mediaLAWS

Anticipazioni

La funzione di *public cybersecurity* come preminente funzione pubblica digitale alla luce della Direttiva NIS2

Alfonso Contaldo

La funzione di *public cybersecurity* come preminente funzione pubblica digitale alla luce della Direttiva NIS2

Abstract

Il cyberspazio è una sorta di non luogo di progettazione matematica in cui oramai si svolgono molte attività umane aventi anche rilevanza economica e finanziaria ed in cui lo Stato si attiva per garantirvi soprattutto la funzione di Pubblica sicurezza, che in riferimento alle attività di governo statale e di livello centrale e locale necessitano di un complesso di apparati, autorità e strutture preposte alla tutela dell'ordine pubblico e all'incolumità delle persone.
La pubblica sicurezza nel cyberspazio riguarda tanto le attività di polizia, volte ad assicurare la "sicurezza" attraverso il rispetto delle norme di legge, quanto quelle comunque finalizzate a "prevenire" che la comunità possa patire danni da eventi fortuiti e accidentali, infortuni e disastri di qualunque altro genere.

Cyberspace is a sort of non-place of mathematical planning in which many human activities now take place which also have economic and financial relevance and in which the State takes action to guarantee above all the public security function, which in reference to the activities of state government and at a central and local level require a complex of apparatus, authorities and structures responsible for the protection of public order and the safety of people.
Public safety in cyberspace concerns both police activities, aimed at ensuring "safety" through compliance with the law, and those aimed at "preventing" the community from suffering damage from fortuitous and accidental events, accidents and disasters. of any other kind.

Sommario

Keyword

cyberspazio – Stato – pubblica sicurezza – prevenzione – danni digitali

1. Il ciberspazio come "ambito spaziale" per le funzioni pubbliche digitali

Il Ciberspazio è il "luogo" nel quale sembra accadere una trasmissione telematica anche *point to point*.[1] Lo "spazio" nel ciberspazio possiede gli aspetti in comune con l'astratto

[1] Vedi B. Sterling, *Giro di vite contro gli hacker*, Boston, 2015, 122 ss.

significato matematico del termine piuttosto che con lo spazio fisico: il significato spaziale può essere attribuito alla relazione tra i *bit*. Il concetto di ciberspazio quindi si riferisce non al contenuto presentato al navigatore, ma piuttosto alla possibilità di navigare tra differenti siti, tramite i cicli di *feedback* tra l'utente ed il resto del sistema (in una soluzione matematica), che crea così la possibilità potenziale di incontrare sempre qualcosa di inatteso e sconosciuto e pertanto lo stesso ciberspazio diventa una sorta di "non luogo" (come soluzione matematica), prescindendo dal contatto personale tra soggetti e consentendo agli utenti, attraverso l'uso di strumenti assai diffusi non solo tra gli *hacker* e i *cracker* di agire nel pieno anonimato, anche durante la pandemia del Covid ad organi costituzionali[2].

Ciò spiega perché l'ordinamento statuale, da alcuni anni a questa parte, stia tentando di garantire in tale ambito il rispetto delle norme giuridiche nazionali[3], l'esercizio di pubbliche funzioni e la repressione di eventuali crimini[4], oltreché l'ingerenza sulla corretta fruibilità dello stesso. Ciò spiega perché nel ciberspazio lo Stato vi operi per il rispetto del suo ordinamento giuridico con settori specializzati delle forze di polizia, con la difesa da attacchi di *cyberwarfare* da raggruppamenti specializzati delle Forze Armate (non da "armi" vere e proprie), mentre le *policies* della "difesa" del ciberspazio viene garantita dall'Agenzia per la Cibersecurity Nazionale (ACN)[5]. Il ciberspazio afferente allo Stato italiano non è quindi un "territorio" difeso da una Forza armata, come lo sono la terra (Esercito), l'aria (Aeronautica militare), il mare (Marina militare), ma una sorta di "non luogo" di struttura matematica avente rilevanza economica anche per la criminalità[6] dove il rispetto dell'ordinamento è garantito dalle attività delle forze di polizia (Polizia di Stato, Carabinieri, Guardia di Finanza), dalle agenzie per la sicurezza nazionale (AISI, AISE) e la cui fruibilità corretta è garantita rispetto a pratiche che danneggerebbero gli *asset* da un'apposita agenzia (Agenzia per la Cibersecurity Nazionale), mentre le Forze armate rispondono agli attacchi di *cyberwarfare*. Sembra così definirsi una sorta di Stato digitale che riporta in codice binario diverse sue attività e competenze pur non riducendosi ad esse[7].

---

[2] Vedi P. Marsocci, *Lo spazio digitale dei lavori parlamentari e l'emergenza sanitaria Covid-19*, in questa *Rivista*, 2020, 2, 52 ss.

[3] Vedi A. Venanzoni, *Sovranità tra ordine costituzionale, digitale e poteri privati*, in M. Proietti-A. Venanzoni, *La sovranità digitale fra sicurezza nazionale e ordine costituzionale*, Pisa, 2023, 137 ss.

[4] Vedi A.C. Amato Mangiameli, *Reato e reati informatici. Tra teoria generale del diritto e informatica giuridica,* in A.C. Amato Mangiameli-G. Saraceni, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino, 2019, 27 ss.

[5] Vedi M.F. Dos Santos-A. Contaldo, *L'Agenzia per la cybersicurezza nazionale: istituzione e problematiche in campo*, in *Riv. amm. Rep. it.,* 5/6, 2022, 343 ss.; G.G. Cusenza, *I poteri dell'Agenzia per la Cybersicurezza Nazionale: una nuova regolazione del mercato cibernetico*, in R. Ursi (a cura di), *La sicurezza nel cyberspazio,* Milano, 2023, 123 ss.

[6] Vedi S. Pietropaoli, *Informatica criminale*, Torino, 2023, 81 ss.

[7] Vedi L. Torchia*, Lo Stato digitale. Un'introduzione*, Bologna, 2023, 72 ss.

2. La vigilanza, l'esecuzione e la giurisdizione sul "cyberspazio nazionale"

La Direttiva NIS 2 (direttiva (UE) 2022/2555) disciplina altresì la giurisdizione e la "competenza" (anche se sulla previsione di un ambito cibernetico, sul quale non è mai intervenuto finora il diritto internazionale), dall'art. 26 e seguenti indicando che i soggetti che rientrano nel suo ambito di applicazione debbano essere «considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti».

A questo principio, la prima e più evidente eccezione riguarda i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico, poiché in entrambi i casi considerati sono posti sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi a prescindere dal luogo dove essi sono stabiliti[8].

La seconda eccezione, invece, più prosaicamente prevede che per la libera circolazione dei servizi debbano essere considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione europea alcune categorie di soggetti tassativamente elencate: a) i fornitori di servizi DNS; b) i registri dei nomi di dominio di primo livello; c) i soggetti che forniscono servizi di registrazione dei nomi di dominio; d) i fornitori di servizi di *cloud computing*; e) i fornitori di servizi di data center; f) i fornitori di reti di distribuzione dei contenuti; g) i fornitori di servizi gestiti; h) i fornitori di servizi di sicurezza gestiti; i) i fornitori di mercati online; l) di motori di ricerca online o di piattaforme di servizi di social network.

In relazione a tale seconda eccezione, al fine di determinare se un soggetto ha il proprio stabilimento principale nell'Unione europea, non sono criteri decisivi la presenza e l'utilizzo dei sistemi informativi e di rete, poiché occorre avere riguardo allo Stato membro in cui sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio di cibersicurezza. Nel caso in cui non sia possibile individuare lo Stato membro si dovrà applicare il successivo criterio secondo il quale lo stabilimento principale è quello nello Stato membro in cui sono effettuate le operazioni di cibersicurezza[9]. Per *extrema ratio*, si applica un terzo criterio, ossia che lo stabilimento principale venga determinato dalla sede con il maggior numero di dipendenti nell'Unione europea[10] .

Con riferimento alla suddetta seconda eccezione è, altresì, prevista la designazione di un rappresentante nell'Unione europea per il soggetto che senza esservi stabilito offra servizi nel territorio di uno Stato membro. E' stato ricordato[11] come ai sensi dell'art. 6, n. 34, della Direttiva NIS 2 il "rappresentante" sia una persona fisica o giuridica

---

[8] Ci si permette di rinviare al nostro *L'attuazione della* cybersecurity *nazionale: un difficile esercizio di una funzione pubblica*, in *Lo Stato*, 2023, 21, 283 ss.

[9] Le operazioni di cybersicurezza diventano così una sorta di stabilimento. Sul punto *Ibid.* e, soprattutto, S. Marchiafava, *Giurisdizione, vigilanza ed esecuzione*, in C. Cavaceppi-A. Contaldo (a cura di), *Cybersecurity connect*, Roma, 2024, 254 ss.

[10] Ma ciò richiede che la previsione di un perimetro cibernetico delle imprese sia attivata da tutti gli Stati europei. Vedi L. Calandriello, *Il perimetro di sicurezza nazionale cibernetica*, in R. Ursi (a cura di), *La sicurezza*, cit., 136 ss.

[11] Ancora S. Marchiafava, *Giurisdizione*, cit., 254 ss.

stabilita nell'Unione europea, espressamente designata ad agire per conto di un fornitore di servizi DNS, un registro dei nomi TLD, un soggetto che fornisce servizi di registrazione di nomi di dominio, un fornitore di servizi di *cloud computing*, un fornitore di servizi di *data center*, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi gestiti, un fornitore di servizi di sicurezza gestiti, o un fornitore di mercato online, di un motore di ricerca online o di una piattaforma di servizi di *social network* che non è stabilito nell'Unione europea, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in sostituzione del soggetto in questione per quanto riguarda gli obblighi posti in capo a quest'ultimo dalla stessa Direttiva NIS 2 .

Quindi il rappresentante è considerato come "stabilito" in uno degli Stati membri in cui sono offerti i servizi, con la conseguenza che il soggetto rappresentato a sua volta sarà sotto la giurisdizione dello Stato membro in cui il suo rappresentante si è stabilito. La mancata designazione del rappresentante nell'Unione europea non è priva di conseguenze. Essa, infatti, ai sensi dell'art. 26, costituisce una violazione degli obblighi previsti dalla Direttiva NIS 2 e «qualsiasi Stato membro in cui il soggetto fornisce servizi» ha il potere di promuovere nei suoi confronti un'azione legale davanti alla Corte di Giustizia; la designazione del rappresentante fa salve le azioni legali che potrebbero essere avviate nei confronti del rappresentato.

Gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca in relazione a uno dei soggetti con stabilimento principale nell'Unione europea possono, entro i limiti di tale richiesta, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto interessato che nel loro territorio fornisce servizi oppure ha un sistema informativo e di rete. La terza e ultima eccezione al principio di stabilimento, sancito dal sopramenzionato art. 26, primo paragrafo, della Direttiva NIS 2, è rappresentata dagli enti della pubblica amministrazione. Secondo la direttiva in parola per «ente della pubblica amministrazione» si intende: un soggetto riconosciuto come tale in uno Stato membro conformemente al diritto nazionale che soddisfa i seguenti criteri: a) è istituito allo scopo di realizzare esigenze di interesse generale ed è privo di carattere industriale o commerciale; b) è dotato di personalità giuridica o autorizzato per legge ad agire a nome di un altro soggetto che ne è dotato; c) è finanziato in prevalenza dallo Stato, da autorità regionali o da altri organismi di diritto pubblico, la sua gestione è soggetta alla vigilanza di tali autorità o organismi, oppure è dotato di un organo di amministrazione, di direzione o vigilanza, in cui più della metà dei membri è designata dallo Stato, da autorità regionali o da altri organismi di diritto pubblico; d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle merci, delle persone, dei servizi o dei capitali. Sono esclusi dalla definizione di ente della pubblica amministrazione: la magistratura, i parlamenti e le banche centrali. Tali enti sono, infatti, considerati posti sotto la giurisdizione dello Stato membro che li ha istituiti.

Assumono, inoltre, un ruolo centrale gli obblighi in materia di vigilanza ed esecuzione previsti in capo agli Stati membri dalla Direttiva NIS 2.

Di qui anche l'esigenza di imporre agli Stati membri: (a) la designazione di una o più autorità nazionali competenti in materia di cibersicurezza per lo svolgimento dei

compiti di vigilanza previsti dalla Direttiva NIS 2; (b) l'individuazione del Single Point Of Contact (SPOC) con funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri[12].

Ai sensi dell'art. 8 della Direttiva NIS 2, ogni Stato membro designa o istituisce una o più autorità competenti responsabili della cibersicurezza e dei compiti di vigilanza disciplinati dal settimo capo VII, nonché sul controllo per quanto riguarda l'attuazione della stessa direttiva a livello nazionale[13], istituendo un Punto Unico di Contatto che svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le omologhe autorità degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA[14], nonché per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro.

Diviene, altresì, compito degli Stati membri assicurare alle rispettive autorità nazionali competenti e ai propri punti di contatto unici, le risorse adeguate a svolgere i compiti loro assegnati e conseguire, quindi, gli obiettivi della Direttiva NIS 2.

Tra le novità anche l'introduzione di un regime di vigilanza ex post applicato a un numero di nuovi soggetti denominati «soggetti importanti». La Direttiva NIS 2 ha l'obiettivo di rendere il livello di *cybersecurity* di operatori considerati «essenziali» e «importanti» uniforme su tutto il territorio europeo. Nella prima categoria troviamo anche le pubbliche amministrazioni, in aggiunta agli operatori del settore energetico, sanitario, spaziale, bancario, dei trasporti, delle infrastrutture digitali, delle acque. Nella seconda categoria troviamo i soggetti importanti, cioè gli operatori di servizi postali e corriere, di gestione dei rifiuti, del settore chimico, del settore agroalimentare. Tale distinzione tra soggetti essenziali e soggetti importanti, contemplata dall'art. 3 della Direttiva NIS 2, rappresenta una delle novità più significative.

La Direttiva NIS 2 contraddistingue tra un regime di vigilanza ex ante per i soggetti essenziali e un regime di vigilanza *ex post* per i soggetti importanti; tale ultimo regime impone alle autorità competenti di adottare provvedimenti quando ricevono elementi di prova o indicazioni che un soggetto importante non soddisfa i requisiti di sicurezza e di segnalazione degli incidenti.

Gli Stati membri devono imporre alle rispettive autorità competenti di monitorare e di vigliare lo stabilimento, imponendo ovviamente di adottare le misure necessarie per garantire l'osservanza[15] della Direttiva NIS 2: pertanto in un approccio basato sul rischio, le autorità nazionali competenti stabiliscono metodologie che permettono di conferire priorità ai compiti di vigilanza esercitati ai sensi degli artt. 32 e 33 della stessa Direttiva NIS 2. Quindi nei casi di incidenti che determinano la violazione di dati personali è contemplata una specifica e stretta collaborazione tra le autorità competenti secondo la Direttiva NIS 2.

---

[12] Ci si permette di rinviare al nostro *L'attuazione*, cit., 294 ss.

[13] Ancora S. Marchiafava, *Giurisdizione*, cit.

[14] Ci si permette di rinviare al nostro *L'ENISA e le competenze comunitarie per la cibersicurezza, in Riv. polizia*, 6/7, 2018, 655 ss.

[15] Vedi I. Forgione, *Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del Sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in R. Ursi (a cura di), *La sicurezza*, cit., 95 ss.

Riguardo agli enti della pubblica amministrazione, tenuti all'osservanza della Direttiva NIS 2, gli Stati membri devono attribuire alle rispettive autorità, in Italia la ACN[16], poteri adeguati e un'indipendenza operativa in relazione alle misure di vigilanza e di esecuzione da imporre a tali enti conformemente ai quadri legislativi e istituzionali nazionali.

Con l'art. 5 del d. lgs. 4 settembre 2024 n. 138 si ribadisce che vengono sottoposti alla giurisdizione nazionale i soggetti di cui all'art. 3 dello steso decreto legislativo stabiliti sul territorio nazionale, ad eccezione degli stessi medesimi casi già previsti dalla direttiva (UE) 2022/2555 (i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico; i fornitori di servizi di sistema dei nomi di dominio DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di *cloud computing*, i fornitori di servizi di *data center*, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che sono sottoposti la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione; gli enti della pubblica amministrazione). Si considera altresì lo stabilimento principale nell'Unione quello dello Stato membro nel quale sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio per la sicurezza informatica. Se non è possibile determinare lo Stato membro in cui sono adottate le suddette decisioni o se le stesse non sono adottate nell'Unione, lo stabilimento principale è quello collocato nello Stato membro in cui sono effettuate le operazioni di sicurezza informatica. Nel caso di soggetti non stabiliti nel territorio dell'Unione ma offrono servizi all'interno dello stesso, essi debbono designare un rappresentante nell'Unione, che è stabilito in uno degli Stati membri in cui sono offerti i predetti servizi ed è sottoposto alla relativa giurisdizione. In caso di mancanza della designazione del rappresentante, l'ACN può avviare un'azione legale, nei confronti dei soggetti inadempienti, anche se non appartenenti al Perimetro Nazionale di Sicurezza Cibernetica, che viene quindi a ricevere una possibile integrazione.

3. La delineazione Perimetro Nazionale di Sicurezza Cibernetica nella legge n. 133 del 2019 e il coordinamento con il d. lgs. n. 138 del 2024

Il Perimetro Nazionale di Sicurezza Cibernetica viene a definirsi come il "non luogo tecnologico" che insistendo sulla rete potrebbe anche concorrere al formarsi di una normativa internazionale che possa delineare il suo rapporto con gli ordinamenti statuali[17], venendo ad acquisire una più significativa connessione operativa con i soggetti

[16] Vedi G.G. Cusenza, *I poteri*, cit., 115 ss.

[17] Vedi G. Sartor, *La rivoluzione informatica e la globalizzazione*, in G. Torresetti (a cura di), *Diritto, politica e realtà sociale nell'epoca della globalizzazione* – Atti del XXII Congresso della Società Italiana di filosofia giuridica e politica, Macerata, 2008, 245 ss.

che ne contribuiscono il suo sviluppo[18]. Quindi nell'attuale quadro normativo delle infrastrutture tecnologiche strategiche, in linea con le più elevate ed aggiornate misure di sicurezza adottate a livello internazionale, l'art. 1 del d.l. 21 settembre 2019, n. 105, così come modificato dalla legge 18 novembre 2019 n. 133, istituisce il cd. Perimetro Nazionale di Sicurezza Cibernetico come una modalità organizzativa al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per «il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale». Inoltre si ricorre alla previsione del regolamentazione attraverso i decreti del Presidente del Consiglio dei Ministri su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), per prevedere ai sensi dell'art. 1-bis del d.l. 15 marzo 2012, n. 21, il contemperamento delle disposizioni in materia di valutazione della presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti inerenti ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G[19] e dei dati che vi transitano con le misure volte ad individuare le attività di rilevanza strategica per il sistema di difesa e di sicurezza nazionale, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'art. 4, c. 3, lett. l), della l. 3 agosto 2007, n. 124.

Il Presidente del Consiglio dei Ministri coordina la coerente attuazione delle disposizioni che disciplinano il Perimetro, anche avvalendosi del Dipartimento delle Informazioni per la Sicurezza, che assicura gli opportuni raccordi con le autorità titolari delle competenze sul settore e con gli altri soggetti interessati.

L'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziale, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici.

Anche se il ritardo temporale rispetto ai quattro mesi dalla l. 18 novembre 2019 n. 133 che ha convertito il decreto-legge istitutivo dell'Agenzia Nazionale della Cybersecurity[20], è stata data l'attuazione della potestà regolamentare in capo al Presidente del Consiglio di Ministri che su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) ha adottato il dPCM 31 luglio 2020 n. 131, al di fine: a) di individuare le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati,

---

[18] Sulla disciplina normativa del perimetro nazionale cibernetico vedi S. Mele*, Il perimetro di sicurezza nazionale cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della Pubblica amministrazione alla sicurezza nazionale*, in G. Cassano-S. Previti (a cura di), *Il diritto di internet dell'era digitale*, Milano, 2020, 185 ss.

[19] Ci si permette di rinviare al nostro, *La disciplina della sicurezza del perimetro cibernetico nazionale anche alla luce dello standard 5G*, in A. Contaldo-D. Mula (a cura di), *Cibersecurity law*, Pisa, 2021, 185 ss.; M. Matassa, *La regolazione della cybersecurity in Italia*, in R. Ursi (a cura di), *La sicurezza*, cit., 21 ss.

[20] Vedi I. Forgione, *Il ruolo*, cit., 95 ss.

inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; alla predetta individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla loro legge istitutiva (l. 3 agosto 2007, n. 124)[21], si procede sulla base dei peculiari criteri[22]; b) di definire i criteri in base ai quali i soggetti già predeterminati in precedenza predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, e nel provvedere all'elaborazione di tali criteri, adottando opportuni moduli organizzativi, sulla scorta di quanto previsto dall'organismo tecnico di supporto al CISR, integrato con un rappresentante della Presidenza del Consiglio dei ministri; c) di curare (sempre a carico dei suddetti soggetti) la trasmissione entro sei mesi dalla data di entrata in vigore del decreto in questione, la trasmissione di tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico (ora MIMIT), i quali a loro volta inoltrano gli elenchi di rispettiva pertinenza al Dipartimento delle Informazioni per la Sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, che ai sensi dell'art. 7 *bis* della l. 31 luglio 2005, n. 155, provvede sia ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate da un apposito decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate, sia ad operare per la prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con i mezzi informatici, con gli ufficiali di polizia giudiziaria all'uopo incaricati anche in collaborazione con gli altri organi di polizia.

Il cyberspazio può, pertanto, essere considerato come delimitazione dello "Stato digitale", secondo una concezione elaborata dalla dottrina giusamministrativa per il quale l'apparato pubblico «continua, naturalmente, a svolgere tutte le funzioni e i compiti da esso precedentemente assunti, ma presenta due caratteristiche nuove rispetto al passato. Sotto un primo profilo, l'attività pubblica nel suo complesso viene trasformata, quanto a modi e strumenti, mediante l'applicazione di nuove tecnologie.

Che si tratti della sicurezza o dei servizi pubblici, della realizzazione di infrastrutture o dell'esercizio della giustizia, della moneta e della difesa, della salute o della pianificazione del territorio, si impone via via il ricorso a strumenti tecnologici che portano con sé sia una riarticolazione e riorganizzazione delle funzioni e delle strutture pubbliche, sia la ridefinizione delle regole di esercizio del potere pubblico e delle relative modalità

[21] Sul punto vedi F. Pastore, *Il coordinamento delle forze di polizia e di sicurezza italiane nella lotta al terrorismo*, in *Diritti fondamentali*, 2021, 2; P. Vipiana, *Introduzione al diritto della sicurezza pubblica*, Torino, 2022, 91 ss.; R. Ursi, *La sicurezza pubblica*, Bologna, 2022, 112 ss.

[22] Questi criteri vengono individuati nelle fattispecie nelle quali: 1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato; 2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

di controllo. Sotto un secondo profilo, lo sviluppo tecnologico investe i rapporti economici e sociali in misura tale da rendere spesso inidonee o obsolete le regole vigenti. Di qui la necessità di una nuova regolazione pubblica volta ad aggiornare discipline già esistenti e a introdurre principi e regole nuove per fenomeni nuovi»[23]. Ora proprio la perimetrazione dello Stato digitale comporta non una sua difesa, perché lo Stato digitale incide su un "non luogo", ma un esercizio di una pubblica funzione derivata dalla sovranità statale[24].

Con l'art. 33 del d.lgs. 138/2024 gli obblighi di gestione del rischio per la sicurezza informatica e di notifica di incidente previsti dal d.l. 21 settembre 2019, n. 105, convertito, con modificazioni, dalla l. 18 novembre 2019, n. 133, sono considerati equivalenti a quelli previsti dal d.lgs. n. 138 del 2024. Inoltre, alle reti, ai sistemi informativi e ai servizi informatici inseriti nell'elenco di cui all'art. 1, c. 2, del d.l. 105/2019, non si applicano le disposizioni di cui allo stesso d.lgs. n. 138/2024, restando fermi gli obblighi per i sistemi informativi e di rete. Infine, i soggetti di cui all'art. 1, c. 2-*bis*, del d.l. 105/2019, non sono sottoposti agli obblighi di notifica per gli incidenti riconducibili a una notifica già effettuata per la specificità dell'attività. Pertanto, proprio come forma di esercizio della *public cybersecurity* dovremmo ritenere l'esercizio sul Perimetro Nazionale dell'esercizio delle competenze dell'Agenzia per la Cybersicurezza Nazionale.

4. L'Agenzia per la Cybersicurezza Nazionale e l'esercizio delle funzioni di vigilanza sul cyberspazio

Il d.lgs. 14 giugno 2021 n. 82 recante "Disposizioni urgenti in materia di cybersicurezza", ha ridefinito l'architettura nazionale di cybersicurezza e ha istituito l'Agenzia per la cybersicurezza nazionale, convertito con modificazioni dalla legge 4 agosto 2021 n. 109.

Esso appare disciplinare il settore della cybersicurezza in Italia, individuando competenze, soggetti e contenendo importanti novità, aspirando così ad essere il prodotto legislativo più completo e aggiornato in materia, anche in allineamento con il Piano nazionale di ripresa e resilienza (PNRR), di cui la sicurezza cibernetica costituisce uno degli interventi previsti[25]. La cybersicurezza costituisce infatti l'Investimento 1.5 - rimesso direttamente all'Agenzia per la cybersicurezza nazionale - della Missione 1 del PNRR - "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo".

Da un punto di vista di qualificazione, a norma dell'art. 7 del d.lgs. 82/2021, l'Agenzia per la cybersicurezza nazionale costituisce l'autorità nazionale competente NIS e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi e Autorità nazionale di certificazione della cybersicurezza.

---

[23] Vedi L. Torchia, *Lo Stato,* cit., 19

[24] Vedi M. Luciani, voce *Integrazione europea, sovranità statale e sovranità popolare*, in *Treccani online*, 2009; R. Bin, *La sovranità nazionale e la sua erosione*, in R. Bifulco-O. Roselli, (a cura di), *Crisi economica e trasformazioni della dimensione giuridica. La costituzionalizzazione del pareggio di bilancio tra internazionalizzazione economica, processo di integrazione europea e sovranità nazionale*, Torino, 2013, 370 ss.; A. Vignudelli, *Diritto costituzionale*, Torino, 2019, 108 ss.; A. Pisaneschi, *Diritto Costituzionale*, Torino, 2016, 84 ss.

[25] Vedi S. Rossa, *Cybersicurezza e pubblica amministrazione,* Napoli, 2023, 62 ss.

In quanto Autorità nazionale di cybersicurezza, l'ACN è chiamata ad assicurare, ferme le competenze di altre amministrazioni e le attribuzioni del Ministero dell'interno nella qualità di autorità nazionale di pubblica sicurezza, «il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale» e promuovere «la realizzazione 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, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore» (art. 7, c. 1, lett. a).

L'Agenzia come autorità nazionale competente NIS (e NIS 2) si sostituisce in una certa misura al Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio, cui il decreto-legge perimetro aveva assegnato tale ruolo[26]. La disciplina elimina il riferimento al SISR, spostando la competenza in capo all'Agenzia relativamente ai settori e sottosettori di cui all'allegato II e ai servizi di cui all'allegato III del d.lgs. NIS, con contestuale designazione delle autorità di settore (art. 15, c. 1 lett. g), che modifica l'art. 7 del d.lgs. c.d. NIS). Proprio nel raccordo tra autorità nazionale competente e autorità di settore, è stato istituito presso l'Agenzia un Comitato tecnico di raccordo, presieduto dall'Agenzia stessa e composto da rappresentanti delle amministrazioni statali individuate quali autorità di settore (art. 15, c. 8, lett. i).

Inoltre, l'Agenzia viene designata quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi (art. 15, c. 3), essendo così chiamata a svolgere una funzione di collegamento e raccordo al fine di garantire la cooperazione transfrontaliera tra l'autorità nazionale competente NIS con le rispettive autorità di altri Stati membri. Come autorità nazionale competente NIS e punto di contatto unico, l'Agenzia consulta e collabora con l'autorità di contrasto e con il Garante per la protezione dei dati personali (art. 15, c. 6) e diviene altresì competente all'accertamento delle violazioni e all'irrogazione delle sanzioni, sempre previste dal d.lgs. c.d. NIS.

Non solo, il d.lgs. 82/2021, alla lett. f) del c. 1 dell'art. 7 specifica che l'Agenzia assume in realtà tutte le funzioni che le disposizioni vigenti attribuiscono al Ministero dello sviluppo economico. Vi si comprendono, in primo luogo, le funzioni che il decreto-legge perimetro ha assegnato al Centro di valutazione e certificazione nazionale, il quale viene, dunque, trasferito presso l'Agenzia per la cybersicurezza nazionale (art. 7, c. 4). Secondo poi, le funzioni relative alla sicurezza e all'integrità delle comunicazioni elettroniche (art. 7, c. 1, lett. f), n. 2) e quelle riferite alla sicurezza delle reti e dei sistemi informativi di cui al d.l.gs NIS (art. 7, c. 1, lett. f), n. 3). Confermano ciò le modifiche testuali di sostituzione apportate al decreto legislativo NIS e al decreto-legge perimetro (artt. 15, c. 2, lett. a), art. 16, c. 6, lett. a), e c. 8 del d.lgs. 82/2021).

Il Ministero dello Sviluppo Economico rimane competente autorità del settore infrastrutture digitali e servizi digitali NIS (art. 15, c. 1, lett. g).

Da enfatizzare, tra le funzioni, la partecipazione dell'ACN nella gestione ed esercizio dei poteri speciali (*golden power*) di cui al d.lgs. 21/2012: infatti, l'art. 7, c. 1, lett. g) dispone la partecipazione dell'Agenzia, per tutti gli ambiti di competenza, al Gruppo di

[26] Vedi L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale,* in *Giorn. dir. amm.,* 6, 2021, 721 ss.; I. Forgione, *Il ruolo,* cit., 95 ss.

coordinamento di cui ai regolamenti attuativi previsti dall'art. 1, c. 8, del d.l. 21/2012.
Continuando sul tema delle funzioni che provengono da altri enti, amministrazioni o organismi e che sono state assegnate all'Agenzia meritano una menzione le lett. h), i) e m) del c. 1 dell'art. 7 d.lgs. 82/2021.
In primo luogo, l'Agenzia assume tutte le funzioni in materia di perimetro di sicurezza nazionale cibernetica che il decreto legge perimetro e successivi provvedimenti attuativi avevano rispettivamente attribuito alla Presidenza del Consiglio dei ministri (lett. h) - incluse le attività di ispezione e verifica *ex* art. 1, c. 6, lett. c) del decreto-legge perimetro e le funzioni relative all'accertamento delle violazioni e all'irrogazione delle sanzioni – al DIS (lett. i) e all'Agenzia per l'Italia digitale (AgID).
In particolare, quanto all'AgID si segnala che il c. 1, lett. m), dell'art. 7 del d.lgs. 82/2021, pone l'accento su alcune delle funzioni attualmente trasferite all'ACN: quelle di cui all'art. 51 del d.l.gs 82/2005 (c.d. Codice dell'amministrazione digitale) in materia di Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni[27]; le competenze *ex* art. 71 del d.lgs. 82/2005 relative all'adozione di linee guida contenenti regole tecniche di cybersicurezza e, infine, le competenze che l'AgID si vedeva assegnata dall'art. 33 *septies,* c. 4, del d.lgs. 179/2012, vale a dire quelle relative a stabilire livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione, nonché alla definizione delle caratteristiche di qualità, sicurezza, performance e scalabilità, interoperabilità, e portabilità dei servizi *cloud* per la pubblica amministrazione. Inoltre, sulla stessa linea - e rientrante in modo più specifico nell'ultimo capoverso dell'art. 33 *septies,* c. 4, del d.lgs. 179/2012 - la lettera m-*ter* dell'art. 7, c. 1, dispone che l'Agenzia «provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione», competenza prima appartenente all'AgID.
Relativamente alle funzioni che vengono trasferite dall'AgID all'Agenzia *ex* art. 7, c. 1, lett. m), il d.lgs. 82/2021 stabilisce che, per le funzioni che restano di competenza dell'AgID, i raccordi tra le due amministrazioni vengono definiti attraverso decreti del Presidente del Consiglio dei Ministri.
Si segnala, inoltre, che il CSIRT italiano, di cui al d.lgs. c.d. NIS, viene trasferito dalla Presidenza del Consiglio dei ministri all'Agenzia, assumendo la denominazione di CSIRT Italia (art. 7, c. 3).
Inoltre, uno dei compiti più rilevanti che l'Agenzia ha in carico è la predisposizione della Strategia nazionale di cybersicurezza (art. 7, c. 1, lett. b) la quale viene approvata dal Presidente del Consiglio dei Ministri, sentito il Comitato Interministeriale per la Cybersicurezza. Recentemente è stata approvata e pubblicata la Strategia Nazionale di cybersicurezza 2022-2026 con relativo piano di implementazione, la quale si compone di tre obiettivi strategici: Protezione, Risposta e Sviluppo. Inoltre, l'ACN svolge attività di supporto al funzionamento del Nucleo per la cybersicurezza (art. 7, c. 1, lett. c) ed è chiamata allo sviluppo di capacità nazionali di prevenzione, monitoraggio, analisi e risposta, al fine di prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia e con la possibilità di promuovere iniziative di partenariato pubblico-privato funzionali allo scopo (art. 7, c. 1, lett. n). In parti-

[27] Ancora L. Parona, *L'istituzione*, cit.

colare, la gestione e mitigazione del rischio in materia di cybersicurezza appartengono all'Obiettivo Strategico "Risposta", che vede tra gli attori principali l'ACN, il Nucleo per la Cybersicurezza e il CSIRT Italia.

In aggiunta, l'ACN è incaricata di curare e promuovere «la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo conto anche degli orientamenti e degli sviluppi in ambito internazionale» ed esprimersi attraverso pareri non vincolanti sulle iniziative di leggi o regolamenti attinenti alla sicurezza cibernetica (art. 7, c. 1, lett. p)[28].

Da un punto di vista delle funzioni sostanziali non può non menzionarsi l'art. 7, c. 1 lettera m-*bis*, la quale dispone che l'Agenzia «assume le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, anche attraverso un'apposita sezione dedicata nell'ambito della strategia di cui alla lettera b)».

La valorizzazione della crittografia viene spiegata, nella medesima disposizione, come parte di una generale attività dell'Agenzia rispetto ad «ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali».

Dal momento che la strategia è disponibile, è possibile verificare che la crittografia rientra nell'Obiettivo Strategico "Protezione" – al cui vertice è collocata l'ACN – i cui beneficiari sono individuati nelle istituzioni, negli operatori privati e nella società civile, dunque, la platea più ampia che la strategia stessa ammette. Altresì, la strategia specifica che la promozione dell'uso della crittografia "come strumento di cybersicurezza" si sostanzia nel favorire un impiego di questa – nella sua tipologia commerciale - lungo tutto il ciclo di vita di prodotti, sistemi e servizi ICT, essendo contestualmente esplicitata l'intenzione dell'Agenzia di sviluppare tecnologie e sistemi di cifratura nazionale.

Sul versante delle funzioni e ruoli dell'Agenzia a livello di cooperazione internazionale ed europea, l'art. 7 offre un quadro più che esteso[29]. Infatti, oltre che al già menzionato ruolo di autorità nazionale competente NIS punto di contatto unico, l'ACN è designata quale Centro nazionale di coordinamento ai sensi dell'art. 6 del regolamento (UE) 2021/887 che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento (art. 7, c. 1, lett. aa), il cui rappresentante nazionale (e sostituto) sono nominati con decreto del Presidente del Consiglio dei ministri.

Da un punto di vista funzionale, l'ACN è deputata a partecipare alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese (art. 7, c. 1, lett. o) e a coordinare, in raccordo con il Ministero degli Affari Esteri e della Cooperazione Internazionale, la cooperazione internazionale in materia di cybersicurezza. In aggiunta, l'Agenzia ha in carico la cura dei rapporti con organismi, istituzioni ed enti competenti e monitorare le tematiche di cybersicurezza, ferme le competenze che già sono attribuite dalla legge ad altre amministrazioni, con le quali comunque l'Agenzia è tenuta ad operare in raccordo per garantire l'uniformità e la coerenza delle posizioni nazionali con le politiche di cybersi-

[28] Ancora I. Forgione, *Il ruolo*, cit.

[29] Ci si permette di rinviare ai saggi contenuti in C. Cavaceppi-A. Contaldo (a cura di), *Cybersecurity*, cit.

curezza definite dal Presidente del Consiglio dei Ministri (art. 7, c. 1, lett. q).
L'Agenzia può altresì stipulare accordi bilaterali e multilaterali, anche coinvolgendo il settore privato e industriale, con istituzioni, enti ed organismi di altri paesi (art. 7, c. 1, lett. s) ed è incaricata di garantire promozione, sostegno e coordinamento alla partecipazione italiana a progetti e iniziative dell'UE e internazionali nel campo della cybersicurezza (art. 7, c. 1, lett. t). Tali funzioni trovano tutte il proprio limite nelle competenze di altre amministrazioni, con cui l'ACN deve sempre assicurare il relativo raccordo, e del MAECI. Da sottolineare il rilievo dell'ultimo capoverso dell'art. 7, c. 1, lett. t), che specifica che la necessarietà del raccordo anche con il Ministero della Difesa per «per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia Europea per la Difesa».

5. Brevi conclusioni: il cyberspazio come non luogo di intervento dello Stato per la funzione di "pubblica sicurezza digitale"

Il cyberspazio appare così come una sorta di non luogo di progettazione matematica in cui oramai si svolgono molte attività umane aventi anche rilevanza economica e finanziaria[30]. Lo Stato pertanto deve attivarsi per garantirvi soprattutto la funzione di Pubblica sicurezza nel cyberspazio[31], che in riferimento alle attività di governo statale e di livello centrale e locale necessitano di un complesso di apparati, autorità e strutture preposte alla tutela dell'ordine pubblico e all'incolumità delle persone. Tali soggetti sono preposti al fine di garantire un minimo grado di sicurezza per i cittadini di uno Stato, per fronteggiare emergenze e gravi necessità collettive, nell'obiettivo dell'incolumità pubblica, e per garantire l'ordine pubblico.
Il grado di sicurezza percepito dalla popolazione fornisce un notevole contributo alla stabilità economica e all'attrattività di un paese, alla produttività dei cittadini e in conclusione al successo economico di una nazione.
La pubblica sicurezza nel cyberspazio riguarda perciò tanto le attività di polizia, volte ad assicurare la "sicurezza" attraverso il rispetto delle norme di legge, quanto quelle comunque finalizzate a "prevenire" che la comunità possa patire danni da eventi fortuiti e accidentali, infortuni e disastri di qualunque altro genere[32], o comunque a prevenirne l'aggravio del danno, attraverso l'organizzazione di forme di prevenzione.
Il costante espresso riferimento normativo, che si traduce in una frequente citazione della locuzione a fini amministrativi e burocratici, ha inoltre segnalato il pesante sbilanciamento ordinamentale verso una preminenza delle funzioni di polizia nelle attività di preservazione della pubblica sicurezza[33]. In particolare, gli interventi legislativi straordinari atti a potenziare le attività di pubblica sicurezza in materia di contrasto al terrorismo internazionale hanno posto l'accento sullo sviluppo delle capacità di inda-

[30] Ancora S. Pietropaoli, *Informatica*, cit. 81 ss.

[31] Vedi R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in Idem (a cura di), *La sicurezza*, cit., 7 ss.

[32] *Ibid.*

[33] Vedi P. Vipiana, *Introduzione*, cit., 131 ss.; R. Ursi, *La sicurezza pubblica*, cit., 182 ss.

gine e prevenzione e sull'aumento e la diversificazione delle forze in campo, ma sono riuscite solo marginalmente nel compito di migliorare il coordinamento degli organi di pubblica sicurezza nazionali.