle regole*, Bologna, 1996, 221. Nello specifico, sul tema del sindacato giurisdizionale sugli atti di discrezionalità tecnica delle Autorità Amministrative Indipendenti si veda S. Torricelli, *Per un modello generale di sindacato sulle valutazioni tecniche: il curioso caso degli atti delle Autorità Indipendenti,* in *Dir. amm.*, 2020, 1, 97.

formation and Communication Technologies (ICT), che con sempre maggiore pervasività dominano il contesto in cui viviamo, si pongono al servizio dell'amministrazione e della società, offrendo delle opportunità in astratto capaci di intercettare quei principi di economicità, efficienza ed efficacia costituzionalmente tutelati e provando a soddisfare quella onnipresente domanda di semplificazione da più parti invocata[14]. Il progresso tecnologico degli apparati burocratici, infatti, viene visto come quell'imprescindibile punto di contatto tra pubblica amministrazione e sviluppo economico, introducendo un modello operativo capace di aumentare calcolabilità e prevedibilità delle decisioni e, in definitiva, la stabilità delle stesse.[15] Il tema dell' *e-governement,* ossia di una attività amministrativa dislocata su piattaforme web e agevolata dall'uso della rete Internet (in questo caso si parla di "servizi online"), è stato rappresentato come il rimedio essenziale per diminuire le esternalità negative derivanti da una rigida formalizzazione delle attività della pubblica amministrazione e dalle inefficienze che "la carta" porta con sé. A titolo di esempio, si pensi come l'obbligo di cui al d.P.R. 28 dicembre 2000, n. 445, ossia quello che impone alla P.A. di non richiedere ai cittadini dati e documenti già in possesso di altre pubbliche amministrazioni, possa essere più facilmente attuato con una infrastruttura Cloud capace di gestire e ottimizzare l'uso dell'enorme mole di dati in possesso dei vari apparati[16]. Ma anche qui, il progresso tecnico, oltre che incidere sui

---

[14] Sull'impatto dell'innovazione tecnologica sulle pubbliche amministrazioni si veda S. Civitarese Matteucci, L. Torchia, *La tecnificazione dell'amministrazione,* op. cit., 10. ; D.U. Galetta, *Digitalizzazione e diritto ad una buona amministrazione,* in *CERIDAP*, 2021, 3, 197; G.M. Racca, *Le innovazioni necessarie per la trasformazione digitale e sostenibile dei contratti pubblici,* in *Federalismi.it*, 2022, 15, 191; R. Cavallo Perin, *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Torino, 2021; R. Cavallo Perin, D. U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020.

[15] Sul tema si veda C. Acocella, *Innovazione tecnologica e innovazione amministrativa. L'automazione delle decisioni nel quadro della riforma della P.A.,* in F. Liguori (a cura di), *Il problema amministrativo, aspetti di una trasformazione tentata,* Napoli, 2021.

[16] Sull'applicazione delle tecnologie Cloud alla realtà delle pubbliche amministrazioni è indispensabile il rinvio alla Strategia Cloud Italia, ossia un documento programmatico pubblicato il 7 settembre 2021 e redatto dal Dipartimento per le Trasformazione Digitale (istituito presso il Ministero per l'innovazione tecnologica e la transizione digitale) e l'Agenzia Nazionale per la Cybersicurezza. Senso di tale intervento è quello di fornire l'indirizzo strategico per l'implementazione e il controllo di soluzioni Cloud nella Pubblica Amministrazione attraverso tre direttrici fondamentali: la creazione di una infrastruttura nazionale e indipendente da fornitori extra-UE per l'erogazione di servizi Cloud (il cd. Polo Strategico Nazionale); una attività di certificazione dei sog-

parametri organizzativi, tende sempre più a imporsi sul contenuto delle decisioni, in ossequio a quelle esigenze di stabilità e certezza del diritto che, almeno in teoria, ben si conciliano con le soluzioni offerte da applicazioni algoritmiche e di *machine learning* in luogo di un procedimento amministrativo "tradizionale".[17] Volendo cogliere i tratti salienti di queste nuove tecnologie, possiamo definire il *cloud computing* quale "*un nuovo paradigma di utilizzo e gestione di risorse computazionali e di servizi informatici erogati su richiesta tramite internet. I servizi Cloud sono offerti mediante cataloghi standardizzati idonei a garantire, in modo sistematico e semplificato (agilità), l'attivazione dei servizi che possono scalare, a seconda dei picchi di carico, con modalità trasparente e automatica (elasticità) potendo operare in contemporanea e in sicurezza su dati e sistemi di utenti diversi (multi-tenant")*[18]. Queste caratteristiche e le altre che tali nuove tecnologie sono capaci di offrire portano in una direzione che tenderebbe a trasformare il linguaggio giuridico in codice[19], ossia in un modo di esprimersi binario che consente di offrire un grado di certezza e di stabilità che, come è noto, raramente le pubbliche amministrazioni nel nostro Paese sono in grado di produrre. Proprio sul già richiamato tema della cd. "calcolabilità del diritto"[20] sembra incidere in maniera pervasiva il sempre più diffuso e auspicato ricorso agli *smart contracts*[21]*,* ossia di quelli che il secondo comma dell'art. 8-*ter* del d.l. n. 135/2018, convertito in legge n. 12/2019 definisce "*un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse*". Tali nuovi fenomeni giuridici sono destinati ad avere un impatto anche sul mondo delle ammi-

getti fornitori di Cloud pubblico al fine di garantire il rispetto dei requisiti di sicurezza, affidabilità e rispetto degli standard; lo sviluppo di una metodologia di classificazione di dati e servizi per individuare la soluzione Cloud più opportuna.

[17] Sull'ampia questione dell'amministrazione per algoritmi e sui problemi sollevati si vedano G. Avanzini, *Decisioni amministrative e algoritmi informatici,* Napoli, 2019; A. Di Martino, *L'amministrazione per algoritmi ed i pericoli del cambiamento in atto,* in F. Liguori (a cura di), *Il problema amministrativo, aspetti di una trasformazione tentata*, Napoli, 2021.

[18] C.f.r. Strategia Cloud Italia, 5.

[19] Sul fenomeno del "*code is law"* e della tesi che vede linguaggio giuridico e informatico posti su due binari paralleli si veda L. Lessig, *Code and Other Law of Cyberspace*, New York, 1999.

[20] Si veda N. Irti, *Un diritto incalcolabile,* Torino, 2016, per le considerazioni espresse in tema di applicabilità degli algoritmi al ragionamento giuridico.

[21] Sul tema degli *smart contracts* e delle tecnologie *blockchain* applicate al diritto si veda, tra i tanti, M. Giuliano, *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, in *Dir. inf. inform.*, 2018, 6, 989.

nistrazioni pubbliche, non essendo queste ultime immuni da una trasformazione dei tradizionali canoni di espressione dell'azione amministrativa attraverso algoritmi. Basti menzionare a tal proposito il dibattito giurisprudenziale e dottrinale[22] sorto in tema di uso degli algoritmi nei procedimenti amministrativi, in particolare dell'apertura che talune pronunce del Consiglio di Stato hanno offerto all'uso di algoritmi "non deterministici"[23] anche per procedimenti amministrativi aventi ad oggetto una attività discrezionale dell'amministrazione e non solamente, come ritenuto pacifico fino a quel momento, per i procedimenti a carattere vincolato. In tali pronunce si afferma infatti che non vi siano "*ragioni di principio, ovvero concrete, per limitare l'utilizzo all'attività amministrativa vincolata piuttosto che discrezionale, entrambe espressione di attività autoritativa svolta nel perseguimento del pubblico interesse'*[24]. La vicenda appena menzionata è solo una delle tante dalle quali emergono i segni del continuo intreccio tra diritto e tecnica, in particolare con le tecnologie dell'informazione. In definitiva, il processo di digitalizzazione e "tecnificazione" della P.A. promette di ridisegnarne schemi operativi e organizzativi, con una trasposizione della attività su piattaforme digitali e interconnesse. Una rivoluzione copernicana che, come tutti i cambiamenti, porta con sé questioni e problemi a cui è necessario dare una risposta, tenendo conto di quei medesimi principi normativi che ne hanno spinto il progresso.

2. Le nuove esigenze di tutela: la cybersicurezza

L'uso delle tecnologie dell'informazione, tanto nel rapporto tra amministrazioni e amministrati quanto nell'erogazione di servizi essenziali da parte di soggetti privati, è divenuta una costante. In molti dei servizi erogati, la fruizione online degli stessi non è rimessa a una libera scelta della singola amministrazione (o privato erogatore

---

[22] Si veda in particolare, G.M. Esposito, *Al confine tra algoritmo e discrezionalità. Il pilota automatico tra procedimento e processo,* in *Dir. proc. amm.*, 2019, 1, 39; M.C. Cavallaro, G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo,* in *Federalismi.it*, 2019, 16, 2; R. Cavallo Perin, D. U. Galletta, *Il diritto dell'amministrazione pubblica digitale*, op. cit.

[23] Ossia di "*programmi informatici che non offrono una correlazione binaria tra dati di input e dati di output ma che introducono una attività decisionale propria che viene anche definita "merito algoritmico*", cfr. A. Di Martino, *L'amministrazione per algoritmi,* op. cit., 232.

[24] Cons. Stato, Sez. IV, 13 dicembre 2019, n. 8472 (punto 10); in maniera conforme anche Cons. Stato, Sez. VI, 4 febbraio 2020, n. 881.

di servizi pubblici). Oggi la legge riconosce un diritto all'uso delle tecnologie, affermando che "*i cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni*" e con gli altri soggetti ad essa riconducibili, compresi i gestori di pubblici servizi, e affidandone anche la tutela al giudice amministrativo (art. 3 d.lgs. 7 marzo 2005, n. 82). Inoltre, "*la presentazione di istanze, la comunicazione di provvedimenti amministrativi o lo scambio di documenti tra le imprese e amministrazioni pubbliche avviene esclusivamente mediante le tecnologie dell'informazione e della comunicazione (art. 5 bis, d.lgs. n. 82/2005)*"[25]. In buona sostanza, si può affermare che, nonostante i rilievi critici e la lentezza del nostro sistema nell'adeguarsi alle tecnologie digitali[26], è ormai tracciato il solco di un percorso che vedrà (anche) l'amministrazione pubblica affidare il proprio funzionamento ad una infrastruttura digitale. Quest'ultimo punto, ossia la dipendenza di fatto dell'amministrazione ad una infrastruttura di rete, rappresenta un tema di sicuro interesse che merita di essere approfondito. Anche perché porta con sé tutta una serie di enormi questioni che valgono per qualsiasi processo di digitalizzazione. Se infatti allarghiamo la prospettiva, la quasi totale trasposizione della vita reale su contesti virtuali ha avuto un impatto sull'economia e sul sistema Paese, rafforzandosi sempre più l'equazione secondo la quale una infrastruttura informatica sicura è il presupposto imprescindibile per una prosperità economica altrettanto solida. Sembra corretto affermare che garantire la sicurezza nel funzionamento delle infrastrutture che reggono i sistemi informatici di uno Stato debba considerarsi attività strategica, rientrando questo obiettivo nella nozione di interesse pubblico al quale l'amministrazione deve tendere, soprattutto nel momento in cui "pretende" che determinati tipi di attività e servizi siano trasferiti in rete[27]. Questa esigenza non coinvolge solamente quelle attività svolte da pubbliche amministrazioni nell'esercizio della funzione, ma si estende a tutti i settori strategici e critici che rappresentano l'ossatura vitale del sistema paese, si pensi a quelli già presi in considerazione dall'or-

---

[25] G. Piperata, *Cittadini e imprese di fronte all'amministrazione digitale*, in *Diritti mercato tecnologia*, 2016, 2, 168.

[26] Per l'esame di questi si rimanda, in definitiva, a E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale,* op. cit.

[27] A titolo puramente esemplificativo di tale "pretesa", si veda come la possibilità di partecipazione a concorsi pubblici sia subordinata al possesso di un indirizzo PEC o di credenziali Spid.

dinamento sotto il profilo degli investimenti esteri diretti quali la difesa, la sicurezza, i trasporti e l'energia[28]. I soggetti privati che operano in questi settori, infatti, sono sottoposti ad una maggiore attenzione sotto i profili della sicurezza informatica, tanto è che la prima normativa che ha affrontato in maniera organica la questione, la Direttiva del 6 luglio 2016, n. 1148 sulla sicurezza dei sistemi delle reti e dell'informazione ("*Network and Information Security*", cd. "Direttiva NIS", al cui esame sarà dedicato in seguito ampio spazio) parla di "*operatori di servizi essenziali e delle infrastrutture critiche*", senza distinguere tra la natura pubblicistica o privatistica del soggetto. Sempre sulla scorta di tale orientamento, come si vedrà ampiamente in seguito, i soggetti destinatari della normativa sono anche i cd. "*fornitori di servizi digitali*", la cui centralità è indissolubilmente legata alla sempre maggiore rilevanza che la loro funzione assume nel mondo economico attuale e nelle relazioni sociali. Sulla base di queste osservazioni, si può certamente dire che l'infrastruttura digitale è diventata strategica poiché il principale fenomeno che da essa trae origine, la digitalizzazione, "*incide trasversalmente sull'organizzazione sociale, a partire dalla più semplice attività condotta dai comuni cittadini (si pensi ai pagamenti elettronici, agli acquisti online, ecc.), passando a quelle compiute dai gestori di servizi – su tutti quelli essenziali (in settori critici quali l'energia, i trasporti, il sistema idrico, l'assistenza sanitaria e la finanza), ma altrettanto può dirsi anche per i fornitori di servizi digitali (mercati online, motori di ricerca e servizi di cloud, cd. "cloud computing", o la "comunicazione da macchina a macchina"– per finire con le operazioni condotte in ambito militare'*[29].

Le complesse problematiche che la sempre maggiore interconnessione tra *devices* e l'alluvione di dati che tra di essi circolano[30], fenome-

[28] Sulla tutela dei settori strategici mediante i poteri speciali attribuiti al Governo in materia di investimenti esteri (su cui si tornerà specificamente in seguito) e la nozione stessa di "strategicità" si veda G. Della Cananea, L. Fiorentino, *I "poteri speciali" del Governo nei settori strategici*, Napoli, 2020; R. Spagnuolo Vigorita, *Golden power: per un nuovo paradigma di intervento dello Stato nell'economia,* in *CERIDAM*, 2021, 4, 112; sui recentissimi interventi in materia si veda R. Chieppa, *La nuova disciplina del golden power dopo le modifiche del d.l. n. 21/2022 e della legge di conversione n. 51/2022,* in *Federalismi.it*, 2022, 51, 2.

[29] L.V.M. Salamone, *La disciplina del cyberspace alla luce della direttiva europea sulla sicurezza delle reti e dell'informazione: contesto normativo nazionale di riferimento, ruolo dell'intelligence e prospettive de iure condendo,* in *Federalismi.it*, 2017, 23, 4.

[30] Interconnessione che è esponenzialmente cresciuta nel momento in cui oltre alle persone hanno iniziato ad interagire tra loro le cose, dando vita al complesso e pionieristico (ma non più tanto) concetto di *Internet of Things (IOT),* sviluppato per la prima volta da K. Ashton, *That 'Internet of Things' Thing, RFID Journal*, 2009, 3. Quando que-

ni ben presenti anche nel mondo delle pubbliche amministrazioni[31], rendono essenziale un inquadramento da un punto di vista tecnico, seppur breve, del concetto di cybersicurezza, essendo questo un inevitabile punto di incontro tra tutti i processi di digitalizzazione, siano essi legati al mondo della pubblica amministrazione o meno, e che finisce col rappresentare una delle sfide più importanti per il legislatore contemporaneo. Tra le esigenze che l'operatore/cittadino ha nel momento in cui svolge una attività online che coinvolge propri diritti soggettivi o interessi legittimi, rientra l'auspicio che le infrastrutture che innervano e danno vita a questi processi siano sicure, integre e capaci di affrontare forme di interferenze esterne e problemi operativi interni (la cd. "resilienza"[32]). Le garanzie che comunemente sono richieste per una corretta utilizzabilità dei sistemi informatici sono più emblematicamente riassunte nella triade "RID", "*riservatezza, integrità, disponibilità"*, con ciò riassumendo un ventaglio di istanze: la tutela della privacy e la protezione dei propri dati messi in circolo sulla rete (incidendo il tal senso la normativa GDPR[33] e la relativa evoluzione giurisprudenziale[34]); la possibilità di utilizzare sistemi capaci di non scomporsi a seguito di eventi patologici (attacchi informatici, *data breaches*, *bug* di sistema etc.); essere in grado di mantenere un diritto di godere e disporre liberamente dei contenuti e delle infrastrutture che si utilizzano. Per inquadrare più da vicino i caratteri di quella che definiamo "sicurezza informatica",

---

ste tecnologie vengono applicate alle realtà produttive si è soliti parlare di "Industria 4.0", con ciò comprendendo la *Additive Manufacturing*, l'uso sempre più pervasivo dei *Big Data*, la *Digital Factory*, le varie applicazioni di Intelligenza Artificiale e la Robotica collaborativa. Si parla anche di "Quarta Rivoluzione Industriale", principalmente sulla base del fatto che viene diffuso un modello di produzione che fa uso di un impiego sempre più pervasivo di dati e informazioni, di tecnologie computazionali e di analisi dei dati, di nuovi materiali, componenti e sistemi totalmente digitalizzati e connessi.

[31] Sul rilievo dei *Big Data* nell'ambito delle attività della pubblica amministrazione si veda M. Falcone, *Big data e amministrazioni pubbliche: prospettive della funzione conoscitiva pubblica*, in *Riv. trim. dir. pubbl*, 2017, 3, 601.

[32] Termine divenuto di moda in più campi e settori, in informatica indica la capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati.

[33] Il riferimento è al Regolamento europeo del 27 aprile 2016, n. 679, definito *General Data Protection Regulation.*

[34] Per approfondimenti in tal senso si veda, tra gli altri, O. Pollicino, M. Bassini, *Libertà di espressione e diritti della personalità nell'era digitale. La tutela della privacy nella dimensione europea,* in G. Enea Vigevani, O. Pollicino, C. Melzi (a cura di), *Diritto dell'informazione e dei media,* Torino, 2018, 91-123.

facciamo riferimento a tre diversi momenti di attenzione che danno poi luogo a diverse fasi di intervento. In primo luogo, le misure di prevenzione, ossia quegli accorgimenti tecnici e operativi volti a sterilizzare il rischio che l'incidente si verifichi (sia esso un attacco esterno o un guasto interno). In secondo luogo, l'attività di monitoraggio, fondamentale per verificare l'esatto *timing* dell'incidente e le conseguenze di breve, medio e lungo periodo. In ultimo, le misure di ripristino in risposta all'evento, puntando sulla minimizzazione del danno. Queste tre fasi sono "*trasversalmente caratterizzate dall'uso di strumenti diversi quali il controllo degli accessi, distaster recovery, crittografia, hardware e software per la difesa perimetrale, sistemi di rilevamento intrusioni e misure di sicurezza fisica, ecc.*"[35] In definitiva, a causa della ineliminabile necessità di utilizzare reti di comunicazione digitali e da strumenti di tecnologia informatica, si può certamente sostenere che "*un attacco può causare non solo danni tecnologici ma, anche, ledere diritti e libertà delle persone, alterare gli equilibri politici di una nazione e, se sono colpite infrastrutture critiche, determinare gravi conseguenze per comunità, istituzioni e imprese.*"[36]
Date queste premesse, la questione si sposta sulle modalità concrete mediante le quali riuscire a perseguire questi specifici interessi, prendendo immediatamente atto che la materia di cui si parla è connotata da un grado di tecnicismo particolarmente elevato, oltre che in costante evoluzione. Diviene utile, a questo punto, svolgere una ricostruzione relativa ai diversi provvedimenti normativi adottati tanto a livello sovranazionale quanto a livello nazionale, provando a individuare un filo conduttore capace di mostrare quali siano le ripercussioni in termini generali nel modello di relazioni tra Stato ed economia. In particolare, una delle conseguenze più immediate sotto il profilo dell'organizzazione amministrativa nel nostro ordinamento è stata, in un'ottica di una maggiore specializzazione delle competenze e di ricorso alla tecnica (come si è visto sopra), l'istituzione dell' Agenzia Nazionale per la cybersicurezza (come si vedrà più approfonditamente in seguito, § 3) ad opera del d.l. 14 giugno 2021, n. 82, convertito con legge 4 agosto 2021, n. 109, le

[35] R. Brighi, P. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea,* in *Federalismi.it*, 2021, 21, 19.

[36] R. Brighi, P. Chiara, *La cybersecurity come bene pubblico,* op. cit., 20. Sul concetto di *cyberwar* e sui suoi impatti sul mondo attuale si vedano: F. Rugge, *Mind hacking: la guerra informativa nell'era cyber*; A. Bonfanti, *Attacchi cibernetici e cyber war: considerazioni di diritto internazionale,* entrambi in G. Ziccardi (a cura di), *La guerra dell'informazione e i nuovi equilibri internazionali: aspetti giuridici, tecnologici e geopolitici*, in *Notizie di Politeia*, 2018, 24, 118-127.

cui funzioni e compiti offrono un interessante spunto per tracciare una direzione verso la quale si muovono le risposte che il diritto amministrativo offre al tema della sicurezza cibernetica. Osservando tale *excursus* normativo, si avrà modo di riflettere sul valore che il tema della *cybersecurity* ha assunto nella dimensione più recente, con una esigenza sempre maggiore di tutela di tale *asset* in quanto bene pubblico e della grande rivoluzione nell'approccio al tema della *cybersecurity* che l'ultimo *step* di tale percorso, ossia la Strategia Nazionale di Cybersicurezza pubblicata il 17 maggio 2022, ha prodotto, (come si vedrà meglio in seguito). Tale ultimo intervento, infatti, sembra qualificare la cybersicurezza quale obiettivo comune al cui perseguimento devono tendere non solo lo Stato e i suoi apparati, bensì anche i soggetti privati, tanto nel perseguimento di una attività di impresa che nell'adempimento dei propri compiti quotidiani, con la creazione di una rete di responsabilità condivise che rappresenta il vero cambio di passo rispetto al passato, qualificando la cybersicurezza quale bene pubblico[37].

3. Il percorso normativo: dalla direttiva "NIS" al d.l. 82/2021

Prima di ripercorrere il percorso normativo europeo e nazionale in materia di cybersicurezza, è opportuna una precisazione sull'effettivo perimetro su cui insistono questi interventi. In particolare, i principi generali dei sistemi di sicurezza delle infrastrutture digitali abbracciano un novero di destinatari che va oltre il mondo delle pubbliche amministrazioni, includendo anche i cd. "operatori dei servizi essenziali" che, come si vedrà meglio in seguito, pur essendo soggetti di natura privatistica (sia formalmente che sostanzialmente) rivestono un ruolo strategico o svolgono una funzione critica che ne rende necessaria l'equiparazione a chi fa strutturalmente parte dell'apparato statale. La cybersicurezza, dunque, rappresenta un'esigenza di tutela che interessa lo Stato in quanto agente attivo,

[37] Come si avrà modo di approfondire in seguito (in particolare §5), tale ricostruzione dottrinale deve la sua principale elaborazione al dibattito sorto negli Stati Uniti in materia, si veda M. Taddeo, *Is Cybersecurity a Public Good?,* in *Minds & Machines*, 2019, 29, 349; P. Rosenzweig, *Cybersecurity and Public Goods: The Public/Private "Partnership",* in *Cyberwarfare: How Conflicts in Cyberspace are Challenging America and Changing the World*, in *Praeger Security International*, 2012, 1, 2; per una riproposizione critica nel contesto italiano si veda R. Brighi, P. Chiara, *La cybersecurity come bene pubblico*, op. cit.

coinvolgendo il "*suo complesso istituzionale (Stato-apparato), sia nelle sue specifiche componenti di Stato-collettività, quali la popolazione (società) e le imprese (economia), sintetizzando così in un unico concetto l'insieme delle prospettive giuridicamente rilevanti del diritto alla sicurezza come individuate dalla dottrina gius-pubblicistica*"[38], ponendo l'accento sulla partecipazione attiva delle infrastrutture critiche, composte sia da soggetti pubblici, sia privati, nelle attività di cybersicurezza nazionale. Un braccio di azione che, in definitiva, possiamo definire universale e trasversale. Detto ciò, per comprendere le fondamenta dell'architettura della normativa in materia di cybersicurezza è necessario partire da una disamina di quello che è l'atto che ha dato lo stimolo necessario al nostro paese affinché iniziasse un serio percorso di potenziamento organizzativo e regolamentare, ossia la Direttiva del 6 luglio 2016, n. 1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, cd. "Direttiva NIS*" (Network and Information Security).* Partendo da tale atto di impulso, il sistema italiano di cybersicurezza inizierà un lento cammino di ammodernamento che dovrà attendere il viscerale cambiamento indotto dalla pandemia di Covid-19 iniziata nel 2020 e dagli stimoli degli aiuti europei (in particolare dal Piano *Next Generation EU*, come si vedrà specificamente in seguito) per garantire una maggiore strutturazione con l'istituzione dell'Agenzia Nazionale della Cybersicurezza e con la conseguente razionalizzazione di competenze e funzioni realizzate con il d.l. 82/2021.

3.1 La Direttiva "NIS" e l'impatto del suo recepimento sul sistema italiano di sicurezza cibernetica

La Direttiva 2016/1148 rappresenta un deciso punto di svolta per l'Unione Europea e per i suoi Stati Membri poiché, oltre ad essere il primo intervento organico in materia di tutela dello spazio cibernetico a livello europeo, offre per la prima volta una esigenza di adeguamento e avvicinamento delle normative nazionali di settore sulla base di un assunto molto preciso: se è vero che è possibile disegnare un'equazione tra alto livello di sicurezza delle infrastrutture digitali e prosperità economica, come già dimostrato in precedenza, al fine di garantire un corretto funzionamento del mercato unico europeo

[38] F. Serini, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021,* in *Federalismi.it*, 2022, 1, 269.

quale pilastro fondante dell'UE[39], è necessario che gli standard di sicurezza informatica siano comuni a tutti gli Stati membri. Abbiamo, dunque, un fine economico da raggiungere mediante dei mezzi appartenenti al mondo della tecnica. L'interconnessione dei sistemi economici degli Stati Membri ha poi subito un'ulteriore accelerazione con la sempre maggiore dipendenza di questi dalle tecnologie *ICT,* creando una commistione tra mercato e mondo digitale che acuisce e rende ancora più evidente quel fenomeno di transnazionalità che spinge il legislatore europeo ad avviare un percorso comune nell'ambito della *cybersecurity*. Prendendo atto della insufficienza dello stato dell'arte del contesto (o meglio, dei contesti) normativo europeo in materia di cybersicurezza, la Direttiva "NIS" indica un punto di partenza da cui dar vita ad un sistema complesso, con il fine immediato del ravvicinamento delle legislazioni dei singoli Stati europei, ma con il più ampio ed ambizioso obiettivo di implementare una strategia comune nel campo della *cybersecurity*, gettando le basi per mettere a punto un'organizzazione difensiva completamente integrata e sotto egida europea. Nelle intenzioni del legislatore europeo, "*mettendo ordine al suo interno, l'Unione avrebbe potuto imporsi a livello internazionale e diventare un partner ancora più credibile per la collaborazione a livello bilaterale e multilaterale, acquisendo così la capacità di promuovere con più forza i diritti e i valori fondamentali dell'UE al suo esterno*"[40]. Sul piano puramente giuridico, tale esigenza di avvicinamento della normativa è pienamente soddisfatta dallo strumento della Direttiva, in forza del principio di sussidiarietà di cui all'art. 5 TUE e, soprattutto, avendo legato gli interventi in materia di cybersicurezza al corretto funzionamento del mercato unico, la Direttiva "NIS" trova la sua base giuridica nell'art. 26 del TFUE , in forza del quale "*l'UE ha il potere di adottare misure destinate all'instaurazione o al funzionamento del mercato interno, conformemente alle disposizioni pertinenti dei trattati*" e, soprattutto, a nell'articolo 114 TFUE, in virtù del quale l'Unione può adottare "*le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione o il*

---

[39] Rilevante è il riferimento all'art. 3.3 del Trattato sull'Unione Europea, che definisce il mercato unico quale uno degli obiettivi principali dell'Unione, "*comportando la creazione di uno spazio senza frontiere nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali*", si veda G. Tesauro, *Manuale di diritto dell'Unione Europea*, Napoli, 2018, 22.

[40] L.V.M. Salamone, *La disciplina del cyberspace alla luce della direttiva europea sulla sicurezza delle reti e dell'informazione*, op. cit., 9.

funzionamento del mercato interno". Questa attenzione dimostrata verso il tema della cybersicurezza, abbinata alla consapevolezza mostrata della centralità della stessa nella vita di tutti i giorni, può rappresentare una grande occasione per la costruzione di un unitario disegno di difesa europea, rendendo "*più facilmente ed opportunamente realizzabile una organizzazione di difesa e contrasto unitaria, nei confronti della minaccia cibernetica, la quale, tra l'altro, costituisce oggi e in prospettiva, minaccia ben più pericolosa per la società europea e per il sistema Europa, nel suo complesso*" [41] . Una organizzazione difensiva unitaria europea, quale è quella che in definitiva emerge dalla Direttiva "NIS", costituisce un fatto di grande rilevanza politica, dal momento che, per la prima volta, l'Unione metterebbe a punto una organizzazione difensiva completamente integrata sotto la sua egida[42].

Venendo ad una disamina più accurata di quanto previsto dalla norma, la logica con la quale ci si muove è quella del *risk based approach,* ossia di una modalità di regolamentazione che prevede innanzitutto strumenti di prevenzione a carattere organizzativo volti a mitigare il rischio di attacco/danneggiamento delle infrastrutture, pur non ignorando l'esigenza di intervento diretto dopo che il rischio potenziale diviene attuale (come si vedrà nello specifico, tale ruolo è rivestito dai CSRIT, ossia dei gruppi di pronto intervento ad attacco informatico in corso). Dunque, sulla base di questa logica di fondo, la Direttiva "NIS" si articola su tre *milestones*: istituire un obbligo per gli Stati ad adottare la strategia nazionale in materia di sicurezza della rete e dei sistemi informativi; aumentare il livello di cooperazione degli Stati Membri con delle organizzazioni specifiche; obbligare operatori nei servizi essenziali (siano essi pubblici o privati) e fornitori di servizi digitali a adottare specifici protocolli e a notificare gli incidenti. Venendo al primo punto, la strategia nazionale in materia di sicurezza della rete e dei sistemi informativi è uno dei punti car-

---

[41] L. Ramponi, *Minaccia cyber è vero pericolo per Italia ed Europa*, in *www.cyberaffairs.it*, 25 marzo 2017.

[42] Il dibattito sulla difesa comune europea è stato rianimato prepotentemente a seguito dell'invasione russa del territorio nazionale dell'Ucraina cominciata il 24 febbraio del 2022 e le conseguenti tensioni politiche, diplomatiche ed economiche tra la Federazione Russa e l'intero mondo occidentale. Per un approfondimento in merito si vedano i rilievi di M. Frau, *I nodi irrisolti della difesa comune europea. Una prospettiva federalista, Federalismi.it*, 2022, 1, 29, il quale offre un quadro conclusivo che riassume le profonde difficoltà nella costruzione di un sistema di sicurezza e difesa comune nella "*eccessiva frammentazione nonché dalla carenza di efficaci meccanismi di controllo democratico-parlamentare a livello sovranazionale*".

dine dell'intero sistema, dal momento che rappresenta il momento programmatico essenziale per la costruzione di un solido sistema di regole. Ai sensi dell'art. 7 della Direttiva, la strategia contiene: gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi; un quadro di governance per conseguire gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; l'individuazione delle misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato; un'indicazione di programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi; un'indicazione di piani di ricerca e sviluppo relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi; un piano di valutazione dei rischi per individuare i rischi; un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi.
Appare molto interessante il ruolo che la norma attribuisce all'ENISA[43], la quale assume una veste di supporto per gli Stati Membri garantendo loro assistenza nella fase di redazione della strategia. Una volta adottata, la strategia viene comunicata entro tre mesi alla Commissione, con ciò dando attuazione concreta a quelle esigenze di coordinamento e reciproca assistenza che la Direttiva intende porre a fondamento del proprio intervento. Come si vedrà in seguito, il nostro Paese ha ottemperato a questo obbligo con l'adozione della Strategia nazionale di cybersicurezza adottata nel maggio del 2022. Tale documento rappresenta uno snodo fondamentale nello sviluppo di una architettura di cybersicurezza nazionale, focalizzando la sua implementazione anche alla diffusione di una cultura comune della cybersicurezza, con uno Stato in veste di coordinatore di un complessivo sforzo capace di coinvolgere istituzioni, imprese e singoli cittadini, (come si vedrà meglio in seguito, §5).
Passando al secondo punto chiave, l'incremento della cooperazione tra Stati in materia di scambio di informazioni e di attività condivise nel settore della cybersicurezza passa per una predisposizione di norme minime volte a dare vita (o ad armonizzare ove già presente) un apparato istituzionale in ciascuno Stato Membro, con

[43] La *European Network and Information Security Agency*, ossia l'Agenzia europea per la cibersicurezza, istituita con il Regolamento europeo n. 406 del 4 marzo2004, avente attualmente sede ad Atene.

funzioni, attribuzioni e caratteristiche tali da rendere compatibile tale collaborazione. Appare logico che prima ancora che il dialogo possa instaurarsi, va adeguatamente garantita la funzionalità di una serie di soggetti istituzionali capaci di parlare un linguaggio comune in termini di giuridici prima ancora che tecnici. Infatti, prodromici alla parte della normativa in materia di istituti di cooperazione sono gli artt. 8 e 9 della Direttiva "NIS". Il primo di questi prevede che "*ogni Stato membro designa una o più autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi"* e che al tempo stesso "*ogni Stato membro designa un punto di contatto unico nazionale in materia di sicurezza delle reti e dei sistemi informativo"*. Merita attenzione il rapporto che la Direttiva costruisce tra queste due entità: la cd. "autorità competente" svolge funzioni operative dirette, che consentono l'applicazione delle regole europee e nazionali di settore; mentre il cd. "punto di contatto unico" è il canale di comunicazione mediante il quale le varie autorità nazionali dialogano e instaurano un collegamento informativo. L'art. 9 della Direttiva, invece, prevede l'instaurazione di un CSIRT, ossia di un *Computer Security Information Response Team,* una struttura che ha la responsabilità di monitorare, intercettare, analizzare e rispondere alle minacce *cyber*, di cui si avrà modo di parlare più diffusamente in seguito. Queste tre strutture, l' "Autorità competente", il "punto di contatto unico nazionale" e il "CSIRT Nazionale" sono a loro volta inseriti in un primo essenziale livello di cooperazione, come riporta l'art. 10, che si premura di precisare che *"se sono separati, l'autorità competente, il punto di contatto unico e i CSIRT dello stesso Stato membro collaborano per quanto concerne l'adempimento degli obblighi di cui alla presente direttiva"*. Fatta questa disamina preliminare, si può passare alle forme di collaborazione transnazionale vera e propria, che sono disciplinate dall'intero Capo III della Direttiva, sotto il titolo di "Cooperazione", e dagli artt. 11 ss. Le due principali sedi nelle quali si prevede che questa collaborazione trovi espressione sono il "Gruppo di collaborazione" di cui all'art. 11 e la "Rete di CSIRT" di cui all'art. 12. Il primo è composto da rappresentanti degli Stati Membri, della Commissione europea e dell'ENISA e si vede attribuite una serie di specifici compiti di scambio di informazioni, buone pratiche ed esperienze delle varie sfaccettature della sicurezza dei sistemi informatici (si va dalle politiche di sensibilizzazione alla elaborazione della strategia nazionale di cui all'art. 7), andando ad individuare delle aree tematiche che si riferiscono sostanzialmente a compiti di pianificazione, guida, segnalazione e

condivisione delle informazioni. L'altro canale di dialogo introdotto dalla Direttiva "NIS" è la "Rete di CSIRT", che altro non è che una interconnessione transnazionale dei singoli CSIRT nazionali con compiti di: scambio di informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione; sostegno agli Stati membri nel far fronte a incidenti transfrontalieri, sulla base dell'assistenza reciproca volontaria; discussione, esame e individuazione di ulteriori forme di cooperazione operativa; formulare orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni in materia di cooperazione operativa. In definitiva, questo secondo punto chiave introdotto dalla Direttiva in relazione agli strumenti di cooperazione sembra rappresentare l'ambizione principale dell'intero impianto, spingendo verso un processo di integrazione che pone non pochi problemi, come spesso accade nel settore della sicurezza pubblica[44].

Terzo e ultimo punto cardine della Direttiva "NIS" è la predisposizione di un set di obblighi per gli operatori dei servizi essenziali e i fornitori di servizi digitali, i cui principali riferimenti normativi sono l'art. 5, che si concentra sulle caratteristiche dei soggetti che rientrano in tale categoria, e l'intero capo IV, che individua gli specifici obblighi e norme da rispettare. Prima di addentrarsi nella disciplina specifica, è essenziale individuare quale sia la definizione rilevante ai sensi della Direttiva "NIS" dei soggetti destinatari della normativa. Ai sensi dell'art. 4, punto 4, si definisce "*operatore di servizi essenziali*" un soggetto pubblico o privato che soddisfa i seguenti criteri: fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; l'erogazione di tale servizio dipende dalla rete e dai sistemi informativi; un incidente avrebbe effetti negativi rilevanti sulla fornitura dello stesso. Si tratta di uno sforzo definitorio non indifferente, che fornisce molte indicazioni soprattutto se si pensa al rango normativo dell'intervento, ossia una Direttiva[45]. Relativamente all'altra categoria di soggetto, ai sensi

[44] Basti pensare agli enormi spazi di autonomia che ancora oggi gli Stati membri godono in materia di Politica estera e di sicurezza comune (PESC) e di Politica di sicurezza e di difesa comune (PSDC), si veda G. Tesauro, *Manuale di diritto dell'Unione Europea,* op.cit*.,* 59.

[45] Si ricordino i connotati giuridici della Direttiva, la quale ai sensi dell'art. 288, comma 3 TFUE "*vincola lo Stato Membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi";* si è quindi di fronte a un atto normativo che consente allo Stato membro di esercitare una discrezionalità circa le modalità e i mezzi di raggiungimento dell'obiettivo prefissato dalla Direttiva.

dell'art. 4, punti 5 e 6, si definisce "*fornitore di servizio digitale*" qualsiasi persona giuridica che fornisce un servizio digitale, individuando quest'ultima definizione ai sensi dell'articolo 1, par. 1, lettera b), della Direttiva del 9 settembre 2015, n. 1535 del Parlamento europeo e del Consiglio di un tipo elencato nell'allegato III della Direttiva in esame (riferendosi nella sostanza alle definizioni di "*mercato online, motore di ricerca online e servizi di cloud computing*"). Venendo al contenuto di quanto stabilito dalle prescrizioni introdotte dalla Direttiva "NIS", gli obblighi per la prima categoria di soggetti, ossia gli operatori dei servizi essenziali, sono riconducibili a due ambiti specifici: obblighi di sicurezza e di notifica. In particolare, ai sensi dell'art. 14 della Direttiva gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni; allo stesso modo introducono misure atte a prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi. Queste prime due prescrizioni fanno riferimento ad una funzione passiva rivestita da tali soggetti, i quali chiaramente dovranno adempiere a tali obblighi sotto la stretta vigilanza delle Autorità preposte. Passando agli obblighi di notifica, questi sono previsti al fine di prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi. Le notifiche includono le informazioni che consentono all'autorità competente o al CSIRT di determinare qualsiasi impatto transfrontaliero dell'incidente. Queste ultime sono descritte dall'art. 14, co. 4, nella parte in cui prevede che per determinare la rilevanza dell'impatto di un incidente si debba tenere conto, in particolare, dei seguenti parametri: il numero di utenti interessati dalla perturbazione del servizio essenziale; la durata dell'incidente; la diffusione geografica relativamente all'area interessata dall'incidente. È giocoforza ritenere che l'operatore debba dare conto di questi parametri nel contenuto della notifica al fine di consentire alle autorità di discernere correttamente l'entità della minaccia. In virtù delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, l'autorità competente o il CSIRT dovrà informare l'altro o gli altri Stati membri interessati se l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali in quello

Stato membro, in una già preannunciata ottica di collaborazione e di coordinamento europeo. Una delle norme più delicate dell'intervento è sicuramente l'art. 15, dal momento che indica agli Stati delle precise linee di intervento e, soprattutto, di sforzo economico per garantire il funzionamento e la corretta attività di controllo delle Autorità, stabilendo che gli Stati membri provvedono affinché le autorità competenti siano dotate dei poteri e dei mezzi necessari per valutare la conformità degli operatori di servizi essenziali agli obblighi loro imposti dall'articolo 14 e i relativi effetti sulla sicurezza della rete e dei sistemi informativi. Passando al capo V, si elencano gli obblighi previsti per la seconda categoria di soggetti di cui all'art. 4, ossia quella dei fornitori di servizi digitali. Sulla falsa riga di quanto previsto in precedenza, anche qui ci troviamo di fronte ad una forte responsabilizzazione per gli Stati Membri. In particolare, è previsto che questi adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi relative al settore nel quale operano. Inoltre, queste precauzioni utilizzate devono tenere conto della sicurezza dei sistemi e degli impianti, del trattamento degli incidenti, della gestione della continuità operativa, del monitoraggio, audit e test e della conformità con le norme internazionali. Ugualmente a quanto previsto all'art. 14, anche per i fornitori di servizi digitali vi è un secondo pacchetto di obblighi che attengono all'esigenza di notificazione degli incidenti all'Autorità competente e al CSIRT indicando i medesimi parametri di cui all'art. 14, oltre ad altri tre dati che sono calati nello specifico contesto dei servizi digitali: la portata della perturbazione del funzionamento del servizio e la portata dell'impatto sulle attività economiche e sociali. Questa aggiunta denota uno dei fili conduttori della normativa in esame, già individuato precedentemente, ossia della presa d'atto della profonda interrelazione tra la digitalizzazione della società e la sicurezza delle infrastrutture su cui questa si realizza.

Dopo aver esaminato le tre principali ramificazioni di questo primo e fondamentale intervento normativo in materia di cybersicurezza, di estremo interesse è l'analisi delle modalità concrete con cui le indicazioni presenti nella Direttiva "NIS" sono poi state recepite nel nostro paese, con una breve disamina del d. lgs. N. 65 del 18 maggio 2018, anche conosciuto come "Decreto NIS". Va sin da subito riconosciuto come tale intervento non abbia avuto quel peso e quel senso di svolta che invece la Direttiva europea voleva attribuirgli. Infatti, il Decreto "NIS" si dedica principalmente alla defi-

nizione di regole di coordinamento interno tra le amministrazioni, di procedure per la redazione futura di documenti quali la Strategia nazionale di sicurezza cibernetica e alla istituzione di punti di contatto e di cooperazione. Va comunque detto che questo intervento normativo si innesta in un quadro nazionale altrettanto timido nella definizione di una organica e maggiormente strutturata architettura di sicurezza cibernetica, che fino a quel momento si era retta su una struttura posta su tre livelli definita Sistema Nazionale di Sicurezza Cibernetica (SNSC), che trova il suo fondamento normativo nel d.P.C.M. n. 66 del 19 marzo 2013[46], successivamente modificato con il d.P.C.M. n. 87 del 17 febbraio 2017. La prima stratificazione di questo livello, disciplinata dagli artt. 3 e 4 del citato d.P.C.M., era di natura politica, ponendo il Presidente del Consiglio dei ministri al vertice di tale organizzazione, coadiuvato dal Comitato Interministeriale per la sicurezza della Repubblica (CISR), istituito con legge 3 agosto 2007, n. 124 presso la Presidenza del Consiglio dei Ministri e avente funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza. Il secondo livello, con una maggiore vocazione esecutiva ai sensi degli artt. 8 e 9 dello stesso d.P.C.M., vedeva la partecipazione del Nucleo per la Sicurezza Cibernetica (NSC), istituito nell'ambito dell'Ufficio del Consigliere Militare presso la Presidenza del Consiglio dei Ministri, con la funzione di supportare il Presidente nella materia della sicurezza del "cyberspazio" per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. Infine, il terzo livello, composto dagli Organismi di informazione per la sicurezza di cui all'art. 7 del medesimo d.P.C.M., responsabili di condurre attività di ricerca informativa, nonché analisi, valutazioni e previsioni sulle minacce, ed alla trasmissione di informazioni rilevanti al Nucleo per la Sicurezza Cibernetica, e agli altri soggetti, sia pubblici che privati, interessati all'acquisizione di informazioni[47]. A questa impalcatura,

[46] Tale originario assetto aveva avuto un suo momento di attuazione e di indirizzo nel Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico emanato nel dicembre 2013 dalla Presidenza del Consiglio dei Ministri. Tale documento si prefiggeva di individuare "*i profili e le tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti d'interesse nazionale"* specificando "*ruoli e compiti dei diversi soggetti pubblici e privati", "gli strumenti e le procedure con cui perseguire l'accrescimento delle capacità del Paese di prevenire e rispondere in maniera compartecipata alle sfide poste dallo spazio cibernetico"* (Quadro Strategico Nazionale, 7).

[47] F. Serini, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge*

il Decreto "NIS" si preoccupa solo di modificare alcune "etichette", conformemente a quanto richiesto dalla Direttiva omonima, al fine di adempiere quantomeno formalmente a quella esigenza di livellamento istituzionale per consentire il funzionamento di un dialogo e di una cooperazione effettiva. Ciò che rileva sin da subito è che questa organizzazione vigente al momento della Direttiva "NIS" e del relativo recepimento aveva ancora un forte ancoraggio agli apparati governativi e ministeriali, mancando quella autonomia e specializzazione a cui invece si giungerà solo con l'istituzione dell'Agenzia Nazionale nel 2021. Prima di arrivare alla svolta del 2021, però, è necessario guardare con attenzione ad un altro importante passaggio, ossia quello relativo ad un nuovo intervento di matrice comunitaria, il Regolamento 881/2019, essenziale ai fini di una costruzione di un sistema di certificazione unico e di individuazione delle infrastrutture critiche nell'ambito delle tecnologie digitali, e quello operato con il d.l. 105/2019 concernente dell'istituzione del cd. "perimetro nazionale di sicurezza cibernetica" . Infine, sulla scia di quest'ultimo importante passaggio, assume rilievo anche la nuova veste attribuita al cd. "*golden power*", ossia il potere speciale di controllo attribuito all'Esecutivo sugli investimenti esteri in settori strategici, che da questa prospettiva finisce con l'essere parte di una complessiva strategia nazionale in materia di sicurezza cibernetica, con il fine specifico di garantire una particolare attenzione ai cd. settori strategici, tra i quali rientrano, senza ombra di dubbio, le infrastrutture digitali del Paese.

3.2 Il d.l. 105/2019 e il ruolo del golden power

Il Regolamento UE del 17 aprile 2019 n. 881 e il d.l. 21 settembre 2019 n. 105 non sono tra di loro retti da un rapporto gerarchico come, ad esempio, quello esistente tra Direttiva "NIS" e relativo decreto attuativo. Eppure, è dato rinvenire tra questi due interventi un collegamento nelle intenzioni e nelle prerogative che ci consentono di apprezzarne la comunione d'intenti e, quindi, una intrinseca complementarità. Per quanto concerne il Regolamento 881/19, sono due le principali linee direttrici: da un lato si introducono disposizioni volte a determinare un rafforzamento del ruolo dell'ENISA, dall'altro si inizia il cammino verso un Quadro comune europeo di certificazione in materia di cybersicurezza, ponendo tale delicato intervento alla

n. 82 del 2021, op. cit., 244-245.

base di una esigenza di sicurezza nella progettazione e distribuzione di dispositivi digitali. Sulla prima questione, ai sensi degli artt. 3 e 4 che individuano mandato e obiettivi dell'Agenzia, il ruolo principale della stessa risulta essere legato all'esigenza di innalzare il livello comune di cybersicurezza in tutta l'UE, fungendo da punto di riferimento e da propulsore per lo sviluppo di competenze e risorse tecniche e umane per perseguire i suoi obiettivi. Molto interessante è la definizione che, nell'ambito della individuazione degli obiettivi, il regolamento attribuisce all'ENISA, quale "*centro di competenze nel campo della cybersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite, alle informazioni che mette a disposizione, alla trasparenza delle procedure, ai metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti* (art. 4, n. 1). [48]

Passando al secondo ambito di intervento su cui si concentra il Regolamento, il "Quadro europeo per la certificazione della cybersicurezza" rappresenta un tassello di una complessiva strategia in materia che merita un adeguato approfondimento. Il peso di tale intervento lo si può già avvertire dai Considerando del Regolamento, dove viene affermato che "*sebbene un numero crescente di dispositivi sia connesso a Internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cybersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti individuali, nelle organizzazioni e nelle aziende dispongano di informazioni insufficienti sulle caratteristiche*"[49]. Come anticipato, con questo intervento si produce qualcosa di simile a quanto in ambito *data protection* viene ricondotto alla nozione di *privacy by design,* ossia di una attenzione che il legislatore rivolge alla tutela della privacy sin dal momento della progettazione e costruzione di un determinato programma o dispositivo. In termini generali, questo si esprime in una tutela del bene giuridico che retrocede al momento tecnico, che va ad animare l'attività del

[48] Seppur marginale ai fini della presente trattazione, merita un cenno la determinazione della struttura organizzativa dell'ENISA, disciplinata dall'intero Capo III del Regolamento. In particolare, l'ENISA è formata da: un consiglio di amministrazione, che stabilisce gli orientamenti generali dell'attività dell'Agenzia, adotta il Documento Unico di Programmazione di cui all'art. 24 e coordina il lavoro con gli Stati membri; un comitato esecutivo e un direttore esecutivo, i quali hanno un maggior ruolo di gestione organizzativa e finanziaria, oltre che lo specifico compito di dare seguito concreto alle decisioni assunte dal consiglio di amministrazione; un gruppo consultivo ENISA e una rete di funzionari nazionali di collegamento, essenziali nell'ambito del Quadro di certificazione comune e di un corretto coordinamento con gli Stati Membri.

[49] Considerando n. 3 del Regolamento.

programmatore e che lo responsabilizza di fronte a specifici obblighi di legge. Con tale concetto, in definitiva, si vuole garantire che la protezione del bene oggetto di tutela sia integrata nell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla sua ultima distribuzione, all'utilizzo e all'eliminazione finale[50]. Ebbene, quando si vuole introdurre una certificazione che stabilisca che un determinato prodotto sia stato progettato, costruito e rilasciato secondo determinate regole, le analogie con quanto sopra riportato appaiono evidenti[51]. Venendo nello specifico, tale sistema può essere definito come un "*meccanismo volto a istituire sistemi europei di certificazione della cybersicurezza e ad attestare che i prodotti, servizi e processi ICT valutati nel loro ambito sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita"* (art. 46, par. 2 del reg. UE 881/19). Si tratta di un progetto molto ambizioso, che seppur con alcune attenuazioni e non pochi passaggi intermedi (si pensi, *in primis*, al fatto che tale sistema sarà inizialmente solo volontario, potendo la Commissione renderlo obbligatorio solo a partire dal 2024) appare indubbio che una simile tappa rappresenta un momento fondamentale nella costruzione di una consapevolezza circa la centralità della cybersicurezza nella definizione delle attuali politiche di sicurezza europee e nazionali. Infatti, la certificazione svolge un ruolo fondamentale nel garantire elevati standard di cybersicurezza per i prodotti, servizi e processi con tre effetti fondamentali: l'aumento della fiducia nei consumatori, lo stimolo al mercato della cybersicurezza e un'agevolazione del mercato in tutta l'Unione Europea.

L'Italia ha fatto ulteriori passi avanti dopo il recepimento della Direttiva "NIS", testimoniando la sempre crescente attenzione attribuita al ruolo che la cybersicurezza gioca nelle attuali dinamiche economiche e sociali. Ciò è dimostrato, in particolare, dall'emanazione del d.l. 105 del 2019, il cui impatto dirimente è già delineato dal titolo "*Disposizioni urgenti in materia di perimetro di sicurezza naziona-*

[50] Per un maggiore approfondimento dei temi in ambito privacy e *data protection* si veda G.E. Vigevani, O. Pollicino, C. Melzi D'Eril, *Il diritto della comunicazione e dei media,* op. cit., 69.

[51] Per una trattazione generale dei sistemi di certificazione si veda F. Fracchia, M. Occhiena, *I sistemi di certificazione tra qualità e certezza,* Milano, 2006; A. Benedetti, *Certezza pubblica e certezze private – Poteri pubblici e certificazioni di mercato,* Milano 2010.

le cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica". In particolare, il concetto di "perimetro di sicurezza" rimanda ad una esigenza di universalità di protezione che si pone oltre la categorizzazione in soggetti individuali o imprese, implicando un preciso dovere dello Stato affinché venga garantito un ombrello di protezione sulle infrastrutture digitali del sistema Paese. Tale impianto normativo, a sua volta specificato da una serie di d.P.C.M.[52], ruota intorno al giudizio di idoneità tecnica sulla capacità dell'operatore di agire nel settore, la cui competenza è devoluta al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello Sviluppo Economico con d.m. del 15 febbraio 2019. Dunque, il Governo, prima ancora di valutare l'esistenza o meno di un pericolo per la sicurezza nazionale, dovrà accertarsi che il soggetto rispetti i canoni di adeguatezza tecnica. Quindi, il CVCN adempie sicuramente ad una funzione di "filtro", impedendo a tutti quei soggetti che non ottengano il certificato di idoneità di poter operare in Italia nei settori ad alta intensità tecnologica. Una volta inserito nel perimetro, il soggetto (che può essere tanto di natura pubblicistica quanto privatistica) è a sua volta oggetto di una serie di obblighi di notifica ai CSIRT, di adempimento delle prescrizioni e degli obblighi di comunicazione al CVCN[53]. Va comunque precisato che, dalla *roadmap* rinvenibile sul sito dell'Agenzia Nazionale per la cybersicurezza, viene individuato il 30 giugno 2022 come data per l'inizio dell'attività del CVCN, ma bisognerà certamente attendere per assistere ad una sua piena operatività. L'altro aspetto estremamente interessante del d.l. 105/2019 è relativo al ruolo attribuito ai poteri speciali di controllo sugli investimenti esteri in settori strategici, il cd. *golden power*. Nell'estendere tale disciplina alla tutela degli investimenti nei settori 5G e delle infrastrutture digitali, il legislatore ha inteso attribuire un'altra faccia al *golden power*, ossia quella di strumento facente parte di una più ampia e complessa strategia di c*ybersecurity* nazionale. Va innanzitutto ricordato che tale disciplina, intro-

[52] In particolare, il d.P.C.M. 131/2020, pubblicato nella Gazzetta Ufficiale n. 261 del 21 ottobre 2020, ha dato forma e sostanza al "Perimetro di Sicurezza Nazionale Cibernetica", definendo modalità e criteri procedurali di individuazione dei soggetti pubblici e privati inclusi nel "Perimetro", i principi attraverso i quali questi soggetti dovranno predisporre e aggiornare un elenco delle reti, i sistemi informativi e i rispettivi servizi informatici.

[53] Tra le ulteriori specifiche attribuzioni del CVCN si veda B. Bruno, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali, Federalismi.it*, 2020, 14, 29.

dotta nel nostro ordinamento dal d.l. 15 marzo 2012, n. 21, convertito dalla legge 11 maggio 2012, n. 56[54], nasceva in un'ottica di straordinarietà, collocando tale invadente potere di condizionamento o addirittura di ostacolo all'autonomia privata in una sacca di residualità, con una circoscrizione precisa dei settori di intervento e con una particolare attenzione alle garanzie dei privati. Con il passare del tempo, però, tale disciplina ha avuto un importante irrobustimento, finendo con l'assumere un ruolo sempre più centrale nella definizione delle linee di politica economica degli Stati. In particolare, tale assetto normativo non rappresenta una peculiarità del nostro ordinamento[55], essendo una simile procedura di *screening* degli investimenti esteri presenti in quasi tutti i paesi dell'UE e nei sistemi normativi delle principali potenze economiche mondiali (USA e Cina su tutte le quali, tra l'altro, utilizzano tale armamentario giuridico come vero e proprio strumento di strategia geopolitica e di guerra economica[56]). Tale torsione, indotta dal clima di contrasto geopolitico che a partire dal 2016 si è creato tra le principali potenze economiche mondiali quali Cina e USA, ed ulteriormente acuitosi con il conflitto russo-ucraino, ha chiaramente reso il *golden power* uno

[54] Introduzione normativa che non rappresentava una svolta assoluta, dal momento che il tema dei poteri di controllo sugli investimenti esteri in settori strategici era ben presente sin dagli inizi degli anni Novanta, dal momento che con le normative di privatizzazione delle ex società pubbliche, in particolare con il d.l. 31 maggio 1994, n. 332, convertito dalla legge 31 maggio 1994, n. 332, venne introdotta la cd. "*golden share*", un meccanismo in parte analogo al *golden power* ma che si muoveva in un'ottica eminentemente privatistica e legata agli statuti delle aziende privatizzate. Per una attenta disamina del percorso che ha portato la *golden share* a trasformarsi in *golden power* si veda A. Comino, *Golden powers per dimenticare la golden share: le nuove forme di intervento pubblico sugli assetti societari nei settori della difesa, della sicurezza nazionale, dell'energia, dei trasporti e delle comunicazioni, Rivista italiana di diritto pubblico comunitario*, 2014, 5, 1019; sul fondamentale ruolo giocato in questo processo dalle istituzioni europee, in particolare dalla giurisprudenza della CGUE, si veda F. Santoanastaso, *La "saga" della "golden share" tra libertà di movimento di capitali e libertà di stabilimento,* in *Giurisprudenza commerciale,* 2007, 3.

[55] Per un approfondimento sulla disciplina specifica del *golden power* e per la sua evoluzione normativa si vedano, tra i tanti, R. Garofoli, *Golden power e controllo degli investimenti stranieri* in *Federalismi.it,* 2019, 17; G. Napolitano, *L'irresistibile ascesa del golden power* in *Giornale di diritto amministrativo*, 2019, 5; G. Napolitano, *Il regolamento sul controllo degli investimenti esteri diretti: alla ricerca di una sovranità europea nell'arena economica globale* in *Rivista della regolazione dei mercati,* 2019, 1.

[56] Sulla dimensione geopolitica di tale strumento di diritto pubblico dell'economia si veda A. Aresu, *Dai campioni nazionali al golden power: le prospettive della tutela del sistema-Paese,* in *Osservatorio globalizzazione,* 2020, 16; A. Aresu, *La Geopolitica della protezione,* in *Limes,* 2018, 10.

strumento essenziale al fine di tutelare il più strategico dei settori delle società contemporanee, ossia le infrastrutture digitali e i settori ad alta intensità tecnologica. Su tutti, il tema maggiormente oggetto di contrasto è legato agli investimenti (ma anche alla mera sottoscrizione di contratti) nel settore del 5G e della cd. "alta intensità tecnologica". Ed è proprio in questo contesto che, come si anticipava, il *golden power* finisce con il collocarsi in una più ampia strategia di sicurezza cibernetica nazionale. Infatti, attribuendo allo Stato (e in particolare all'Esecutivo) il compito di valutare minacce derivanti da flussi finanziari provenienti da paesi esteri, si offre uno strumento di tutela della sicurezza nazionale che, inevitabilmente, ricade anche sul concetto di sicurezza cibernetica, in un rapporto *genus ad speciem* che offre una interessante angolatura di considerazione della disciplina del *golden power*. In particolare, i cd. "settori ad alta intensità tecnologica", introdotti con il d.l. 16 ottobre 2017, n. 148, convertito, con modificazioni, dalla legge 4 dicembre 2017, n. 172, allargano il perimetro della nozione di "settori delle telecomunicazione" dell'originario impianto del 2012[57], introducendo nozioni quale quelle di infrastrutture critiche o sensibili, tra le quali rientrano quelle di immagazzinamento e gestione dati e le infrastrutture finanziarie, le tecnologie critiche, compresa l'intelligenza artificiale, la robotica, i semiconduttori, le tecnologie con potenziali applicazioni a doppio uso, la sicurezza in rete, la tecnologia spaziale o nucleare, l' accesso a informazioni sensibili o capacità di controllarle. Ultimo approdo, come si anticipava, è la peculiare disciplina introdotta all'art. 1bis del decreto *golden power* dal d.l. 105/2019, il quale ha previsto la specifica normativa in materia di 5G. In particolare, viene nei fatti stravolto il quadro relativo all'intervento "per settori", prevedendo una possibilità di bloccare addirittura operazioni contrattuali e non societarie, stabilendo che "*la stipula di contratti o accordi aventi ad oggetto l'acquisizione, a qualsiasi titolo, di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti*" relative alla telecomunicazione con tecnologia 5G, ovvero "*l'acquisizione, a qualsiasi titolo, di componenti ad alta intensità tecnologica funzionali*

[57] Il quale era stato a sua volta specificato con il d.P.R. n. 85 del 2014 che aveva individuato, con riferimento al settore delle comunicazioni, tre categorie di *assets* strategici e, segnatamente: le reti dedicate; la rete di accesso pubblica agli utenti finali in connessione con le reti metropolitane, i router di servizio e le reti a lunga distanza; gli impianti utilizzati per la fornitura dell'accesso agli utenti finali dei servizi rientranti negli obblighi del servizio universale e dei servizi a banda larga e ultralarga.

alla predetta realizzazione o gestione, quando posti in essere con soggetti esterni all'Unione europea, è soggetta alla notifica, al fine dell'eventuale esercizio del potere di veto o dell'imposizione di specifiche prescrizioni o condizioni" (art. 1 bis, comma 2). L'attenzione è tutta rivolta alla realizzazione di una profilazione del soggetto che si propone nella erogazione del servizio, il quale dovrà fornire un'informativa completa sul proprio *business plan* e sulla propria compagine azionaria. Questa documentazione dovrà essere trasmessa nel termine di dieci giorni dalla conclusione del contratto alla Presidenza del Consiglio per consentire l'avvio dell'istruttoria di cui al d.l. 21/2012 e i successivi decreti attuativi.[58] Il legislatore del 2019, pur richiamando gli stessi parametri da seguire al fine di pervenire alla scelta sull'esercizio o meno del *golden power*, ossia la "minaccia di grave pregiudizio" , palesa delle preoccupazioni più specifiche rispetto al tema dei rischi di una devoluzione in mano straniera della gestione e manutenzione delle reti 5G. Infatti, ai fini della valutazione sulla opportunità o meno di esercizio dei poteri, il Governo deve tener conto della presenza di "*fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano*" (così come previsto alla luce del nuovo art. 1 bis d.l. 21/2012). Si pone quindi un tema più ampio di sicurezza nazionale, nel caso specifico di cybersicurezza. Alla luce di ciò, appare inevitabile la conclusione a cui si accennava in premessa: la precisa volontà di rendere il *golden power* uno strumento collocato in un più complesso armamentario posto a salvaguardia della sicurezza cibernetica del Paese.

---

[58] Il riferimento è ai d.P.R. 19 febbraio 2014, n. 35 e 25 marzo 2014, n. 86, con cui sono state individuate le procedure per l'attivazione dei poteri speciali, rispettivamente, nei settori della difesa e della sicurezza nazionale e dell'energia, dei trasporti e delle comunicazioni.

In estrema sintesi, il procedimento è demandato al Gruppo di Coordinamento interministeriale costituito ai sensi dell'art. 3 d.P.C.M. 6 agosto 2014 e presieduto dal Segretario generale della Presidenza del Consiglio dei ministri. Ruolo preminente all'interno del Gruppo è assunto dal Ministro competente a seconda del settore interessato, il quale entro il termine individuato per legge (45 giorni) ha l'obbligo di concludere l'istruttoria. All'esito di questa, si giunge poi all'emanazione del decreto del Presidente del Consiglio dei ministri di esercizio dei poteri speciali, tramite l'imposizione di condizioni o il veto, oppure alla delibera del Consiglio dei ministri con cui si dispone il non esercizio dei poteri speciali. Per ulteriori approfondimenti e per le problematiche sollevate in ordine a tale peculiare procedimento si rimanda a G. Della Cananea, *Golden power e garanzie*, in G. Della Cananea, L. Fiorentino (a cura di), *I poteri speciali del Governo nei settori strategici*, Napoli, 2020.

3.3 Il d.l. 82/2021 e i più recenti interventi in Italia

Sulla base di quanto esposto fino ad ora, si può dire che fino ai più recenti interventi, sulle cui origini ci si soffermerà a breve, l'impianto normativo italiano in materia di cybersicurezza era essenzialmente un'appendice del Sistema di informazione per la sicurezza della Repubblica, disciplinato dalla l. 3 agosto 2007, n. 124, con un'organizzazione fondata su quattro livelli di cui si è già parlato precedentemente (si veda § 3.1). Prima di incentrarsi sull'analisi dettagliata della grande svolta istituzionale e politica che si è avuta con l'approvazione del d.l. 14 giugno 2021 n. 82 dal titolo "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", è necessario un sintetico cenno su quelli che sono stati i principali stimoli che hanno portato il nostro Paese a dare una maggiore razionalizzazione e specializzazione del sistema di sicurezza cibernetica nazionale, con l'istituzione dell'Agenzia Nazionale per la Cybersicurezza Nazionale (ACN) e con il rilevante accentramento di competenze in essa transitate ad opera del medesimo decreto.
La principale spinta propulsiva è arrivata, senza alcun dubbio, dal Piano Nazionale di Ripresa e Resilienza, il grande progetto di ripartizione dei fondi straordinari europei derivanti dal maxibond emesso dalla Commissione europea con il piano *Next Generation UE*[59], che ha due obiettivi fondamentali: riparare i danni economici e sociali della crisi pandemica e contribuire ad affrontare le debolezze strutturali dell'economia italiana. In particolare, Il Piano Nazionale di Ripresa e Resilienza definitivo ammonta complessivamente a 222,1 miliardi di euro, di cui 191,5 miliardi riferibili al piano *Next Generation UE* e 30,6 miliardi del Fondo Complementare istituito con Decreto Legge n.59 del 6 maggio 2021, in forza dello

[59] Il Piano Nazionale di Ripresa e Resilienza (PNRR), infatti, si pone quale implementazione nazionale del programma *Next Generation EU* (NGEU), il pacchetto da 750 miliardi di euro, costituito per circa la metà da contributi a fondo perduto e per la restante parte da prestiti a tassi agevolati, concordato dall'Unione Europea in risposta alla crisi pandemica. La principale componente del programma NGEU è il Dispositivo per la Ripresa e Resilienza (*Recovery and Resilience Facility*, RRF), che ha una durata di sei anni, dal 2021 al 2026, e una dimensione totale di 672,5 miliardi di euro (312,5 sovvenzioni, i restanti 360 miliardi prestiti a tassi agevolati). Per una approfondita disamina del poderoso intervento si rimanda al documento ufficiale: "Il Piano Nazionale di Ripresa e Resilienza (PNRR) - Ministero dell'Economia e delle Finanze" (mef.gov.it).

scostamento pluriennale di bilancio approvato nel Consiglio dei ministri del 15 aprile. Per quanto riguarda ciò che interessa in questa sede, nell'ambito di quella che viene definita la "Prima Missione", intitolata "Digitalizzazione, innovazione, competitività, cultura", la transizione digitale sarà il primo obiettivo del PNRR e stanzierà 49,2 miliardi, di cui 40,7 miliardi dal Dispositivo per la ripresa e la resilienza e 8,5 miliardi dal Fondo Complementare. A fronte di questi, vengono impiegate cospicue risorse, 620 milioni di euro, nello specifico investimento 1.5 intitolato proprio "*Cybersecurity*", il cui principale beneficiario risulta proprio essere l'Agenzia Nazionale per la Cybersicurezza. Appare logico che a fronte di uno sforzo finanziario così rilevante venisse sottoscritto un impegno per fare in modo che il nostro Paese si dotasse di un sistema di sicurezza cibernetica molto più strutturato e specializzato e puntasse, per la prima volta, al raggiungimento di un'autonomia tecnologica nazionale. Ed è lo stesso d.l. 82/2021 a prevedere un intervento riformatore al fine di dare attuazione al Piano nazionale di ripresa e resilienza, che prevede apposite progettualità nell'ambito della cybersicurezza, in particolare per l'istituzione di un'Agenzia di cybersicurezza nazionale, quale fattore necessario per tutelare la sicurezza dello sviluppo e della crescita dell'economia e dell'industria nazionale, oltre ad altri tipi di interventi che fanno leva sul coinvolgimento dei principali partner della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia.. Dalla centralità della transizione digitale in questa fase storica del nostro Paese deriva, come diretta conseguenza, un ruolo altrettanto fondamentale della cybersicurezza (sulla profonda interconnessione tra queste si rimanda a §2). Ma oltre a queste cause che potremmo definire "istituzionali", sono state anche le vicende di più stretta attualità a rendere palese che in un mondo sempre più digitalizzato ed interconnesso i rischi da dover mitigare debbano essere affrontati con interventi calibrati per lo specifico dominio cibernetico[60]. In particolare, l'evento che più di tutti ha rafforzato l'impegno governativo nell'accelerare il processo di riforma fu il grave cyberattacco che colpì la rete informatica della Regione Lazio, mandando in tilt i servizi digitali a privati e aziende, tra cui il sistema

[60] Non può non citarsi, in particolare, l'importanza attribuita al dominio cibernetico da parte della NATO: nel Vertice di Varsavia del 2016, infatti, la Nato ha elevato lo spazio cibernetico a dominio operativo, equiparandolo agli altri domini militari convenzionali (aereo, militare e terrestre). Si rimanda nello specifico al documento ufficiale approvato in merito, il *Cyber Defense Pledge* dell'8 luglio 2016.

informatico sanitario e quello dedicato alla vaccinazione contro il COVID-19[61]. Se poi guardiamo a come la situazione sia evoluta nel corso di un solo anno e come questi episodi si siano moltiplicati (anche in ragione del conflitto russo-ucraino), si può assolutamente concludere che quella "necessità e urgenza" così tanto abusata dalla normazione mediante decreti-legge sia stata in questo caso adeguatamente e correttamente ponderata.

Passando ad una disamina specifica del d.l. 14 giugno 2021 n. 82, notiamo come un ruolo centrale nell'economia dell'intero sistema sia sempre attribuito al Presidente del Consiglio dei Ministri, al quale sono attribuite ai sensi dell'art. 1 del d.l. 82/2021 in via esclusiva "*l'alta direzione e la responsabilità generale delle politiche di cybersicurezza; l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza*" (di cui si è già detto, vedi § 3.1) *di cui all'articolo 4*; *la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale"*. Ugualmente vengono razionalizzate e specificate le competenze di un altro organo già facente parte del precedente sistema di cybersecurity nazionale, ossia il già citato Comitato Interministeriale per la cybersicurezza, al quale ai sensi dell'art. 4 del d.l. 82/2021 sono attribuiti compiti di proposta alla Presidente dal Consiglio degli indirizzi generali in materia di cybersicurezza nonché di promozione delle iniziative di collaborazione nazionale e internazionale; inoltre, il CIC esprime una funzione di valutazione del bilancio preventivo e consuntivo dell'Agenzia per la cybersicurezza e, soprattutto, esercita l'alta sorveglianza per l'attuazione della strategia nazionale per la cybersicurezza nazionale (su cui si tornerà in seguito). A dimostrazione della universalità e trasversalità delle esigenze di sicurezza cibernetica, assume particolare rilievo la composizione di detto organo interministeriale, il quale, ai sensi del comma 3 dell'art. 4, "*è composta dall' Autorità delegata, il Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico, dal Ministro della transizione ecologica, dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale e dal Ministro delle infrastrutture e della mobilità sostenibili"*. Il

[61] Per un approfondimento della vicende e per una considerazione di sistema dell'episodio si rimanda a *Attacco hacker alla Regione Lazio: cosa sappiamo e cosa ci insegna* in *PandaSecurity* del 21 settembre 2021 e *Il cyber attacco alla Regione Lazio e la vulnerabilità delle infrastrutture italiane, in Analisi Difesa* del 4 agosto 2021.

fatto che il Presidente del Consiglio dei Ministri occupi il ruolo di presidente conferma il ruolo apicale attribuito al capo dell'esecutivo nel complessivo quadro risultante dall'intervento riformatore.
Prima di concludere e di passare alla approfondita dinamica di quella che rappresenta la vera grande novità introdotta dal d.l. 82/2021, ossia dell'Agenzia nazionale per la cybersicurezza nazionale, occorre svolgere una breve analisi dell'ultimo e recentissimo atto di questo variegato e complesso percorso normativo che si è cercato di ripercorrere. Il riferimento è alla recente emanazione della Strategia Nazionale di cybersicurezza 2022-2026, ossia di un fondamentale momento di indirizzo politico (che deve la sua paternità all'art. 7 della Direttiva NIS, come già affrontato, vedi §3.1) espresso dal CIC nella riunione del 18 maggio 2022, durante la quale si è provveduto anche a emanare l'ultimo d.P.C.M. per la realizzazione del Perimetro di sicurezza nazionale cibernetica gestito dall'Agenzia per la Cybersicurezza Nazionale, la cui introduzione risultava necessaria, come si è già avuto modo di approfondire (si veda §3.2) per la piena operatività dello stesso ai sensi dell'art. art. 1 co.7, lett. B) d.l. 105/2019.[62]
Venendo a quanto previsto dalla Strategia, i suoi 85 punti programmatici assumono valenza concreta solo se combinati con l'annesso Piano di implementazione, approvato durante la medesima riunione del CIC, il quale consente di dare copertura finanziaria e operativa alle ambizioni contenute nella Strategia. Ciò che maggiormente colpisce di questo documento è la capacità di visione d'insieme che si offre al tema della *cybersecurity,* cogliendone la trasversalità ed universalità in un'ottica di collaborazione tra pubblico e privato e di coinvolgimento della società civile, rendendo possibile una qualificazione della cybersicurezza quale bene pubblico, (sulle tesi che sostengono tale argomentazione si tornerà più approfonditamente in seguito, come si vedrà nel §5). Nel delineare quelli che sono gli obbiettivi da perseguire, nella seconda sezione della Strategia, viene individuata una tripartizione composta dai concetti di "protezione, risposta e sviluppo". Per quanto concerne la protezione, questa si pone come una esigenza di valorizzazione di competenze volte a porre in essere un quadro normativo e delle misure tecnico-opera-

[62] In particolare, in tale normativa di rango secondario sono indicati i criteri che i centri privati devono rispettare per accreditarsi come laboratori di prova per il Centro di valutazione e certificazione nazionale (CVCN) per verificare sicurezza, assenza di vulnerabilità note, contenuti, comunicazione tra il CVCN e i laboratori stessi e tra il CVCN e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa.

tive orientate alla gestione e mitigazione del rischio cyber, con un ruolo apicale in tal senso rivestito dal CVCN (di cui si è già parlato, si veda § 3.3) e dall'apporto concreto che può essere offerto in tal senso dalle altre pubbliche amministrazioni (in particolare i Centri di Valutazione del Ministero dell'Interno e della Difesa) e dai soggetti privati. Il secondo obiettivo, ossia la risposta, ha a cuore la capacità di garantire un intervento tempestivo e risolutivo in caso di attacco *cyber*, prevendendo una rete di monitoraggio, rilevamento, analisi e, per l'appunto, risposta capace di coinvolgere tutti gli attori che operano nell'ecosistema della cybersecurity nazionale ed internazionale (tale sistema di gestione delle crisi è affidato, nel nostro caso, al Nucleo per la Cybersicurezza e dai CSIRT, di cui si dirà in seguito)[63]. Infine, il terzo obiettivo principale è relativo allo sviluppo, dove viene data enorme importanza alle capacità di ricerca che il mondo accademico e delle imprese può offrire in tal senso. In un settore in così costante evoluzione come quello relativo alle tecnologie digitali, garantire adeguata attenzione e, soprattutto, risorse alle capacità di aggiornamento e di adeguamento del sistema consente di dare concretezza a tutto quanto detto in precedenza. Sempre parlando di sviluppo, il documento si conclude con un interessantissimo richiamo alla necessità di promozione della cultura della sicurezza cibernetica, al fine di aumentare la consapevolezza del settore pubblico e privato e della società civile sui rischi e le minacce *cyber*, le quali includono anche fenomeni come la diffusione di contenuti *fake* e di distorsione dell'opinione pubblica che presenta un medesimo livello di offensività per la società contemporanea (sul tema di tornerà in seguito, vedi §5).

4. L'Agenzia nazionale per la *cybersecurity*: natura, poteri e funzioni

Il principale intervento, rappresentativo dell'autentica svolta politica prima ancora che giuridica realizzata dal nostro Paese, contenuto nel d.l. 82/2021, in particolare all'art. 5, è l'istituzione dell'Agenzia Nazionale per la *Cybersecurity*. Questo nuovo soggetto istituzionale, la cui prefigurazione era già avvenuta in sede di emanazione della Direttiva "NIS" (come si è visto precedentemente, § 3.1), si affianca al ruolo eminentemente politico rivestito dal CIC, garantendo un

[63] In tema di gestione degli incidenti e delle crisi di cybersicurezza, si rimanda all'interessante approfondimento presente nella Strategia Nazionale di Cybersicurezza alla pag. 20.

profilo di specializzazione delle competenze certamente in linea con quelle esigenze già elencate di rafforzamento del sistema di cybersecurity nazionale (si veda § 3.3). Oltre a ciò, con la creazione dell'Agenzia si è riconosciuta autonoma dignità alle nozioni di sicurezza e resilienza cibernetica, attraverso un più ampio ruolo di sinergia e coordinamento dei vari soggetti coinvolti ad opera di un'a*uthority* ad hoc. Infine, si è inteso costruire un ulteriore pilastro tecnico operativo nell'architettura nazionale di cybersicurezza, affiancando i compiti di cura della c*ybersecurity* e resilienza attribuiti all'Agenzia agli altri attori già fino a quel momento in campo, in particolare all'attività di prevenzione e contrasto alla criminalità informatica di competenza della Polizia di Stato attraverso il Servizio di Polizia postale e delle Comunicazioni[64], a quella di difesa e sicurezza militare affidata invece al Ministero della Difesa e, infine, al ruolo di ricerca ed elaborazione informativa affidata al comparto Intelligence. Passando alle disposizioni del d.l. 82/2021, gli artt. 5-6-7 individuano le attribuzioni dell'Agenzia Nazionale per la cybersicurezza, il cui insieme consente di definire tale istituzione come "*soggetto pubblico che svolge una funzione strumentale all'esercizio delle competenze*"[65] attribuite dal medesimo decreto al Presidente del Consiglio dei ministri, a tutela degli interessi nazionali nel campo della cybersicurezza. La scelta organizzativa adottata è ricaduta sulla "agenzia": tale *species* organizzativa (già prevista a livello generale dalla legge sull'organizzazione del Governo ex art. 8, co. 1 del d.lgs n. 300 del 1999) consente di destinare a specifici soggetti istituzionali una attività a carattere tecnico-operativo, con un grado di autonomia funzionale e di bilancio che consente di delinearne una autonoma personalità giuridica, pur operando sempre al servizio delle amministrazioni pubbliche.[66] Nel caso di specie, l'ANC, ai sensi del comma 2 dell'art. 5, "*ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria*". Tale ampia caratterizzazione consente di apprezzare un maggiore spazio di autonomia lasciato alla ANC, come tra l'altro ben sottolineato dal

[64] A questa va aggiunto il ruolo dell'Arma dei Carabinieri con il Reparto Indagini Telematiche del Raggruppamento Operativo Speciale (ROS) e della Guardia di Finanza con il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche.

[65] F. Serini, *La nuova architettura della cybersicurezza,* op. cit., 5.

[66] Per un approfondimento su tale forma organizzativa si veda D. Sorace, *Diritto delle amministrazioni pubbliche,* op. cit., 95; L. Casini, *Le agenzie amministrative*, in *Riv. trim. dir. pubbl.*, 2003, 3, 393; C. Corsi, *Agenzia e agenzie: una nuova categoria amministrativa?,* Torino, 2005;

Dossier del Servizio studi della Camera, discostando tale peculiare esperienza dal modello sopra richiamato del d.lgs. 300 del 1999[67]. Vero e proprio punto di incontro tra l'attività tecnico-operativa dell'Agenzia e quella di indirizzo espressa dal CIC e dalla Presidenza del Consiglio dei Ministri è il direttore dell'Agenzia[68], quale "*diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, ed è gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia*". Tale figura, nel complesso, sembra assumere un ruolo di particolare rilievo, sia sul piano prettamente operativo quanto su quello di rappresentanza dell'Agenzia nelle sue attività nazionali ed internazionali[69]. Subito dopo la figura del Direttore generale vi è quella del Vice Direttore[70], la cui nomina esula degli stringenti requisiti di cui all'art. 18 della l. 400 del 1988 ma il cui mandato è soggetto ai medesimi incarichi e funzioni di quella del Direttore generale.
Per quanto concerne l'organizzazione complessiva dell'Agenzia, questa viene delegata dall'art. 6 del d.l. 82/2021 ad un regolamento attuativo che è arrivato, con insolita tempestività, con l'emanazione del d.P.C.M. 9 dicembre 2021, n. 223, dal titolo "*Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale*". Tale norma ha delineato con maggiore precisione il profilo di un altro importante organo dell'ANC, ossia il Collegio dei revisori

[67] Il riferimento è al Dossier A.C. 3161 "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*" del 23 luglio 2021, 19.

[68] Il comma 3 dell'articolo 5 delinea il profilo e la regolamentazione dell'incarico del direttore, prevedendo che questi è scelto soggetti appartenenti a una delle categorie di cui all'articolo 18, comma 2, della legge 23 agosto 1988, n. 400, (ossia di quelli candidabili al ruolo di Segretario Generale alla Presidenza del Consiglio dei Ministri, quali tra i magistrati delle giurisdizioni superiori ordinaria ed amministrativa, gli avvocati dello Stato, i dirigenti generali dello Stato ed equiparati, i professori universitari di ruolo ovvero tra estranei alla pubblica amministrazione) in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione. Gli incarichi del direttore generale e del vice direttore generale hanno la durata massima di quattro anni e sono rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni.

[69] Nell'agosto 2021 Roberto Baldoni, già Vice Direttore Generale del DIS, è stato nominato dal Presidente del Consiglio Mario Draghi, previa deliberazione del Consiglio dei ministri e comunicazione al Presidente del COPASIR e alle Commissioni parlamentari competenti, Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, un mandato che ha assunto da settembre 2021.

[70] Il 16 settembre 2021 Nunzia Ciardi, già capo della Polizia Postale e delle Comunicazioni, è stata nominata dal Presidente del Consiglio Mario Draghi Vice Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale.

dei conti, il quale svolge, ai sensi dell'art. 7, importanti funzioni di controllo contabile effettuando il riscontro degli atti della gestione finanziaria e formula le proprie osservazioni, svolgendo almeno una volta ogni tre mesi, verifiche di cassa e di bilancio ed esprime, in apposita relazione, parere sul progetto di bilancio preventivo, nonché sul rendiconto annuale. Tornando al d.P.C.M. 231/2021, questo razionalizza l'organizzazione interna dell'Agenzia, prevedendo al suo articolo 4 una distinzione tra "Divisioni" e "Servizi"[71] e specificando compiti e attribuzioni del Direttore generale[72].

Passando alle funzioni dell'Agenzia nazionale per la cybersicurezza, queste vengono individuate dall'art. 7 del d.l. 82/2021, e possono essere essenzialmente ricondotte a 4 filoni principali che ci si appresta ad analizzare analiticamente: "*l'esercizio di funzioni derivanti dalla qualifica di Autorità nazionale per la cybersicurezza; il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale; la promozione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni; il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a*

[71] In particolare, i Servizi sono istituiti, nel numero di sette quali strutture di livello dirigenziale generale nei limiti stabiliti dall'articolo 6, comma 1, del decreto-legge, a presidio di ambiti di notevole ampiezza e complessità, che sono direttamente correlati alle funzioni e alle politiche generali dell'Agenzia, e questi vengono individuati in: Gabinetto; Autorità e sanzioni; Certificazione e vigilanza; Operazioni; Programmi industriali, tecnologici, di ricerca e formazione; Risorse umane e strumentali; Strategie e cooperazione. Mentre invece le Divisioni sono istituite per la gestione di un insieme omogeneo di tematiche e macro-processi e operano, di norma, all'interno dei Servizi. Nel numero massimo di trenta, sono individuate le Divisioni di maggiore complessità, quali articolazioni di livello dirigenziale non generale.

[72] Nello specifico, l'art. 5 del d.P.C.M. specifica le attribuzioni del direttore generale, in particolare: a) è il legale rappresentante dell'Agenzia e ne ha la rappresentanza esterna; b) cura i rapporti con le pubbliche amministrazioni nazionali e con i soggetti pubblici e privati, con le istituzioni, gli organismi e le agenzie dell'Unione europea, nonché con le organizzazioni estere ed internazionali; c) svolge le funzioni di segretario del CIC, supportandone le funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza; d) partecipa alle riunioni del Comitato interministeriale per la sicurezza della Repubblica (CISR), di cui all'articolo 5 della legge 3 agosto 2007, n. 124 in materia di gestione delle situazioni di crisi di cui all'articolo 10, comma 1, del decreto-legge; e) presiede il Nucleo per la cybersicurezza, il Tavolo Perimetro, il Comitato tecnico di raccordo (CTR) e il Comitato tecnico-scientifico (CTS), istituiti presso l'Agenzia; f) sottoscrive i contratti, ove non siano espressamente delegati i Capi dei Servizi competenti, ovvero altro personale dell'Agenzia; g) svolge le altre funzioni espressamente attribuite dalla legge e dai regolamenti o dal Presidente del Consiglio dei ministri.

tutela degli interessi nazionali nel settore"[73]. Partendo dal primo, è evidente che il fatto stesso che l'Autorità si ponga in un tale veste operativa faccia sì che essa finisca per attrarre tutte quelle competenze che in precedenza erano rimaste frammentate tra le varie amministrazioni, oltre che chiaramente esercitarne talune specificamente create *ad hoc*, quale la predisposizione della Strategia nazionale di cybersicurezza. Venendo ai compiti "acquisiti", questi derivano principalmente dal MISE (in particolare riguardo le competenze in tema di CVCN che passa sotto l'egida e il controllo organizzativo dell'ANC), dalla Presidenza del Consiglio dei ministri, dal Dipartimento delle informazioni e della sicurezza e dall'Agenzia per l'Italia digitale (specialmente riguardo alle competenze e funzioni già affrontate con il Decreto NIS e con il decreto istitutivo del Perimetro Nazionale di sicurezza cibernetica). Tale consegna di attribuzioni è molto rilevante, dal momento che finisce per consentire all'Agenzia di "*condurre attività di ispezione e verifica anche su soggetti pubblici afferenti al Perimetro, conferendole così un generale potere di ispezione, verifica e accertamento delle violazioni su tutti i soggetti, sia pubblici che privati, afferenti al PSNC*"[74]. In tal senso, si giustifica pienamente quella già richiamata nozione di agenzia, che fa dell'esercizio di attività tecnico-operative caratterizzate da altissima specializzazione tecnica il suo nucleo portante.

Venendo al secondo filone di attribuzioni, ossia quello relativo al coordinamento tra i vari soggetti pubblici coinvolti nel sistema nazionale di cybersicurezza, appare evidente che si faccia menzione in questo caso ad una attività di collaborazione con soggetti quali il Garante per la protezione dei dati personali o altre Autorità indipendenti, le Forze armate e di polizia e gli altri enti pubblici. Un più generale obbligo di leale collaborazione quale principio generale dell'ordinamento innerva tale norma.[75]

Passando al terzo filone, ossia la promozione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche, appare pertinente il richiamo all' art. 7, co. 1, lett. m-*bis*) del d.l. n. 82 del

---

[73] F. Serini, *La nuova architettura di sicurezza cibernetica,* op. cit., 245.

[74] F. Serini, *La nuova architettura di sicurezza cibernetica,* op. cit., 253.

[75] In merito a quest'ultimo, volendo coglierne la sua portata generale, sia il Consiglio di Stato che la Corte costituzionale hanno tratto a partire dall'art. 97 Cost. il principio in virtù del quale "*rapporti tra pubblici poteri sono improntati al principio della leale collaborazione, il quale si lega strettamente a quello di sussidiarietà, e si concretizza nella collaborazione reciproca nell'esercizio delle funzioni amministrative spettanti a ciascun livello di governo, nella comunicazione dei dati informativi, nelle iniziative in programma*". Tra le tante, si veda Corte cost., 1 gennaio 1991, n. 37 e Cons. Stato, Sez. VI, 5 marzo 2014, n. 1059.

2021, ove è precisato che l'ACN può farsi promotrice di tale iniziativa "*anche attraverso un'apposita sezione dedicata nell'ambito della strategia*". E infatti, come già visto, la seconda sezione della Strategia è proprio dedicata agli obiettivi da perseguire nell'ambito della visione strategica nazionale, attraverso quei tre pilastri fondanti costituiti da protezione, risposta e sviluppo già analizzati (si veda § 3.3). In seconda battuta, nell'ambito di tale intervento può essere inquadrata anche la possibilità di collaborazione con partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei Ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri. Infine, l'obiettivo relativo al "*conseguimento dell'autonomia nazionale ed europea su prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore della sicurezza cibernetica*" centra a pieno uno dei temi e delle questioni maggiormente dibattute e di più stringente attualità, quale è quella della sovranità digitale nazionale ed europea e della esigenza di affrancamento dalle tecnologie e dalle catene di approvvigionamento estere.[76] Il tema investe diverse questioni, prima fra tutte "*quella relativa alla catena di approvvigionamento di tali prodotti e servizi, la c.d. supply chain, ossia quell'insieme di processi che interessano la distribuzione di hardware e software, storage in cloud o locale, a cui deve essere garantito un certo livello di affidabilità in termini di sicurezza informatica*"[77].

A conclusione della disamina non può non farsi cenno ad altre due strutture che rientrano nell'organizzazione dell'ANC, ossia del Nucleo per la cybersicurezza e il CSIRT Italia (*Computer Security Response Team*). Questi soggetti istituzionali, seppure già presenti nell'ordinamento italiano a partire dal Decreto NIS, hanno subito un processo di migrazione presso la struttura organizzativa dell'ANC che ne ridisegnano la collocazione ordinamentale. Per quanto concerne il primo, ai sensi dell'art. 8 del d.l. 82/2021, il Nucleo per la cybersicu-

[76] Se si pensa ai più recenti avvenimenti, si può notare la profonda apprensione creata dai rischi sollevati dal fatto che il più noto software antivirus utilizzato nelle Pubbliche Amministrazioni, chiamato *Kaspersky* e prodotto da un'azienda russa, potesse provocare una serie di rischi e possibilità di penetrazione nel perimetro di sicurezza cibernetico italiano in conseguenza della crisi ucraina. In particolare, fu proprio l'ANC che il 15 marzo 2022 emanò un report su una analisi del rischio tecnologico e della conseguente esigenza di diversificazione. Tale alert raccomandava di "*considerare le implicazioni di sicurezza derivanti dall'utilizzo di tecnologie informatiche fornite da aziende legate alla Federazione Russa, procedendo urgentemente a un'analisi del rischio derivante dalle soluzioni di sicurezza informatica utilizzate e di considerare l'attuazione di opportune strategie di diversificazione*".

[77] F. Serini, *La nuova architettura di cybersicurezza,* op. cit.*,* 259.

rezza svolge compiti di supporto per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. È composto in via permanente presso l'Agenzia da vari soggetti istituzionali quali, il Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS e dell'Agenzia informazioni e sicurezza esterna (AISE), oltre che del Dipartimento di Protezione civile. La struttura è logicamente presieduta dal Direttore generale dell'Agenzia. Tra le principali funzioni rientrano quella di "*formulare proposte di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia e di promuovere, la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale*"[78]. La struttura, quindi, è collegata al CSIRT dal momento che riceve da quest'ultima le notifiche relative agli incidenti e funge da collegamento tra il piano operativo e quello politico. Infatti, è proprio il CSIRT Italia, collocato presso l'Agenzia ma già operante nel nostro ordinamento dal 2018[79], a svolgere i compiti maggiormente operativi, in particolare questi includono: il monitoraggio degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale. Il CSIRT Italia partecipa attivamente anche alla "CSIRT Network", la rete composta dagli CSIRT europei per contribuire a sviluppare la fiducia tra gli Stati membri UE e promuovere la cooperazione internazionale, di cui si è già parlato precedentemente (§3).

5. Una infrastruttura cibernetica sicura è un bene pubblico?

La ricostruzione degli interventi normativi sull'attuale sistema normativo italiano di cybersicurezza evidenzia come, ad oggi, l'architettura istituzionale in materia sia essenzialmente costruita su due livelli. Vi è un primo piano che vede un ruolo di indirizzo politico attribuito al Presidente del Consiglio dei Ministri e all'Autorità delegata (nel caso italiano questo si è tradotto nella creazione di una

[78] Art. 8 d.l. 82/2021.

[79] In particolare, è stato introdotto dal d.lgs. 18 maggio 2018, n. 65 e dal d. P.C.M. 8 agosto 2019 art. 4.

carica Sottosegretario di Stato alla Presidenza del Consiglio quale Autorità delegata per la sicurezza della Repubblica) e un secondo livello caratterizzato da un'attività tecnico-operativa demandata all'Agenzia Nazionale per la Cybersicurezza nelle sue diverse articolazioni (CVCN, Nucleo per la *cybersecurity* e CSIRT). Tale complessa evoluzione, sebbene indotta da fattori esterni quali il PNRR e le incessanti evoluzioni economico-sociali, conduce ad una riflessione di fondo circa il nuovo modo di intendere il concetto di cybersicurezza nella prospettiva del ruolo dello Stato. In particolare, sembra delinearsi un quadro che rende interessante la discussione relativa alla possibilità o meno di inquadrare la *cybersecurity* nel novero dei beni pubblici[80], intendendo tale tradizionale categoria come riferibile ad una serie di beni caratterizzati dal fatto che "*il loro consumo presenti le caratteristiche della non-rivalità e non-escludibilità, ossia quando la propria fruizione può essere garantita a più agenti simultaneamente e quando nessuno può essere escluso dalla possibilità di usufruirne, con la possibilità per gli utenti di non sostenere alcun costo* (cd. *free riding*)"[81]. Appare interessante notare come la cybersicurezza possa collegarsi alla definizione di bene pubblico con particolare riferimento alla cd. "robustezza dei sistemi", ossia a quelle famose esigenze di riservatezza, integrità e disponibilità alle quali i sistemi di tutela delle infrastrutture cibernetiche che innervano e fanno funzionare i sistemi operativi sui quali quotidianamente viviamo devono tendere (la famosa triade "RID" di cui si è già detto, vedi §2). La dottrina economico-giuridica del bene pubblico, infatti, "*rivela un interessante quadro di responsabilità condivise, nell'ottica del comune interesse ad avere un soddisfacente grado di sicurezza dei sistemi informatici alla base delle nostre società*"[82], dove si individuano la redistribuzione delle responsabilità, la cooperazione pubblico-privato e lo scambio di informazioni come gli elementi cardine per una dottrina della *cybersecurity* come bene pubblico[83]. Se

[80] Si fa riferimento al dibattito introdotto in R. Brighi, P. Chiara, *La cybersecurity come bene pubblico*, op. cit.

[81] Definizione questa attribuita ai risultati dei lavori della Commissione Rodotà nel primo decennio del 2010 per una riforma del sistema italiano dei beni pubblici, si veda U. Mattei, E. Reviglio, S. Rodota', *Invertire la rotta: Idee per una riforma della proprietà pubblica*, Bologna, 2007, 58.

[82] R. Brighi, P. Chiara, *La cybersecurity come bene pubblico,* op. cit., 40.

[83] Particolare rilevanza ha assunto questo dibattito negli Stati Uniti, a fronte di una forte dialettica tra ruolo del pubblico e del privato nello sviluppo dei sistemi di sicurezza cibernetica. In particolare, si veda M. Taddeo, *Is Cybersecurity a Public Good ?,* op. cit., 354; P. Rosenzweig, *Cybersecurity and Public Good*, op. cit., 7.

si sposa tale concezione, si individua la cybersicurezza innanzitutto come un "*compito del settore pubblico stabilire norme, procedure di certificazione, collaudo e verifica in grado di garantire un livello sufficiente di sicurezza"*, al tempo stesso è richiesto comunque uno sforzo dall'altra parte, dal momento che è "*il settore privato ad essere robusti e dello sviluppo e del miglioramento di nuovi metodi di sicurezza*"[84] responsabile della progettazione di sistemi. Sulla scorta di una tale ricostruzione, assume un enorme importanza la combinazione di sforzi tra pubblico e privato, che nel nostro ordinamento finisce con l'avere una importante ricaduta sull'istituto del partenariato pubblico-privato (il cd. PPP[85]), destinato a rivestire un ruolo sempre più importante, anche alla luce della rilevantissima posizione che gli viene attribuito della Strategia di cybersicurezza nazionale. Riportando questa analisi nell'ambito di questa ultimissima innovazione normativa, è proprio il ruolo del privato che finisce con il rivestire una rilevanza strategica, con il preciso obiettivo di fare in modo che le enormi competenze che possono emergere dal mondo dell'impresa e dell'università siano messe a disposizione dell'interesse pubblico alla sicurezza e resilienza delle infrastrutture cibernetiche. Una prospettiva diversa, ma decisiva e che inverte la tendenza rispetto ad una costruzione di un sistema di sicurezza cibernetica solamente incentrato sul ruolo dello Stato e dei suoi apparati. Una prospettiva che legga la *cybersecurity* come bene pubblico, e dunque come un interesse il cui soddisfacimento passa per più apporti concreti, derivino essi dallo Stato, dal mondo delle imprese o delle università e dalla stessa società civile. Dove i

---

[84] M. Taddeo, *Is Cybersecurity a Public Good ?*, op. cit., 351.

[85] Il PPP comprende una vasta gamma di modelli di cooperazione tra il settore pubblico e quello privato. Il ricorso al PPP, attraverso le sue diverse metodologie attuative può, in generale, essere evocato in tutti quei casi in cui il settore pubblico intenda realizzare un progetto che coinvolga un'opera pubblica, o di pubblica utilità, la cui progettazione, realizzazione, gestione e finanziamento, in tutto o in parte, siano affidati al settore privato. Per una più diffusa trattazione di questa specifica forma di collaborazione tra pubblico e privato si veda, tra i tanti, R. Dipace*, Partenariato pubblico privato e contratti atipici,* Milano, 2006, 76; M. Chiti, *I partenariati pubblico-privati e la fine del dualismo tra diritto pubblico e diritto comune*, Napoli, 2010; S. Amorosino, *Profili sistematici del partenariato pubblico-privato per le infrastrutture e le trasformazioni urbanistiche*, in *Rivista Trimestrale degli Appalti*, 2011, 2, 381; M. Rutigliano, L. Faccincani, *Project finance nel partenariato pubblico-privato e valutazione del piano economico finanziario*, in *Riv. Dottori comm.*, 2012, 1, 127; C. P. Santacroce, *Osservazioni sul «partenariato pubblico-pubblico», tra elaborazioni ed applicazioni giurisprudenziali del modello e nuove direttive europee in tema di appalti e concessioni*, in *Riv. giur. urb.,* 2014, 17; P. De Luca, *Il partenariato pubblico-pubblico nel diritto comunitario degli appalti pubblici*, in *Dir. U.E.*, 2013, 381.

destinatari della norma finiscono loro stessi per divenire da soggetti meramente passivi a parti in causa attive nel processo di innovazione e di sviluppo della tutela delle infrastrutture digitali. Come precisa la medesima Strategia nazionale di cybersicurezza, l'approccio da adottare in materia è "*whole-of-society*"[86], ossia capace di coinvolgere anche i soggetti solitamente posti fuori dal circuito regolamentare ma che, grazie anche ai sopracitati strumenti di collaborazione orizzontale, finiscono per giocare un ruolo decisivo. Viene ad avere piena attuazione quel principio di rango costituzionale di cui all'art. 118 co. 4 (come modificato dalla l. cost. n. 3/2001), che stabilisce che i pubblici poteri nazionali "*favoriscono l'autonoma iniziativa dei cittadini, singoli e associati, per lo svolgimento di attività di interesse generale*"[87]. Attraverso questa prospettiva si giunge, in definitiva, ad una qualificazione della cybersicurezza come bene pubblico la cui tutela passa per un'azione sinergica e coordinata tra settore pubblico e privato, capace di produrre effetti benefici tanto per l'uno quanto per l'altro.

[86] Si veda quanto detto nella sezione 2, 26 della Strategia Nazionale di Cybersicurezza.
[87] In materia di principio di sussidiarietà e del ruolo dell'iniziativa privata si veda G.U. Rescigno, *Principio di sussidiarietà orizzontale e diritti sociali*, in *Dir. pubbl.*, 2002, 1, 5; L. Grimaldi, *Il principio di sussidiarietà orizzontale tra ordinamento comunitario e ordinamento interno*, Bari, 2006; C. Marzuoli, *Sussidiarietà e libertà,* in *Riv. dir. priv.* , 2005, 5; F. Trimarchi Banfi, *Il principio di concorrenza: proprietà e fondamento,* in *Dir. amm.* , 2013, 15.