«Il diritto dell'economia» issn 1123-3036, anno 72, n. 119 (2-3 2026) pp. 137-161

Articoli e saggi

Le tutele per le imprese all'interno del Perimetro di Sicurezza Nazionale Cibernetica

Paolo Campagna

Sommario: 1. Premessa. – 2. I fondamenti giuridici della limitazione nell'esercizio della libertà di impresa. – 3. La posizione degli operatori economici privati all'interno del Perimetro Nazionale di Sicurezza Cibernetica. – 4. L'applicazione della direttiva NIS 2 sugli operatori economici privati "perimetrati". – 5. Conclusioni.

1. *Premessa*

Per effetto della "quarta rivoluzione"[1] affermatasi nel corso degli ultimi decenni, l'alta tecnologia ha invaso ogni ambito della vita di miliardi di utenti, grazie alla diffusione dei prodotti IOT (*Internet of Things*)[2], che garantiscono l'accessibilità allo spazio cibernetico.

Se, da una parte, il carattere "aperto" acquisito dal *cyberspace*[3] parrebbe rappresentare una significativa occasione per la promozione del benessere sociale, dall'altra legherebbe alla tenuta dello spazio cibernetico la vita quotidiana degli utenti, nonché l'economia e la stessa sicurezza degli Stati[4].

[1] L'attuale periodo storico, contrassegnato dalla diffusione dei computer e dalle tecnologie ICT in generale, è indicato in letteratura come l'ultima di quattro rivoluzioni scientifiche che hanno prodotto un impatto rivoluzionario sulla storia dell'essere umano. Sul punto, L. Floridi, *La quarta rivoluzione*, Milano, 2019, 87 ss.

[2] Ovvero tutti quegli apparecchi dotati di sensori e di *communication capabilities* che rendono possibili sia un "dialogo" persona-macchina, sia tra gli stessi dispositivi. Gli IoT sono in grado di: immagazzinare e comunicare dati, accedere ad informazioni aggregate da parte di altri apparecchi e utilizzare *software* e tecnologie per l'analisi dei dati. Sul punto L. Coppolino, S. D'Antonio, L. Romano, L. Sgaglione, *IoT: una tecnologia "disruptive"*, 274, disponibile su: https://www.mimit.gov.it/images/stories/digitale/Rivista/2016/17_iot_a_disruptive_technology.pdf (ultima consultazione 10/03/2026).

[3] M. Mirti, *Il cyberspace*, Napoli, 2021, 54, che fa riferimento al carattere "aperto" dello spazio cibernetico per indicare la generalizzata accessibilità al *cyberspace* grazie alla diffusione delle tecnologie ICT (*Information and Communication Technologies*), ampia categoria comprensiva degli IoT.

[4] Sul punto, parte della dottrina ha osservato un processo di «militarizzazione» dello spazio cibernetico, divenuto fonte di pericoli per gli stessi Stati. In merito si rinvia a L. Martino, *La quinta dimensione della conflittualità*, in *Politica e Società*, n. 1/2018, 62 ss.

In tal senso, centrale rilievo sembra assumere il fenomeno dei *cyberattack*[5], in considerazione dell'aumento esponenziale del numero di episodi registrati e della crescente portata lesiva dei singoli attacchi[6], in grado di inibire, alterare o addirittura distruggere dati, *hardware*, reti o eventuali servizi e sistemi ad essi connessi[7].

Alla luce di tali elementi, come teorizzato dalla dottrina, la sicurezza cibernetica si porrebbe come una nuova funzione pubblica[8]. In merito, sarebbe errato ritenere che lo Stato sia investito del compito di eliminare alla radice la minaccia cibernetica, posto che i sistemi informatici conserveranno sempre un margine di insicurezza[9]. La sicurezza cibernetica avrebbe dunque carattere composito, risultando comprensiva di almeno tre funzioni interdipendenti[10]: la difesa da minacce attuali o potenziali (attacchi informatici, intrusioni, sabotaggi); la prevenzione, ossia la riduzione del rischio sistemico, attraverso norme, procedure e cultura della sicurezza; la resilienza, intesa come la capacità di resistere, assorbire e ripristinare la funzionalità dei sistemi dopo un incidente.

La funzione di sicurezza cibernetica, dunque, non si esaurirebbe nell'attività di difesa, ma si realizzerebbe attraverso le attività di *governance* del rischio[11], intrinseco al sistema.

Nell'ultimo decennio, il legislatore italiano è intervenuto per disciplinare la materia in esame, mediante una normativa che, pur stimolata in parte dagli impulsi promanati dall'ordinamento europeo, appare caratterizzata da uno spiccato carattere identitario.

In particolare, la disciplina interna parrebbe ricollegare la funzione di *cybersecurity* alla tutela della sicurezza nazionale. Rievocare tale concetto, tradizionalmente indeterminato, potrebbe costituire fonte di criticità, posto che il richiamo

---

[5] Come tale deve intendersi, secondo la definizione fornita dal Glossario Intelligence del SISR, ogni «azione ostile finalizzata a danneggiare la riservatezza, l'integrità e la disponibilità di dati memorizzati o elaborati da sistemi informatici». Sul punto si rinvia alla voce del Glossario online, disponibile su: https://www.sicurezzanazionale.gov.it/comunicazione/glossario/311 (ultima consultazione 10/02/2026).

[6] Da ultimo, allarmanti risultano i dati raccolti dal CLUSIT. Il rapporto di metà anno del 2025, infatti, conferma l'andamento negativo degli ultimi anni sia in termini di aumento degli attacchi, sia in termini di gravità, con un incremento degli attacchi di particolare gravità. Preoccupante risulta anche il dato relativo al nostro Paese, che continua a essere destinatario di un numero sproporzionato di attacchi -oltre il 10,2% degli attacchi informatici globali si sono registrati in Italia- in relazione al peso economico e demografico della Nazione. Il rapporto completo è consultabile su https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_aggiornamento_10-2025_web.pdf (ultima consultazione: 10/02/2026).

[7] N. De Felice, *Strategia di difesa nel cyberspazio quale contributo alla tutela degli interessi nazionali*, in U. Gori, L.S. Germani (a cura di), *Information warfare 2011*, Milano, 2012, 69 ss.

[8] Il riferimento è in particolare a R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in Id. (a cura di) La sicurezza nel cyberspazio, Milano, 2023, 7 ss.; M. Macchia, G. Sferrazzo, *Sicurezza e rischio tecnologico: la funzione di "cybersecurity"*, in *Diritto amministrativo*, n. 1/2025, 109 ss.; nonché il recente lavoro monografico di M. Matassa, La sicurezza cibernetica come funzione pubblica, Milano, 2025.

[9] G. D'Angelo, G. Giacomello, *Cybersicurezza*, Bologna, 2023, 49 ss.

[10] R. Ursi, *La declinazione cibernetica della sicurezza nazionale tra vecchie ambiguità e nuove sfide*, in *Rivista dello Stato digitale*, 2025, 2, 155.

[11] *Ibidem*.

alle esigenze securitarie ha generalmente determinato l'adozione di misure limitative di diritti di particolare gravità[12]. Spesso, infatti, la necessità di assicurare all'ordinamento una efficace risposta alla minaccia in corso ha indotto a tralasciare una necessaria ponderazione tra le esigenze di protezione e il rispetto dei diritti di libertà[13].

Nell'ambito della sicurezza cibernetica, la suddetta problematica potrebbe riproporsi con riferimento all'esercizio della libertà di impresa. Il legislatore nazionale ed europeo, preso atto della posizione strategica ricoperta dal privato nel *cyberspace*, hanno perseguito l'ambizioso obiettivo di procedere secondo un approccio collaborativo con gli operatori economici, spesso tradottosi, tuttavia, nell'imposizione di obblighi stringenti.

Sintomatica potrebbe apparire in tal senso la posizione di alcuni soggetti che, da una parte, in ragione della particolare rilevanza dell'attività esercitata per gli interessi strategici nazionali, sono stati ricompresi all'interno del Perimetro di Sicurezza Nazionale Cibernetica (PSNC, istituito mediante il d.l. n. 105/2019); dall'altra, per quanto non previsto dalla normativa interna, sono stati successivamente assoggettati anche alla disciplina di derivazione europea, sancita dalla recente direttiva (UE) 2022/2555 (direttiva NIS 2).

Appare dunque emergere l'esigenza di individuare le garanzie che possono riconoscersi alle imprese di fronte al pubblico potere, per valutare la proporzionalità degli interventi in materia di sicurezza cibernetica. Per rispondere a tale esigenza, risulta in primo luogo necessario identificare i presupposti che consentono al legislatore nazionale di limitare l'esercizio dell'attività di impresa, per poi soffermarsi sulla valutazione della posizione delle imprese all'interno del PSNC.

2. *I fondamenti giuridici della limitazione nell'esercizio della libertà di impresa*

La libertà di impresa è implicitamente riconosciuta dall'art. 41 della Costituzione, che sancisce la più generale libertà di iniziativa economica privata[14][15].

[12] G. de Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 2019, 4, 70.

[13] Ivi, 71.

[14] Risalente il dibattito circa l'estensione dei concetti di «libertà di impresa» e «libertà di iniziativa economica privata», da tempo superato dalla dottrina e dalla giurisprudenza nel senso dell'impossibilità di ritenere i due sintagmi perfettamente sovrapponibili. La libertà d'impresa costituisce la più importante estrinsecazione della libertà riconosciuta all'art. 41 della Costituzione, ma non esaurisce tale categoria. Sul punto cfr. M. Cecchetti, *Le limitazioni alla libertà di iniziativa economica privata durante l'emergenza*, in *Rivista AIC*, 2020, 4, 60.

[15] La configurazione della libertà di impresa, quale articolazione della libertà di iniziativa economica privata riconosciuta in Costituzione, non appare discutibile sulla base delle ricadute di tale attività sulla generalità dei consociati. Sul punto, è possibile richiamare la ricostruzione di tale concetto da parte di autorevole dottrina:

Com'è noto, in netta soluzione di continuità rispetto allo Statuto albertino, la Carta costituzionale non attribuisce ai diritti economici il valore di attributi indefettibili dell'uomo[16]. I membri dell'Assemblea costituente, pur nella diversità delle loro posizioni politiche, appaiono condividere la convinzione circa il fallimento del sistema liberale e della necessità di controlli di carattere giuridico volti a coordinare le iniziative individuali, generalmente consentite, per impedire che dall'esercizio della libertà di iniziativa economica privata possano discendere pregiudizi per gli interessi della collettività[17].

In questa prospettiva la Costituzione intende realizzare un processo di «funzionalizzazione»[18], che riconoscerebbe la libertà di iniziativa economica privata ma al contempo ne ammetterebbe l'esercizio solo nel rispetto di limiti positivi di carattere sociale (e da ultimo anche ambientale[19]), individuati al comma 2 dello stesso articolo, per mezzo dei quali l'autorità pubblica stabilirebbe le finalità e i modi di uso di un'impresa[20].

Gli interventi nazionali in materia di sicurezza cibernetica sembrerebbero muoversi secondo queste coordinate, alla luce del costante richiamo alla sicurezza nazionale, delineato in alcune fonti come ampia categoria di cui la *cybersecurity* costituisce estrinsecazione; mentre in altre come materia incisa solo in parte dalla sicurezza cibernetica[21].

«perché l'attività imprenditoriale produce ricchezza ed è preordinata alla circolazione di questa con una positiva ricaduta sulla comunità, la Costituzione repubblicana ne indica i caratteri, le finalità e pone ad essa limiti da osservare», V. Buonocore, *Impresa* (Voce), in *Enciclopedia del diritto*, Annali I, Milano, 2007, 765 ss.

[16] Paradigmatica appare in tal senso l'art. 29 dello Statuto albertino, che riconosceva l'inviolabilità di tutte le proprietà, pur ammettendo la possibilità di espropriazione per motivi di interesse pubblico.

[17] In merito appare particolarmente efficace la sintesi realizzata dall' On. A. Moro durante i lavori della prima Sottocommissione della Commissione per la Costituzione, che come emerge dal verbale della seduta del 3 ottobre 1946 definisce «insostenibile la concezione liberale in materia economica, in quanto vi è la necessità di un controllo in funzione dell'ordinamento più completo dell'economia […] anche e soprattutto per raggiungere il maggiore benessere». Nella stessa direzione la posizione dell'On. O. Mastrojanni, che sottolinea come dalla discussione in seduta affiori la preoccupazione di «evitare che la ricchezza, accumulandosi nelle mani di pochi, possa portare a conseguenze funeste anche di carattere politico» esprimendo dunque la necessità di controlli statali, finalizzati ad «evitare abusi e […] regolare il sistema economico nazionale». I verbali dei lavori dell'Assemblea costituente sono consultabili su: *La nascita della Costituzione* (ultima consultazione 15/02/2026).

[18] S. Cassese, *La nuova costituzione economica,* Bari, 2007, 20.

[19] Il riferimento è alla recente modifica della Carta costituzionale per effetto della l. cost. n. 1/2022, che ha introdotto anche la salute e l'ambiente tra i limiti che arginano l'esercizio della libertà di impresa. In merito cfr. M. Benvenuti, *La revisione dell'articolo 41, commi 2 e 3, della Costituzione, i suoi destinatari e i suoi interpreti*, in *Rivista AIC*, 2023, 2, 59 ss.

[20] S. Cassese, *La nuova costituzione economica*, cit., 20.

[21] Nei primi interventi in materia, il legislatore sembra porre la sicurezza nazionale e la sicurezza cibernetica in un rapporto di genere-specie. In tal senso, l'art. 1 del DPCM n. 66/2013 (c.d. decreto Monti), primo intervento normativo in materia di *cybersecurity*, individua le finalità dell'intervento nella definizione dell'architettura volta a tutelare «(la) sicurezza nazionale […] con particolare riferimento alla protezione cibernetica e alla sicurezza informatica…». Gli interventi normativi più recenti, invece, parrebbero non consentire di qualificare la cibersicurezza come categoria perfettamente sussumibile all'interno della sicurezza dello Stato. Tali conclusioni potrebbero trarsi, ad esempio, dal più recente d.l. n. 82/2021 che definisce la *cybersecurity* come «l'insieme

Il richiamo alla sicurezza nazionale determina specifici effetti sui diritti di libertà interessati nell'ambito della sicurezza cibernetica. Per osservare tale fenomeno, risulta preliminarmente necessario fornire una definizione di tale concetto.

Le difficoltà insite nell'attività ricostruttiva e definitoria del sintagma sono comprovate in letteratura, considerando che già durante il secolo scorso la dottrina d'oltreoceano ha fatto riferimento alla sicurezza nazionale ricorrendo all'espressione di «simbolo ambiguo»[22]. Nel corso del tempo non sembrerebbero essere stati registrati significativi progressi, se si considera che anche recentemente la letteratura ha ritenuto la sicurezza dello Stato «un concetto giuridicamente evanescente»[23] tanto da relegarla alla sfera del «pre- meta o extragiuridico»[24].

Fattore concorrente ad incrementare l'inafferrabilità della sicurezza nazionale è, per altro, l'assenza di definizioni normative, nonostante il richiamo da parte degli artt. 117 e 126 della Costituzione. Nel silenzio della legge, i lineamenti del sintagma in esame possono essere tratteggiati a partire da un consolidato indirizzo della Corte costituzionale, in base al quale la sicurezza nazionale attiene alla cura della «*salus rei publicae*»[25] e coincide con l' «interesse dello Stato-comunità alla propria integrità territoriale, alla propria indipendenza e, al limite, alla stessa sua sopravvivenza»[26]; individuato l'oggetto della sicurezza nazionale, la Consulta riconosce il carattere «preminente» di questo «supremo interesse» su ogni altro.

Pur costituendo un valido ausilio, le indicazioni offerte dalle pronunce della Consulta non esauriscono la questione definitoria, posto che tale concetto, soggetto a costante evoluzione nel corso del tempo[27], ha visto una progressiva estensione dei propri confini.

Ciò appare emergere, innanzitutto, dalla l. n. 124/2007, recante disposizioni in materia di Sistema di Informazione per la sicurezza della Repubblica e sul segreto di Stato. Detto intervento, che si inserisce nella recente fase di «normativizzazione»[28] della sicurezza nazionale, restituisce un'accezione più

---

delle attività […] necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici… anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale».

[22] A. Wolfers, *"National Security" as an Ambigous Symbol,* in *Political Science Quarterly*, 1952, 4, 481 ss.

[23] M. Barberis, *Non c'è sicurezza senza libertà*, Bologna, 2017, 89.

[24] *Ibidem.*

[25] Cfr. Corte cost., sentt., nn. 82/1976; 86/1977; 110/1998; 106/2009; 40/2012.

[26] Cfr. Corte cost., sent., n. 86/1977.

[27] Sul punto A.V. Vigneri, *I profili giuridici della sicurezza nazionale. Tra collocazione sistematica e problemi definitori: un'introduzione critica*, in R. Ursi (a cura di), *La sicurezza cibernetica nel cyberspazio*, Milano, 2023, 43 ss., in cui si illustra il processo evolutivo attraversato dalla sicurezza nazionale, originariamente sovrapponibile con il concetto della difesa militare, per poi acquisire un significato più ampio.

[28] A. Monti, *Ordine pubblico, sicurezza nazionale e sicurezza cibernetica: una prospettiva di sistema*, disponibile su: https://www.ictlex.net/ordine-pubblico-sicurezza-nazionale-e-sicurezza-cibernetica-una-prospettiva-di-sistema/ (ultima consultazione: 01/02/2026).

ampia dello stesso concetto[29], individuando i compiti delle istituite AISE e AISI nella «protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia»[30].

Più di recente, il fenomeno di espansione dei confini della sicurezza nazionale pare aver ricevuto nuovo impulso da parte delle minacce che attentano alle democrazie contemporanee[31]. Tra queste si inserisce la minaccia cibernetica, che sembrerebbe aver prodotto un'ulteriore dilatazione dei confini di tale sintagma[32].

È alla luce della progressiva metamorfosi del concetto di sicurezza nazionale che emergerebbe un elemento di criticità insito nell'ordinamento. Nonostante, sul piano teorico, non sembrino esservi ostacoli ad ammettere un giudizio di bilanciamento tra la sicurezza dello Stato e altri interessi costituzionalmente garantiti, nella prassi la giurisprudenza costituzionale ha generalmente ritenuto prevalenti le esigenze securitarie[33].

Se la sicurezza nazionale determina una compressione di diritti di libertà costituzionalmente garantiti, ci si interroga se l'ordinamento debba rassegnarsi ad una progressiva compressione della sfera giuridica dei singoli, parallela al delineato processo di estensione dei confini della sicurezza dello Stato.

In tal senso assume significato l'auspicio di parte della dottrina ad una ridefinizione dei confini della sicurezza nazionale, in modo da impedire che la stessa acquisisca un contenuto talmente ampio e indeterminato da convertire la *salus rei publicae* in una «valvola di sfogo dell'ordinamento in grado di ricomprendere ogni interesse politico […] rilevante»[34]; esito che contrasterebbe evidentemente con i principi della Carta costituzionale e che risulterebbe altresì controproducente sul piano pratico, privando le questioni di sicurezza nazionale della loro indiscutibile specificità[35].

Aderendo a tale visione prospettica, potrebbe essere opportuno isolare un'accezione ristretta del concetto di sicurezza nazionale, intrinsecamente connessa al mantenimento dell'integrità territoriale e dell'assetto istituzionale repubblicano, e che coinciderebbe con la *salus rei publicae* richiamata dalla giurisprudenza costituzionale. Al fianco del "nocciolo duro" della sicurezza nazionale si accosterebbe un'accezione più ampia, inerente alle attività volte al mantenimento della sovranità nazionale attraverso il perseguimento degli interessi strategici

---

[29] T.F. Giupponi, *I rapporti tra sicurezza e difesa. Differenze e profili di convergenza*, in *Diritto costituzionale*, 2022, 1, 43.

[30] Cfr. artt. 6 e 7, l. n. 124/2007.

[31] T.F. Giupponi, *I rapporti tra sicurezza e difesa. Differenze e profili di convergenza,* cit., 32.

[32] F. Violi, *Libertà della rete e Cybersecurity: la questione del segreto di Stato*, in M. Distefano (a cura di) *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017, 67 ss.

[33] T.F. Giupponi, *I rapporti tra sicurezza e difesa. Differenze e profili di convergenza*, cit., 37 ss.

[34] *Ibidem.*

[35] *Ibidem*.

nazionali[36], posti a tutela dell'«indirizzo politico costituzionale, così come assunto dalle forze politiche egemoni in un determinato momento storico non coincidente (quindi) con l'indirizzo politico delle forze di maggioranza»[37].

Dall'accoglimento di siffatta distinzione potrebbe discendere una maggiore incidenza dei diritti di libertà che di volta in volta verrebbero in rilievo nelle fattispecie inerenti alla sicurezza nazionale in senso ampio; mentre per quanto concerne le ipotesi riguardanti la necessità di salvaguardare l'esistenza stessa della Repubblica italiana, le esigenze securitarie avrebbero con ogni probabilità carattere prevalente rispetto ad altri interessi compresenti.

Nell'ambito della *cybersecurity*, chiarire il contenuto e i confini della sicurezza nazionale parrebbe risultare necessario anche per osservare il rapporto che intercorre tra la disciplina interna e gli interventi di carattere europeo, che come accennato in sede introduttiva, hanno rappresentato un impulso fondamentale alle politiche nazionali in materia di sicurezza cibernetica.

Sul piano sovranazionale, il contrasto alle minacce cibernetiche si qualifica come elemento funzionale a garantire il «corretto funzionamento del mercato interno», come emerge sin dai primi documenti strategici[38]. Per assicurare il raggiungimento di simile obiettivo, si è assistito al susseguirsi di numerosi interventi normativi dalla progressiva pervasività.

Il riferimento è in particolare alla direttiva (UE) 2022/2555 (direttiva NIS 2), che mostrerebbe uno spiccato grado di maturazione raggiunto dal legislatore europeo nel contrasto alla minaccia cibernetica e segnerebbe l'inizio di una nuova fase delle politiche europee, il cui obiettivo principale non dovrebbe più individuarsi nel rafforzamento del mercato unico, bensì nell'implementazione della sicurezza stessa[39]. Secondo parte della dottrina le ragioni giustificative di tale fenomeno possono individuarsi nel progressivo avvicinamento dei concetti di «tutela del mercato europeo» e di «sicurezza economica»[40]. In particolare, la sicurezza economica, che sul piano costituzionale si individuerebbe quale precipuo obiettivo statale a garanzia delle fasce deboli della popolazione, si è gradual-

[36] Nel senso di una distinzione tra un'accezione più ristretta ed una più ampia di sicurezza nazionale si rinvia M. Matassa, *La sicurezza cibernetica come funzione pubblica,* Milano, 2025,113 ss., nonché di recente R, Ursi, *La declinazione cibernetica della sicurezza nazionale tra vecchie ambiguità e nuove sfide*, in *Rivista dello Stato digitale*, 2025, 2, 146 ss.

[37] A. Barbera, *Regioni e interesse nazionale,* Milano, 1973, come opportunatamente ricordato da T.F. Giupponi, *I rapporti tra sicurezza e difesa. Differenze e profili di convergenza,* cit., 45.

[38] Il riferimento è in particolare alla «Strategia dell'Unione europea per la cibersicurezza: uno spazio aperto e sicuro» del 2013. Ancorché privo di efficacia cogente, tale documento strategico costituisce il primo atto in materia di *cybersecurity* a livello europeo, costituendo la base per i successivi interventi normativi.

[39] M. Matassa, *La sicurezza cibernetica come funzione pubblica*, cit., 103.

[40] Ivi, 104.

mente inserito tra le finalità perseguite dall'UE, come risulterebbe da un'analisi complessiva delle disposizioni sancite dalla Carta di Nizza[41].

Nella materia in esame, dunque, la sicurezza economica potrebbe individuarsi come il punto di incontro tra gli ambiti di competenza europea e nazionale.

Alla luce di quanto sinora osservato, la sicurezza cibernetica parrebbe qualificabile come una «funzione pubblica multilivello»[42] che può essere descritta ricorrendo all'immagine dei cerchi concentrici[43]: alcuni aspetti della sicurezza cibernetica sono direttamente ricollegati alla protezione dell'esistenza stessa dello Stato e, dunque, rientrando all'interno della sicurezza nazionale, sono di esclusiva competenza statale; all'estremo opposto, si individuano le questioni attinenti alla *cybersecurity* estranee alle logiche della sicurezza nazionale (quale, ad esempio, l'individuazione di standard tecnici comuni) oggetto degli interventi di matrice europea, volti a tutelare l'integrità e il funzionamento del mercato unico.

Tra i due estremi, i cui confini possono essere individuati con certezza, si colloca una «scala di grigi», un'area dai contorni sfumati, data dalla comune volontà di tutelare gli interessi strategici nazionali o la sicurezza economica[44].

3. *La posizione degli operatori economici privati all'interno del Perimetro Nazionale di Sicurezza Cibernetica.*

L'istituzione del PSNC, mediante l'emanazione del d.l. n. 105/2019, parrebbe aver segnato un momento particolarmente significativo nelle recenti politiche in materia di sicurezza cibernetica. Il legislatore avrebbe circoscritto – o per lo meno gettato le basi per circoscrivere successivamente[45] – un segmento dello spazio cibernetico rilevante per la sicurezza nazionale, accordando a determinati soggetti, operanti in settori strategici per lo Stato, particolare protezione[46].

---

[41] M. Clarich, *La sicurezza economica?*, in *Diritto e processo amministrativo*, 2013, 2-3, 345 ss. In questa sede si fa riferimento in particolare all'accezione più forte della sicurezza economica, definita dall'autore come «sicurezza economica come obiettivo».

[42] M. Matassa, *La sicurezza cibernetica come funzione pubblica*, cit., 149.

[43] Ivi, 307.

[44] *Ibidem*.

[45] Come osservato da B. Carotti, *Sicurezza cibernetica e Stato-nazione,* in *Giornale di diritto amministrativo,* 2020, 5, 629 ss., il legislatore ha in realtà realizzato una meta-definizione del PSNC, limitandosi a delineare una normativa essenziale mediante il d.l. n. 105/2019 mentre l'effettiva realizzazione del perimetro è avvenuta attraverso successivi interventi di carattere regolamentare: DPCM n. 131/2020 (DPCM 1); DPR n. 54/2021; DPCM 81/2021 (DPCM 2); DPCM 15 giugno 2021 (DPCM 3) e il DPCM 18 maggio 2022 (DPCM 4).

[46] L. Calandriello, *Il perimetro di sicurezza nazionale cibernetica,* in R. Ursi (a cura di) *La sicurezza nel cyberspazio*, Milano, 2023, 139 ss.

L'inserimento all'interno del PSNC determina il sorgere di obblighi gravosi in capo ai soggetti individuati, che possono essere suddivisi in obblighi volti a prevenire gli attacchi cibernetici e obblighi volti a gestire gli incidenti informatici[47].

La prima categoria[48] si articola ulteriormente in[49]: obblighi di comunicazione[50]; obblighi di adeguamento delle tecnologie e dei processi interni[51]; obblighi di formazione e consapevolezza dei dipendenti; obblighi che incidono sulle procedure di approvvigionamento e fornitura di beni, sistemi e servizi ICT[52].

In merito alla gestione delle crisi informatiche, si fa invece riferimento agli obblighi di notifica degli incidenti. Per altro il DPCM n. 81/2021 prevede termini particolarmente stringenti (un'ora in caso di incidenti più gravi, sei ore per quelli meno gravi[53]), anche tracciando un paragone con altre fonti normative, e che inducono la dottrina a dubitare circa le reali possibilità di adempimento da parte delle imprese[54].

La soggezione agli obblighi imposti dalla disciplina interna discende direttamente dall'inserimento dell'operatore economico privato all'interno del perimetro.

In estrema sintesi, spetta in prima battuta alle «amministrazioni CISR»[55] predisporre, ognuna per il proprio settore, una lista di soggetti potenzialmente idonei ad essere ricompresi all'interno del Perimetro; tale elenco di nomi è sottoposto al CISR tecnico e successivamente al CISR.

Su proposta di quest'ultimo organo, l'elenco dei soggetti effettivamente ricompresi all'interno del PSNC è adottato (e periodicamente aggiornato), attraverso un atto del Presidente del Consiglio dei ministri[56]. Si tratta di un atto

---

[47] E. Buoso, *Ritorno al futuro: il perimetro di sicurezza nazionale cibernetica,* in *Teoria e critica della regolazione sociale*, 2025, 1, 33 ss.

[48] Cfr. art. 1, co. 3, lett. b, d.l. n. 105/2019.

[49] E. Buoso, *Ritorno al futuro: il perimetro di sicurezza nazionale cibernetica*, cit., 40.

[50] Ai sensi dell'art. 1, co. 2, lett. b, d.l. n. 105/2019, almeno una volta l'anno i soggetti perimetrati devono trasmettere all'Agenzia Nazionale per la cybersicurezza, un elenco delle reti, dei sistemi informativi e dei servizi informatici che sia strumentale all'esercizio di una funzione essenziale dello Stato o assicuri un servizio essenziale. La comunicazione risulta un presupposto fondamentale per consentire all'Agenzia di assolvere i propri compiti istituzionali in materia di prevenzione, preparazione e gestione delle crisi cibernetiche.

[51] Cfr. art. 1, co. 3, d.l. n. 105/2019.

[52] Cfr. art. 1, co. 6, d.l. n. 105/2019, che prevede che i soggetti perimetrati comunichino al Centro di valutazione e certificazione nazionale (CVCN) la volontà di procedere all'affidamento di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sistemi informativi e per l'espletamento dei servizi informatici che ne hanno determinato l'inclusione nel PSNC. Entro il termine di 45 giorni, prorogabile di altri 15 in casi di estrema complessità, il CVCN può effettuare test sull'affidabilità del bene o del servizio ICT, il cui superamento è evidentemente condizionato il possibile impiego da parte del soggetto perimetrato. In ogni caso il CVCN deve pronunciarsi sull'affidabilità della nuova componentistica ICT entro il termine di 60 giorni, altrimenti il soggetto potrà proseguire con la procedura di affidamento

[53] Cfr. art. 3, co. 4, DPCM n. 81/2021.

[54] S. Poletti, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, in *Medialaws*, 2023, 2, 398 ss.

[55] Cfr. art. 3, co. 2, DPCM n. 131/2020.

[56] Cfr. art. 5, co. 2, DPCM n. 131/2020.

amministrativo di estremo rilievo, che viene trasmesso al Comitato parlamentare per la sicurezza della Repubblica (Copasir), non è soggetto a pubblicazione ed è sottratto al diritto di accesso[57].

Preme sottolineare che sino all'adozione dell'atto i soggetti individuati non sono a conoscenza dell'inserimento all'interno del PSNC. Essi sono informati entro 30 giorni dall'adozione dell'elenco da parte del Presidente del Consiglio dei ministri, tramite una comunicazione personale inoltrata dal DIS[58].

Appare corretto qualificare tale determinazione del Presidente del Consiglio dei ministri come un atto di alta amministrazione, ovvero quegli atti amministrativi che svolgono una fondamentale funzione di raccordo tra gli indirizzi espressi a livello politico ed i provvedimenti di amministrazione attiva[59].

Tale conclusione pare confermata dalla possibilità di escludere che l'atto di inserimento di un'impresa nel PSNC possa qualificarsi come un atto politico, concetto tradizionalmente contrapposto a quello di atto di alta amministrazione, pur in assenza di una sicura linea di demarcazione tra le due categorie[60].

Com'è noto, il tema assume notevole rilevanza pratica, in virtù della tradizionale sottrazione al sindacato giurisdizionale dell'atto politico, oggi sancita dall'art. 7 del c.p.a.

La distinzione tra atto politico e atto di alta amministrazione, è stato osservato, determina specifiche ricadute su due cardini del sistema democratico: il principio di giustiziabilità dell'azione amministrativa e il principio di separazione dei poteri[61].

Il riconoscimento del principio di giustiziabilità dell'azione amministrativa all'interno del nostro ordinamento appare innegabile con l'entrata in vigore della Costituzione, ed emerge segnatamente dal combinato disposto degli artt. 24 e 113. Lo stesso trova altresì riconoscimento nell'ordinamento sovranazionale, all'art. 6 della CEDU.

L'introduzione di detto principio ha portata "rivoluzionaria", sancendo come il potere pubblico non possa godere di spazi di immunità[62].

---

[57] B. Carotti, *Sicurezza cibernetica e Stato-nazione*, cit., 635.

[58] Cfr. art. 5, co. 3, DPCM n. 131/2020.

[59] G. Crepaldi, *La motivazione degli atti di alta amministrazione*, nota a Cons. St., sez. IV, 10 novembre 2003 n. 7137 e Cons. St., sez. IV, 10 novembre 2003 n. 7189, in *Foro amministrativo: Consiglio di Stato,* 2003, 12, 3688 ss.

[60] G. Pepe. *Il principio di effettività della tutela giurisdizionale tra atti politici, atti di alta amministrazione e leggi- provvedimento*, in *federalismi.it*, 2017, 22, 2 ss.

[61] G. Mancini Palomi, *La sindacabilità dell'atto politico e i rapporti con gli atti di alta amministrazione*, in P. Cerbo, G. D'Angelo, S. Spuntarelli (a cura di), *Amministrare e giudicare. Trasformazioni ordinamentali*, Napoli, 2022, 358.

[62] A. Rauti, G. Tropea, *Il ritorno dell'atto politico nell'età del dialogo fra le corti e della geopolitica*, in *Amministrativamente*, 2025.

Data l'affermazione del principio di giustiziabilità, molti in letteratura hanno ritenuto incompatibile la permanenza della categoria dell'atto politico, ma in realtà la stessa parrebbe giustificata.

L'atto politico, lungi da essere un "relitto ottocentesco", risulterebbe rispondere alla necessità dell'ordinamento di riconoscere l'esistenza di determinate forme di esercizio di potere non riconducibili al perseguimento dell'interesse pubblico, ma mosse dal perseguimento di finalità istituzionali superiori[63], che se rese oggetto di sindacato giurisdizionale determinerebbero l'intrusione del giudice nell'ambito degli altri poteri dello Stato.

La sottrazione al sindacato giurisdizionale, per altro, non si porrebbe in contraddizione con il principio di giustiziabilità, in quanto, come chiarito dalla Corte costituzionale, all'interno dell'ordinamento sono previste molteplici forme di controllo[64], con la conclusione che la qualificazione di un atto come "atto politico" non determinerebbe il ritorno dell'impunità del potere pubblico, ma lo sottoporrebbe ad una forma di controllo diversa, di carattere politico.

Fermo quanto osservato sin qui, non vi è dubbio che, in forza del dettato costituzionale, l'atto politico costituisce un'eccezionale ipotesi di sottrazione di atti al sindacato giurisdizionale, e la sua sussistenza dev'essere accertata all'esito di un meticoloso accertamento[65].

In tal senso, il soggetto istituzionale deputato a stabilire in concreto il delicato punto di equilibrio tra il principio di separazione dei poteri e il principio di giustiziabilità dell'azione amministrativa si individuerebbe nel giudice amministrativo[66].

Sulla base di tale assunto, rispetto all'annosa questione definitoria relativa all'atto politico[67], parrebbe opportuno valorizzare il contributo fornito dal formante giurisprudenziale.

Come osservato dalla dottrina, tra le molteplici ricostruzioni della categoria in esame[68], la tesi nettamente prevalente individua l'atto politico sulla base di due elementi: il primo, di carattere soggettivo, che coincide con l'emanazione

---

[63] V. Giomi, *L'atto politico nella prospettiva del giudice amministrativo: riflessioni su vecchi limiti e auspici di nuove aperture al sindacato sul pubblico potere*, in *Diritto processuale amministrativo*, 2022, 1, 49.

[64] Corte cost., sent. n. 103/1993, come opportunatamente ricordato da A. Rauti, G. Tropea, *Il ritorno dell'atto politico nell'epoca del dialogo tra le corti*, cit.

[65] G. Mancini Palomi, *La sindacabilità dell'atto politico e i rapporti con gli atti di alta amministrazione*, cit., 365.

[66] V. Giomi, *L'atto politico nella prospettiva del giudice amministrativo: riflessioni su vecchi limiti e auspici di nuove aperture al sindacato sul pubblico potere*, cit., 23.

[67] Circa l'impossibilità di elaborare una definizione unica ed immutabile di atto politico si veda G. Tropea, *Genealogia, comparazione e decostruzione di un problema ancora aperto: l'atto politico*, in *Diritto amministrativo*, 2012, 3, 329 ss.

[68] Tra gli sforzi compiuti in letteratura volti a fornire una definizione esaustiva della categoria in esame, può essere ricordata quella elaborata in epoca risalente da dottrina autorevole quale G.B. Garrone, *Atto politico (Voce)*, in Digesto (discipline pubblicistiche), vol. I, Torino, 1987, che ha fatto riferimento all'atto politico come: «la manifestazione tipica della funzione politica e di governo: atto attraverso cui si estrinsecano l›attività

dell'atto da parte dell'autorità di governo; il secondo, di carattere oggettivo, sussiste qualora l'atto adottato sia espressione della funzione di indirizzo politico, ovvero delle scelte in materia di costituzione e salvaguardia dei pubblici poteri[69].

L'analisi della giurisprudenza più recente parrebbe tuttavia ritenere insufficiente la definizione ora fornita, individuando l'atto politico sulla base di alcuni elementi che non sostituirebbero, ma integrerebbero, quelli tradizionalmente individuati dalla dottrina.

In particolare, tale ricostruzione tende a escludere la sussistenza di un atto politico in presenza di una norma che disciplini l'esercizio del potere, ovvero quando l'atto sia idoneo ad incidere su situazioni giuridiche soggettive[70].

Per quanto interessa maggiormente in questa sede, sulla base di quest'ultima ricostruzione si individuerebbero alcuni elementi attraverso i quali escludere che l'atto di inserimento dell'impresa all'interno del PSNC possa qualificarsi come atto politico, ricadendo invece nella diversa categoria dell'atto di alta amministrazione.

Preliminarmente occorre osservare che già il dettato normativo sembrerebbe deporre in favore della tesi prospettata, considerando che lo stesso DPCM n. 131/2020, all'art. 5, qualifica l'individuazione dell'impresa come soggetto perimetro quale «atto amministrativo», categoria generale che ricomprende, per l'appunto, anche gli atti di alta amministrazione[71].

A ciò si aggiunga che l'esercizio del potere determina la limitazione di una libertà costituzionalmente garantita quale la libertà di impresa. Infine, le disposizioni tese a procedimentalizzare l'inserimento dell'operatore economico all'interno del PSNC potrebbero qualificarsi come norma tesa a disciplinare l'esercizio del potere.

A questo punto della riflessione, è utile ricordare quali siano gli elementi caratterizzanti l'atto di alta amministrazione, ovvero l'imputabilità all'autorità politica e l'ampissima discrezionalità riconosciuta all'autore dell'atto.

Soprattutto quest'ultimo elemento incide sulla struttura dell'atto stesso, in particolar modo sull'obbligo di motivazione. Sul punto, tuttavia, si registrano orientamenti contrastanti in giurisprudenza: secondo una prima impostazione, le peculiari caratteristiche di tale atto giustificherebbero un obbligo di motivazione attenuato[72]; secondo altro indirizzo, invece, trattandosi pur sempre di un atto

---

di direzione suprema della cosa pubblica (›indirizzo politico) e ›attività di coordinamento e controllo delle singole manifestazioni in cui la direzione stessa si estrinseca».

[69] C. Cudia, *Considerazioni sull'atto politico*, in *Diritto amministrativo*, 2021, 623.

[70] Ivi, 624.

[71] G. Pepe, *Il principio di effettività della tutela giurisdizionale tra atti politici, atti di alta amministrazione e leggi- provvedimento*, in *federalismi.it*, 2017, 22, 13.

[72] *Ex multis* Cons. Stato, sez. IV, sent. n. 120/1999; Cons. Stato, sez. IV, sent. n. 173/1999.

amministrativo, è necessaria un'adeguata motivazione[73], ancorché, in concreto, tale onere possa atteggiarsi in maniera differente a seconda del tipo di scelta effettuata[74].

Con riferimento all'atto di inclusione, appare necessario che l'impresa sia in grado di comprendere le ragioni che hanno determinato l'inserimento all'interno del PSNC, anche nel rispetto della clausola generale di buona fede, che trova applicazione nei rapporti tra il settore pubblico e il settore privato[75], e che assume in tale materia particolare rilievo.

La collaborazione del settore privato è infatti necessaria per il raggiungimento di un livello di sicurezza adeguato rispetto alle minacce cibernetiche[76].

Non potendo rilevare la conformazione dell'atto di inclusione nel PSNC a causa della (necessaria) segretezza dello stesso, tuttavia, si ha ragione di temere che alla luce della necessità di tutelare la sicurezza nazionale la motivazione di tale provvedimento rischi di assumere contorni assai generici, limitandosi ad esempio, all'indicazione della funzione o del servizio essenziale offerto dall'operatore, insindacabile salvo macroscopici travisamenti[77].

La necessità di una motivazione idonea risulta fondamentale anche per il rispetto del principio di effettività della tutela giurisdizionale, riconosciuto, come anticipato, sia all'interno della Carta costituzionale, sia all'interno delle principali fonti internazionali in materia di tutela di diritti[78].

Bisogna infatti considerare che l'elevata discrezionalità propria degli atti di alta amministrazione circoscrive il sindacato giurisdizionale alla irragionevolezza o alla illogicità dell'atto stesso[79]; ove l'atto di inclusione all'interno del PSNC adducesse generiche ragioni di salvaguardia della sicurezza nazionale, non sarebbe possibile l'espletamento del sindacato giurisdizionale, neppure secondo tale forma "attenuata".

L'effettiva consistenza della tutela giurisdizionale per le imprese in tale settore, già limitata a causa degli elementi ora evidenziati, rischia per altro di assottigliarsi ulteriormente, considerando che nei settori della difesa e della sicurezza si

---

[73] *Ex multis* Cons. Stato, sez. IV, sent. n. 1139/1998; Cons. Stato, sez. IV, sent. n. 1139/1998; Cons. Stato, sez. IV, sent. n. 629/1997.

[74] G. Crepaldi, *La motivazione degli atti di alta amministrazione*, nota a Cons. St. sez. IV, 10 novembre 2003 n. 7137 e Cons. St, sez. IV, 10 novembre 2003 n. 7189, cit., 3692.

[75] A. Mandara, *La buona fede come parametro di validità del provvedimento amministrativo*, in *Giornale di diritto amministrativo,* 2024, 4, 527 ss.

[76] L. Previti, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *federalismi.it*, 2022, 25, 65 ss.

[77] E. Buoso, *Ritorno al futuro: il perimetro di sicurezza nazionale cibernetica*, cit., 43.

[78] G. Pepe, *Il principio di effettività della tutela giurisdizionale tra atti politici, attività di alta amministrazione e leggi- provvedimento,* cit., 1.

[79] G. Crepaldi, *La motivazione degli atti di alta amministrazione*, nota a Cons. St. sez. IV, 10 novembre 2003 n. 7137 e Cons. St, sez. IV, 10 novembre 2003 n. 7189, cit., 3692.

registra un atteggiamento di *self-restraint* che induce a riconoscere una tendenziale prevalenza degli interessi pubblici rispetto ai diritti e alle libertà dei cittadini[80].

Una volta riflettuto sulle (esigue) garanzie giurisdizionali poste a tutela dell'imprese rispetto all'inserimento all'interno del PSNC, è necessario soffermarsi sulle tutele procedimentali che possono essere riconosciute agli operatori privati.

Come visto in precedenza, l'inserimento all'interno del PSNC è una decisione a cui si giunge attraverso un sistema preordinato di fatti e atti che può essere descritta come un procedimento amministrativo[81].

Risulta invece più complesso stabilire l'eventuale applicabilità delle disposizioni sul procedimento amministrativo previste dalla l. n. 241/1990.

In particolare, la questione fondamentale verte circa la compatibilità delle garanzie previste dalla l. n. 241/1990 con il sistema delineato dal decreto perimetro, volto alla tutela della sicurezza nazionale.

Sul punto parte della dottrina ha osservato come la terminologia utilizzata dal legislatore (che ricorre al vocabolo «procedura» e non all'espressione procedimento) sarebbe volta a marcare la distanza tra la l. n. 241/1990 e la disciplina del PSNC[82].

Ci si chiede se tale passaggio sia tuttavia sufficiente per escludere l'applicazione di quella che viene definita «fonte modello» del procedimento amministrativo[83].

Secondo il parere di chi scrive, l'applicazione della disciplina della l. n. 241/1990 appare materialmente incompatibile con i caratteri peculiari della disciplina posta dal d.l. n. 105/2019.

La necessità di tutelare la sicurezza nazionale rende assai difficile sostenere, ad esempio, l'applicazione della disciplina in merito alla comunicazione di avvio del procedimento, posto che le esigenze securitarie sottese al procedimento di cui art. 5 del DPCM n. 131/2020 potrebbero consentire agevolmente il richiamo alle «ragioni di particolare celerità» indicate dall'art. 7 della l. n. 241/1990 come elemento di esclusione della disciplina in materia di comunicazione di avvio.

A ciò si aggiunge l'esplicita disapplicazione dalla disciplina dell'accesso agli atti, che rappresenta un elemento ostativo a qualsiasi forma di contraddittorio all'interno di tale procedimento[84].

---

[80] R. Ursi, *Sicurezza e difesa nel sindacato del giudice amministrativo*, in *PA Persona e Amministrazione*, vol. 13, 2024, 2, 477 ss.

[81] R. Ursi, *Diritto amministrativo generale,* Milano, 2024.

[82] E. Buoso, *Ritorno al futuro: il perimetro di sicurezza nazionale cibernetica*, cit., 41.

[83] M. Timo, *Considerazioni sull'ambito di applicazione della legge 241/1990, anche alla luce della "riforma Madia"*, in *Amministrazione In Cammino*, disponibile su: https://unige.iris.cineca.it/retrieve/e268c4c8-800d-a6b7-e053-3a05fe0adea1/Considerazioni%20sull%e2%80%99ambito%20di%20applicazione.pdf (ultima consultazione: 29/12/2025).

[84] Cfr. art. 1, co. 2, d.l. n. 105/2019.

Le esigenze securitarie sottese al decreto perimetro, dunque, appaiono aver indotto il legislatore a comprimere il più possibile le garanzie procedurali e giurisdizionali riconosciute alle imprese nel momento dell'inserimento all'interno del PSNC[85].

Appare invece possibile riconoscere l'applicabilità delle disposizioni relative alla l. n. 241/1990 con riferimento ad alcuni subprocedimenti di carattere tecnico, come la procedura di certificazione disciplinata dal DPR n. 54/2021[86].

Tale assunto sembra confermato dal dato positivo. Si pensi all'ipotesi, trattata in precedenza, della procedura volta all'utilizzo di un nuovo componente ICT previa approvazione del CVCN, che consente all'impresa di proseguire nella procedura di affidamento ove fosse inutilmente spirato il termine di 60 giorni.

Si tratta di una disposizione che appare riconducibile all'istituto del silenzio-assenso, disciplinato dall'art. 20 della l. n. 241/1990[87].

La disposizione è stata peraltro criticata e indicata come un possibile elemento di inefficienza rispetto alle esigenze di effettività proprie della disciplina del PSNC, dovendosi preferire l'applicazione della disciplina del silenzio diniego[88].

A costo di anticipare parte delle conclusioni in questa sede, tale elemento risulta sintomatico di alcune criticità legate al d.l. n. 105/2019. Anche alla luce delle osservazioni in merito alla terminologia utilizzata per far riferimento al momento di inclusione dell'impresa all'interno del PSNC, secondo il parere di chi scrive, in sede di redazione del decreto il legislatore ha omesso di confrontarsi con le necessarie garanzie da riconoscere al cittadino.

Le tutele che possono essere accordate agli operatori economici si riespandono in sede di esercizio dei poteri di vigilanza e di carattere sanzionatorio da parte dell'ACN, grazie al richiamo alla l. n. 689/1981 da parte dell'art. 1 co. 13 del d.l. n. 105/2019.

A seguito dell'applicazione di una delle sanzioni amministrative di carattere pecuniario, l'impresa gode di una tutela giurisdizionale piena, garantita dal ricorso dinanzi al giudice amministrativo.

Bisogna infatti rammentare in questa sede che la tradizionale distinzione, propria dell'ordinamento giuridico italiano, tra sanzione penale e sanzione amministrativa, è stata disconosciuto dalla Corte EDU.

Secondo la Corte di Strasburgo, la nozione di "pena" deve essere individuata sulla base di criteri di carattere sostanziale, (differentemente da quanto avviene

---

[85] M. Matassa, *La sicurezza cibernetica come funzione pubblica,* cit., 291.
[86] *Ibidem*.
[87] *Ibidem*.
[88] Ivi, 271.

sul piano interno), affinché le tutele previste dall'art. 7 della Convenzione sul piano interno siano effettive[89].

Già nel 1976, la Corte EDU ha elaborato tre criteri alternativi, che consentono di individuare una pena in senso sostanziale: la qualificazione giuridica della misura in causa nel diritto nazionale; la natura stessa di quest'ultima; la natura e il grado di severità della sanzione[90].

In sostanza, secondo la giurisprudenza della Corte, sono pene tutte le misure che, rivolte ad una generalità di destinatari, risultino caratterizzate da un contenuto sostanzialmente punitivo e da una dimensione intrinsecamente afflittiva[91], indipendentemente dalla scelta del legislatore nazionale di attribuire la qualifica di sanzione "amministrativa".

Gli effetti della giurisprudenza sul piano interno sono evidenti, in quanto, come accennato, la tradizionale distinzione tra sanzione penale e sanzione amministrativa perde significato, risultando preferibile distinguere tra mere sanzioni amministrative e sanzioni amministrative punitive[92], rientrando all'interno di tale categoria «tutte le sanzioni di carattere punitivo-afflittivo»[93], le quali «devono essere soggette alla medesima disciplina delle sanzioni penali in senso stretto»[94].

Da quanto sinora osservato dalla dottrina, discende, da una parte la necessità che l'accertamento della violazione debba presentare una fisionomia analoga a quella riferita ad un reato in senso stretto; dall'altra l'esigenza di un sindacato pieno e profondo da parte del giudice amministrativo, corrispondente a quello tipico del processo penale e secondo gli standard del diritto europeo[95].

Tali sono dunque le garanzie che devono essere riconosciute alle imprese in relazione all'accertamento delle violazioni e all'applicazione delle sanzioni previste dall'art. 1 co. 9 del d.l. n. 105/2019, evidentemente sussumibili all'interno della categoria delle sanzioni di carattere punitivo-afflittivo.

In sintesi, il sistema delineato dal d.l. n. 105/2019 comprime le garanzie individuali nella fase procedimentale, che si riespandono solo in un momento successivo, dinanzi al giudice amministrativo.

Sorge l'interrogativo se un sistema così strutturato offra al privato tutele adeguate di fronte al pubblico potere.

---

[89] F.G. Scoca, *Il punto sulla nozione e sulla disciplina delle sanzioni amministrative,* in *Diritto Amministrativo*, 2025, 1, 3 ss.

[90] Corte EDU, sent. n. 22/1976.

[91] F.G. Scoca, *Il punto sulla nozione e sulla disciplina delle sanzioni amministrative*, cit., 27.

[92] Ivi, 28.

[93] Corte cost., sent., n. 276/2017, per come opportunatamente ricordato da F.G. Scoca, *Il punto sulla nozione e sulla disciplina delle sanzioni amministrative,* cit., 28.

[94] *Ibidem.*

[95] M. Lipari, *Il sindacato pieno del giudice amministrativo sulle sanzioni secondo i principi della CEDU e del diritto UE. Il recepimento della direttiva n. 2014/104/EU sul private enforcement (decreto legislativo n. 3/2017): le valutazioni tecniche opinabili riservate all'AGCM,* in *federalismi.it*, 2018, 8, 2 ss.

Sul punto, la giurisprudenza della Corte EDU ha disegnato un rapporto di alternatività tra il procedimento amministrativo e il processo, come emerge dalla sentenza Grande Stevens[96].

In tale pronuncia la Corte ha ravvisato una violazione dell'art. 6 CEDU (giusto processo), considerando che il procedimento sanzionatorio si era celebrato dinanzi ad un organo non imparziale, in assenza di una regolare udienza pubblica e privo di un regolare contraddittorio. Tuttavia, la Corte ha altresì precisato che, nonostante il procedimento dinanzi all'autorità amministrativa (nel caso di specie la CONSOB) fosse privo dei requisiti di equità ed imparzialità oggettiva richiesti dall'art. 6, il privato cittadino ha «beneficiato del successivo controllo da parte di un organo indipendente e imparziale, dotato di piena giurisdizione».

In sintesi, la Corte EDU valuterebbe il rispetto delle garanzie fondamentali riconosciute al cittadino da parte dell'ordinamento attraverso un esame complessivo delle tutele offerte nel procedimento amministrativo e nel processo dinanzi al giudice.

Il punto appare esplicitato dalla recente giurisprudenza della Corte di cassazione, che dal diritto convenzionale ricava il principio secondo cui «allo Stato è lasciata la libertà di scegliere se assicurare tutte le garanzie del giusto processo già nella fase amministrativa, ovvero sottoponendo il provvedimento sanzionatorio al sindacato giurisdizionale pieno»[97].

A fronte della prospettiva accolta dalla giurisprudenza, parte della dottrina ha tuttavia mostrato alcune perplessità. Secondo una corrente di pensiero, l'intervento del sindacato giurisdizionale rischia di risultare tardivo e incapace di compensare l'eventuale pregiudizio subito dal privato nei suoi interessi[98].

In tal senso, potrebbe rivelarsi paradigmatica proprio la posizione dell'impresa inclusa all'interno del PSNC. Alla luce dell'incidenza degli obblighi imposti dal d.l. n. 105/2019, ci si interroga se il sistema adottato non determini un'eccessiva compressione delle garanzie riconosciute al privato dinanzi al pubblico potere. Se così fosse, il rischio sarebbe quello di compromettere l'esistenza della singola impresa, e più in generale del tessuto economico nazionale, per assecondare esigenze securitarie.

---

[96] Corte EDU, sent., 4 marzo 2014, Grande Stevens c. Italia.

[97] Cass. civ., sez. II, sent., n. 9906/2019, come opportunamente ricordato da N. Vettori, *Le garanzie individuali nei confronti del potere sanzionatorio di CONSOB nella "confusione" tra vigilanza e sanzione,* in *Rivista trimestrale di diritto dell'economia*, n. 2020, 2, supplemento, 185 ss.

[98] P. Mezzanotte, *Giusto procedimento e tutela dei diritti. Riflessioni a margine della giurisprudenza CEDU in rapporto alle tradizioni costituzionali nazionali*, in *Rivista AIC*, 2023, 3, 5 ss.

4. *L'applicazione della direttiva NIS 2 sugli operatori economici privati "perimetrati"*

Come ricordato, la direttiva NIS 2 parrebbe aver segnato un punto di svolta nelle politiche comunitarie in materia in materia di *cybersecurity* abrogando sostanzialmente la precedente direttiva UE 2016/1148 o NIS 1, ritenuta generalmente inefficace[99] anche a causa della mancata inclusione di settori rilevanti nel proprio perimetro applicativo[100].

Per mezzo della direttiva NIS 2 si assiste dunque ad un ampliamento dei settori interessati e dei soggetti coinvolti[101], nonché ad una intensificazione degli obblighi imposti[102], ancorché l'esatta definizione di quest'ultimi sia rimessa alle Autorità nazionali dei singoli Stati membri[103].

Dalla prospettiva interna, il tentativo di innalzare ulteriormente il livello di sicurezza interna all'Unione, pur risultando lodevole, sembrerebbe determinare il rischio di una duplicazione dei doveri e delle responsabilità in capo agli operatori economici privati ricompresi nell'ambito del PSNC.

Per scongiurare tale scenario, il legislatore nazionale ha previsto specifici meccanismi di raccordo tra la disciplina di matrice europea e il d.l. n. 105/2019, attraverso una "clausola di equivalenza", prevista dall'art. 33 del d.lgs. n. 138/2024, atto di recepimento interno della direttiva.

Detta disposizione parrebbe infatti escludere i soggetti tenuti al rispetto delle misure imposte dal decreto perimetro dall'applicazione delle disposizioni sancite dalla direttiva NIS 2, considerando «almeno equivalenti» gli obblighi interni.

Per espressa previsione dello stesso art. 33 del d.lgs. n. 138/2024, residuerebbe tuttavia uno spazio di applicazione della normativa di carattere europeo

---

[99] E. Kaiser, *The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations,* in *Medialaws*, 2023, 1, 343 ss.

[100] Particolarmente critica la mancata inclusione del settore spaziale o quello delle pubbliche amministrazioni, sul punto si rinvia a M. Matassa, *La regolazione della cybersecurity in Italia,* in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano, 2023, 21 ss.

[101] C. Giustozzi, *Direttiva NIS 2: genesi, attuazione, impatti,* in *Rivista elettronica di Diritto, Economia, Management*, 88.

[102] Per l'impatto prodotto sull'organizzazione societaria deve segnalarsi quanto stabilito dall'art. 20 della direttiva 2022/2555 e dall'art. 23 del d.lgs. n. 138/2024, che appaiono tesi a realizzare un'operazione di "responsabilizzazione" degli organi di *governance* dei soggetti obbligati. Gli organi amministrativi e gestori sono ora tenuti ad approvare le modalità di implementazione delle misure di gestione dei rischi e a sovrintendere sul rispetto degli obblighi derivanti dal decreto, imputando loro la responsabilità in caso di violazioni. Per conformarsi a tali disposizioni è necessario che gli organi amministrativi e direttivi siano dotati di specifiche competenze tecniche, che saranno loro assicurate da attività di formazione continua, anch'esse obbligatorie, per effetto dello stesso art. 23. Secondo alcuni autori, la disciplina ora richiamata mostra una presa di consapevolezza del legislatore sul carattere strategico e non meramente tecnico della *cybersecurity,* che deve essere rimessa alla responsabilità dell'Alta Direzione. Sul punto C. Giustozzi, *Direttiva NIS 2: genesi, attuazione, impatti,* cit., 92.

[103] Cfr. art. 10, d.lgs. n. 138/2024.

per quanto concerne le reti, i sistemi informativi e i servizi informatici diversi da quelli impiegati nell'esercizio di una funzione o nell'erogazione di un servizio ritenuto essenziale per lo Stato, e in forza del quale si è scelto di ricomprendere quel soggetto all'interno del PSNC[104].

In base al dettato normativo, è possibile che un operatore economico privato ricompreso all'interno del PSNC sia, al contempo, soggetto agli obblighi derivanti dalla direttiva NIS 2.

Risulta dunque necessario osservare tali disposizioni, ed in particolare, soffermarsi sul rapporto che intercorre tra gli operatori economici privati e l'ACN, posto il ruolo di assoluta centralità attribuito all'Agenzia.

Sotto un primo profilo, come in parte già accennato, il legislatore europeo si è limitato a delineare la struttura fondamentale della disciplina relativa alle misure di gestione del rischio imposte dalla direttiva NIS 2, affidando la loro definizione agli Stati membri, nel rispetto dei canoni di adeguatezza e proporzionalità[105].

Così facendo, il legislatore europeo avrebbe inteso adottare un approccio di tipo «*risk-based*»[106] consentendo un adattamento delle misure imposte alle specificità di ciascun settore.

In merito agli operatori economici che rientrano nella giurisdizione italiana[107], è all'ACN che spetta il compito di definire il contenuto degli obblighi da rispettare, in qualità di Autorità nazionale NIS 2[108].

In virtù della stessa qualifica, l'ACN è altresì tenuta a vigilare sul rispetto della direttiva e sul relativo decreto di attuazione, attraverso l'esercizio di poteri di vigilanza e sanzionatori.

Con riferimento a quest'ultime attribuzioni è stato tuttavia osservato come il sistema attuale appaia concepire l'ACN non solo come un organo sanzionatorio, ma anche (o soprattutto) dedito alla *compliance*[109], alla luce dell'ampio novero di misure volte a conformare l'attività delle imprese in relazione alle misure di gestione dei rischi cibernetici[110], configurando l'applicazione di sanzioni come uno strumento di carattere residuale.

Il sistema, inoltre, sembra prevedere una serie di garanzie procedimentali volte a tutelare gli operatori economici dinanzi al potere dell'Autorità nazionale NIS 2. Tra queste, appaiono particolarmente rilevanti: un onere di motivazione rafforzata volta ad assicurare il contraddittorio tra le parti e la sindacabilità in

[104] Cfr. art. 33, co.1, lett. b, d.lgs. n. 138/2024 e art. 1, co. 2, d.l. n. 105/2019.
[105] Cfr. art. 21, direttiva (UE) 2022/2555.
[106] M. Matassa, *La sicurezza cibernetica come funzione pubblica*, cit., 223.
[107] Cfr. art. 26, direttiva (UE) 2022/2555 e art. 5, d.lgs. n. 138/2024.
[108] Cfr. art. 10, d.lgs. n. 138/2024.
[109] M. Matassa, *La sicurezza cibernetica come funzione pubblica*, cit., 242 e ss.
[110] Cfr. art. 35, d.lgs. n. 138/2024.

sede giurisdizionale delle decisioni dell'Agenzia[111]; l'obbligo dell'ACN, in materia di «diffide» e «ordini vincolanti», di comunicare le proprie conclusioni preliminari, garantendo al privato un termine di almeno 15 giorni per presentare le proprie osservazioni[112].

La tenuta dell'impianto adottato dalla direttiva NIS 2 (e dall'atto di recepimento interno) deve essere analizzata anche sotto il profilo del sistema sanzionatorio. In tal senso, le disposizioni previste dal d.lgs. n. 138/2024 parrebbero mostrare alcune criticità.

Preliminarmente, occorre segnalare che anche l'impianto sanzionatorio di matrice europea sembrerebbe assumere un carattere sostanzialmente punitivo, in virtù dei già citati criteri elaborati dalla giurisprudenza europea.

Se si accoglie tale prospettiva, appare possibile sostenere che le disposizioni sanzionatorie del d.lgs. n. 138/2024 siano sostanzialmente lesive di alcune fondamentali garanzie che l'ordinamento riconosce a tutela del cittadino.

In primo luogo, risulterebbe non conforme al principio di tipicità la previsione dei commi 8 e 10 dell'art. 38.

Ad una prima lettura le disposizioni ora citate sembrano volte a circoscrivere le fattispecie la cui violazione determina l'esercizio dei poteri sanzionatori da parte dell'ACN; tuttavia, un'analisi più attenta del dettato legislativo sembrerebbe rilevare una sostanziale indeterminatezza delle condotte punite.

Per quanto concerne il comma 8, sono genericamente richiamati tutti i principali obblighi imposti alle imprese (responsabilità degli organi di amministrazione, misure di gestione dei rischi per la *cybersecurity*, obblighi in materia di notifica di incidente) attraverso il rinvio agli articoli 23, 24 e 25 del decreto legislativo; a ciò si aggiunga, come più volte sottolineato, che l'effettiva determinazione degli stessi obblighi è demandata all'ACN, come emerge dalla lettura dell'art. 31 del d.lgs. n. 138/2024, anch'esso richiamato dalla disposizione normativa in esame.

Una riflessione analoga parrebbe percorribile in relazione al comma 10, relativo alle violazioni di minore gravità. Nonostante la fattispecie sembrerebbe svolgere richiami più puntuali rispetto alla precedente, anch'essa appare non conforme ai canoni della tipicità. Anche in questo caso il contenuto delle fattispecie sanzionate è determinato in taluni casi dall'ACN, per effetto del rinvio all'art. 31. L'ACN determina altresì le modalità di registrazione sulla piattaforma di cui all'art. 7, la cui inosservanza è punita su disposto della lettera b. Particolarmente generica sembrerebbe anche la disposizione di cui alla lettera f, che punisce la «mancata collaborazione con il CSIRT Italia».

---

[111] M. Matassa, *La sicurezza cibernetica come funzione* pubblica, cit., 284.

[112] *Ibidem*.

In secondo luogo, l'impianto sanzionatorio previsto dal d.lgs. n. 138/2024 sembra porsi in contrasto con il principio di determinatezza. La tecnica redazionale utilizzata dal legislatore, infatti, si limita ad indicare i massimi edittali[113] per la violazione delle fattispecie indicate dai commi 8 e 10 dell'art. 38, rimettendo per il resto alla discrezionalità dell'Agenzia la determinazione della misura della sanzione.

Ciò sembrerebbe determinare un elevato grado di incertezza che pregiudica le imprese in quanto potenziali destinatarie delle sanzioni.

Inoltre, siffatta conformazione delle disposizioni sanzionatorie, a parere di chi scrive, rischia di privare il sistema di un'adeguata proporzionalità. Come evidenziato in precedenza, infatti, l'ambito di applicazione della direttiva NIS 2 assume contorni molto ampi e in grado di ricomprendere anche piccole imprese[114].

Sul punto deve segnalarsi come in sede di recepimento sia stata prevista una «clausola di salvaguardia»[115] volta a bilanciare l'estensione dell'ambito di applicazione della disciplina europea con la necessità di imporre gli obblighi in materia di *cybersecurity* ai soli soggetti capaci di rispettare le misure impartite. Tuttavia, bisogna altresì osservare che, al fine di impedire un utilizzo elusivo della clausola di salvaguardia, il legislatore ha previsto che la stessa possa applicarsi solo ai soggetti che dimostrino la presenza di particolari condizioni[116].

Per quanto la disposizione in esame si mostri come il risultato di una difficile operazione di bilanciamento tra le esigenze securitarie e la necessità di tutelare le piccole e le microimprese, la ristrettezza dell'ambito applicativo della clausola potrebbe rendere la stessa uno strumento di per sé non sufficiente ad escludere dal campo di applicazione degli obblighi in materia di *cybersecurity* soggetti dalle dimensioni eccessivamente esigue.

Realtà economiche di ristrette dimensioni sarebbero irrimediabilmente pregiudicate dall'applicazione di una sanzione nella misura dei massimi edittali previsti dai commi 9 e 11 dell'art. 38 del d.lgs. n. 138/2024. Unico argine di fron-

---

[113] Per altro, dal contenuto dei commi 9 e 11 dell'art. 38, emerge il particolare carattere afflittivo-punitivo delle sanzioni in esame, data la possibilità di determinare la misura della sanzione basandosi sul fatturato dell'impresa qualora ciò consentisse di individuare una cifra superiore (nello specifico caso del co. 9) ad 1 milione di euro.

[114] Nonostante l'art. 2 della direttiva NIS 2 definisca l'ambito di applicazione della disciplina introdotta mediante il ricorso ad un criterio di carattere dimensionale che limita l'applicazione delle disposizioni previste ai soggetti pubblici e privati, operanti all'interno dell'UE con i soggetti pubblici o privati con almeno 50 addetti e un fatturato compreso fa i 10 e i 50 milioni di euro, è pur vero che lo stesso art. 2, paragrafo 2, della direttiva NIS 2 individui svariate ipotesi in cui il suddetto criterio dimensionale non trova applicazione.

[115] Cfr. art. 7, co. 7, d.lgs. n. 138/2024.

[116] Come specificato dal DPCM n. 221/2024, l'esenzione dagli obblighi imposti dalla NIS 2 è riservata ai soggetti in possesso di due requisiti congiuntamente necessari: la totale indipendenza dei propri sistemi informativi e di rete NIS da quelli delle imprese collegate; la totale indipendenza delle proprie attività e servizi «NIS» da quelli svolti dalle imprese collegate.

te al rischio di un nocumento irreversibile per le piccole e microimprese sarebbe allora rappresentato dalla ragionevolezza dell'ACN, una garanzia che potrebbe tuttavia rivelarsi insufficiente. Secondo il parere di chi scrive, in coerenza con l'enunciata proporzionalità perseguita dal legislatore europeo nel delineare il sistema NIS 2, sarebbe forse stata necessaria la previsione di apposite disposizioni sanzionatorie relative ai soggetti di minori dimensioni.

In definitiva, ci si interroga se il sistema sanzionatorio delineato in sede di recepimento della direttiva NIS 2 abbia portato con sé le criticità proprie del sistema sanzionatorio del GDPR (General Data Protection Regulation), posto che, come evidenziato poc'anzi, il legislatore appare essersi ispirato a tale modello per la previsione delle sanzioni in caso di violazione degli obblighi in materia di *cybersecurity*.

In relazione al Regolamento Europeo Generale sulla protezione dei dati personali, infatti, parte della dottrina ha a suo tempo sollevato un possibile contrasto con i principi di tassatività, determinatezza e proporzionalità, imprescindibili garanzie da riconoscere ai cittadini anche in materia di sanzioni amministrative sostanzialmente punitive, sino a sostenere l'illegittimità del sistema sanzionatorio previsto in sede europea[117].

5. *Conclusioni*

Le recenti politiche in materia di sicurezza cibernetica appaiono determinare la creazione di un sistema multilivello in grado di rafforzare le difese degli Stati membri di fronte alle minacce informatiche.

Come evidenzia la dottrina, e come parrebbe emergere dalle disposizioni citate, nel prossimo futuro i privati avranno un ruolo fondamentale nel contrasto ai *cyberattacks*, ed è ormai pacificamente condivisa la necessità di un loro coinvolgimento nelle politiche di sicurezza.

Le modalità di inclusione dei privati in una materia su cui storicamente lo Stato esercita la propria sovranità esclusiva, rappresenta una delle maggiori sfide per il futuro delle politiche di *cybersecurity*.

In relazione agli interventi analizzati nel presente contributo, sorgono dunque delle perplessità, considerando che «i soggetti chiamati a sostenere i costi

[117] Si veda in tal senso A. Ciccia Messina, *Profili di criticità e di invalidità delle norme sanzionatrici del GDPR,* in *Ciberspazio e diritto*, 2021, 1, 3 ss.

dell'intera infrastruttura europea risultano oggi in larga parte coincidenti con gli stessi onerati ad adempiere ai diversi obblighi previsti dall'attuale architettura»[118].

Il d.l. n. 105/2019, alla luce della necessità di tutelare la sicurezza nazionale, impone una serie di obblighi che il privato deve limitarsi ad adempiere, secondo le logiche tipiche delle obbligazioni di mezzo[119].

Si tratta di un approccio differente rispetto a quello adottato dagli interventi più recenti di tipo *risk-based*. Conformare le misure adottate alle minacce che si intende contrastare, infatti, appare essere il modo più efficace per garantire elevati livelli di sicurezza.

La disciplina interna solleva alcune perplessità rispetto alla posizione delle imprese, private di un'adeguata conoscenza degli atti che incidono sulla propria posizione e della possibilità di interloquire adeguatamente con l'autorità se non in sede giurisdizionale.

Forse sembra essere giunto il momento di un aggiornamento della disciplina interna, considerando anche la presenza di un elemento paradossale: le sanzioni previste dalla disciplina interna in relazione alla sicurezza nazionale sono esigue rispetto a quelle disposte dal legislatore europeo per tutelare il mercato unico. L'esito, dunque, è quello di un sistema «a tutele invertite»[120].

La disciplina europea mostra in tal senso un approccio più maturo, ma che non sembra essere immune da critiche.

L'ambito di applicazione, particolarmente ampio, ricomprende anche piccole imprese che rischiano di non essere in grado di adeguarsi alle misure imposte. In tal senso, come già sottolineato, le misure di bilanciamento adottate in sede di recepimento rischiano di rivelarsi insufficienti a causa del ristretto ambito di applicazione. Da una parte, ciò potrebbe convertirsi in un limite all'accesso al mercato da parte di operatori economici, che nell'avvio della propria attività potrebbero non disporre delle risorse necessarie per far fronte agli obblighi in materia di sicurezza cibernetica; dall'altra, gli stessi obblighi potrebbero costituire un deterrente per gli operatori economici già presenti, poiché un potenziale aumento della produzione potrebbe determinare l'inclusione all'interno della disciplina in materia di sicurezza cibernetica.

Nonostante il dettato normativo sottolinei l'esigenza di modulare gli obblighi imposti ai diversi soggetti secondo un criterio di proporzionalità, si teme comunque il rischio di una eccessiva pressione esercitata sugli operatori privati, soprattutto di minori dimensioni.

---

[118] R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in *Teoria e Critica della Regolazione Sociale,* 2025, 1, 7 ss.

[119] M. Matassa, *La sicurezza cibernetica come funzione pubblica*, cit., 277.

[120] Ivi., 280.

Delineare un sistema idoneo a fronteggiare la minaccia cibernetica tenendo in debita considerazione le libertà proprie dei privati non è certamente un compito agevole; tuttavia, tendere ad un continuo perfezionamento del sistema risulta necessario. Un sistema eccessivamente sbilanciato in favore delle istanze securitarie, infatti, potrebbe essere dannoso quasi quanto un sistema eccessivamente vulnerabile, danneggiando gli operatori economici attraverso l'imposizione di obblighi eccessivamente stringenti e privati di idonee garanzie dinanzi al pubblico potere.

Paolo Campagna - Abstract

Le tutele per le imprese all'interno del Perimetro di Sicurezza Nazionale Cibernetica

Il presente lavoro intende analizzare le tutele da riconoscere agli operatori economici privati inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC), nonché destinatari in via residuale degli obblighi di matrice europea posti dalla direttiva NIS 2. La prima parte dell'articolo si sofferma sui presupposti che legittimano il legislatore nazionale a comprimere la libertà di impresa, con particolare riferimento alla sicurezza nazionale. La seconda parte analizza il d.l. n. 105/2019, istitutivo del PSNC, per individuare le garanzie sostanziali e procedurali da assicurare ai soggetti "perimetrati". Infine, ci si sofferma sulle disposizioni della direttiva NIS 2, per valutare, anche rispetto agli obblighi promanati dal diritto europeo, le necessarie guarentigie da riconoscere a tali soggetti.

Protections for Businesses Within the National Cybersecurity Perimeter

This paper aims to analyze the protections to be afforded to private economic operators included within the National Cyber Security Perimeter (PSNC), as well as those subject, on a residual basis, to the European obligations set forth by the NIS 2 Directive. The first part of the article focuses on the grounds that justify the national legislature in restricting freedom of enterprise, with particular reference to national security. The second part analyzes Decree-Law n. 105/2019, establishing the PSNC, to identify the substantive and procedural safeguards to be ensured for entities within the "perimeter." Finally, the article examines the provisions of the NIS 2 Directive to assess, including in light of obligations under European law, the necessary safeguards to be granted to such entities.