RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0142 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Marina Pietrangelo

Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa

L'Autrice è primo ricercatore presso l'IGSG/CNR

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. Premessa

Il disegno di legge AC 1717 *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* d'iniziativa governativa (Presidente del Consiglio Meloni e Ministro della Giustizia Nordio) è stato depositato alla Camera dei deputati il 16 febbraio 2024 ed è attualmente all'esame di merito delle Commissioni riunite Affari costituzionali e Giustizia. La proposta interviene su un quadro regolatorio complesso, risultato della stratificazione di numerose fonti interne ed eurounionali, e prossimo ad essere ulteriormente novellato dalla *Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (cosiddetta "direttiva NIS 2")*. La delega per l'adozione del decreto legislativo di recepimento della NIS 2 è nella legge di delegazione europea 2022-2023 (cfr. l'art. 3, l. 21 febbraio 2024, n. 15, *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2022–2023)*. Di tale direttiva – che ha innovato significativamente le norme pregresse e di cui si attende il recepimento in ottobre – il disegno di legge governativo anticipa alcune misure, senza tuttavia prevedere forme di raccordo con essa. L'intervento proposto risulta quindi asincrono, e rischia di produrre ulteriore incertezza.

2. Sui tratti generali del ddl

A prima lettura, il progetto legislativo sembra presentare più d'una criticità tanto sotto il profilo sostanziale, che sconfina inevitabilmente ben oltre la cybersicurezza in senso stretto (che è «l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche», secondo la definizione dell'art. 1, co. 1, n. 1, *Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza,*

e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013; ripresa in art. 1, co. 1, lett. a), *d.l. 14 giugno 2021, n. 82 recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, conv. con modifiche nella legge n. 109/2021), che sotto quello parimenti rilevante – e al primo strettamente embricato – del modello regolatorio.

La proposta è costruita attorno a due distinte aree di intervento: la prima insiste specialmente sulla cybersicurezza delle amministrazioni pubbliche e sulla governance di settore; la seconda contiene misure di carattere penale. La prima coincide col Capo I (artt. 1-10) intitolato "Disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la cybersicurezza nazionale. Nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici"; la seconda col Capo II (artt. 11-18) recante "Disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi ai sistemi informatici e telematici".

Nel paragrafo successivo saranno esaminate più in dettaglio alcune disposizioni del Capo I, che potrebbero porre problemi sotto il profilo della sostenibilità amministrativa e più in generale in termini di leale collaborazione tra gli enti interessati dalla nuova normativa. Prima però di addentrarci nello specifico di queste previsioni, qualche notazione di carattere generale. Anzitutto, l'articolato nel suo complesso tradisce l'idea di un irrobustimento della cybersicurezza che si esprime attraverso una verticalizzazione della relativa governance, con un ulteriore accentramento di poteri e funzioni nell'apparato governativo dello Stato. A tenore della proposta, infatti, l'endiadi legislativa "sicurezza e resilienza" delle amministrazioni pubbliche parrebbe assicurata esclusivamente mediante un nuovo rilevante carico di prescrizioni, anche laddove vi fossero margini di collaborazione funzionali a garantire l'interesse alla sicurezza cibernetica come interesse nazionale, comune e condiviso dalle istituzioni della Repubblica (per una cybersicurezza cooperativa). Su questo profilo si dirà meglio più avanti, poiché tale approccio emerge con speciale nitidezza dall'impostazione del Capo I, che impone alle pubbliche amministrazioni centrali e del sistema delle autonomie tutta una serie di obblighi di notifica degli incidenti informatici e di risoluzione delle vulnerabilità "potenziali" nei dati e sistemi di loro pertinenza, "tratti" dalla NIS 2, ma declinati in senso fortemente prescrittivo. Non dissimile, sempre sotto il profilo sostanziale, la linea riformatoria del Capo II, improntato al medesimo rigore prescrittivo, espresso anzitutto attraverso l'inasprimento delle pene edittali per i crimini informatici, in un disegno complessivo che peraltro tradisce la rappresentazione di una criminalità informatica 1.0.

Con riguardo al modello regolatorio, come anticipato sopra e specie in relazione al Capo I, una delle maggiori criticità della proposta discende dalla scelta di una fonte ordinaria – apprezzabile "solo" se comparata con la pregressa modalità di regolare la materia per decretazione d'urgenza – che però si muove su piani diversi: in alcuni casi novella le norme previgenti (es. i d.l. convertiti), in altri introduce disposizioni formalmente sganciate dalla regolazione di settore (es. l'art. 10 in tema di appalti). Nessuna misura di coordinamento o previsione di riordino, che auspicabilmente dovrà arrivare col decreto di recepimento della NIS 2. Non è più rinviabile, infatti, una qualche attività manutentiva, un codice (almeno ricognitivo); su tale profilo sembra in parte aprire la delega (art. 3, co. 1, lett. p), legge n. 15/2024: «apportare alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il coordinamento con le disposizioni emanate in attuazione del presente articolo»). Sempre sotto il più generale profilo regolatorio, mancano due clausole essenziali: una prima, col regime transitorio, almeno in relazione ai nuovi oneri e obblighi di cui al Capo I; e una seconda, con la copertura finanziaria. L'intero progetto non è credibile se non si individuano risorse adeguate. In tal senso, in vista della predisposizione della nuova legge di bilancio è opportuno legare le misure del ddl al rifinanziamento dei due fondi sulla cybersicurezza (istituiti con la legge di bilancio per il 2023 – l. 29 dicembre 2022, n. 197, art. 1, co. 899): il "Fondo per l'attuazione della Strategia nazionale di cybersicurezza", per gli investimenti finalizzati all'autonomia tecnologica in ambito digitale e all'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali (lett. a); e

il "Fondo per la gestione della cybersicurezza", per finanziare le attività di gestione operativa dei progetti. Infine, si fa particolarmente notare l'assenza di una valutazione d'impatto di alcune delle nuove misure. È pur vero che essa non è prescritta per le proposte in materia di "sicurezza interna ed esterna dello Stato" (che rientra tra i casi di esclusione di cui all'art. 6, co. 1, lett. c), d.P.C.M. 15 settembre 2017, n. 169), ma il Consiglio dei Ministri (o le Commissioni parlamentari poi) avrebbe ben potuto richiederla ai proponenti. Si tratta certamente di una pratica residuale, se non addirittura di un'ipotesi di scuola. Ma certamente una indicazione realistica degli impatti attesi su cittadini, imprese e pubbliche amministrazioni e una effettiva comparazione delle eventuali opzioni regolatorie considerate avrebbero conferito nel merito alla proposta legislativa maggiore qualità. Tenuto conto poi che nel nostro ordinamento nazionale manca una legge annuale sulla transizione digitale, sul modello delle altre leggi periodiche, che potrebbe agevolare il monitoraggio dello stato di attuazione delle norme di settore e la programmazione degli interventi attuativi. In definitiva, quindi, una valutazione pur se minima avrebbe senz'altro rafforzato la "credibilità" dell'intero progetto.

3. Sulla sostenibilità amministrativa (Capo I)

Veniamo ora all'esame più in dettaglio di alcune disposizioni del Capo I, che – come anticipato – potrebbero porre problemi sotto il profilo della sostenibilità amministrativa e più in generale in termini di leale collaborazione tra gli enti interessati dalla nuova normativa. Tra gli altri, destano interesse gli articoli 1 e 2, che estendono alle pubbliche amministrazioni l'ambito di applicazione delle misure di cybersicurezza, di fatto anticipando nel merito il d.lgs. di recepimento della NIS 2. Nello specifico, tali disposizioni introducono obblighi di notifica degli incidenti significativi e di adeguamento alle segnalazioni dell'Agenzia per la cybersicurezza nazionale (ACN), tra gli altri, a carico di regioni e province autonome, comuni con popolazione superiore ai 100.000 abitanti, comuni capoluogo di regione, società di trasporto pubblico con numero di utenti non inferiore a 100.000, aziende sanitarie locali. Tali enti saranno tenuti a notificare gli incidenti informatici che impattano su reti, sistemi e servizi di propria pertinenza, secondo meccanismi di controllo e sanzione (dalla sanzione amministrativa alla responsabilità disciplinare o contabile) gestiti dall'ACN, i cui ulteriori poteri ispettivi non sono precisati, ma verranno declinati con provvedimento del suo direttore. Si ricorda qui che la platea degli incidenti è molto ampia, ricomprendendo tutti gli eventi di natura accidentale o intenzionale che causano malfunzionamento, interruzione (anche parziale) e utilizzo improprio di reti, sistemi informativi o servizi informatici (così l'art. 1, co. 1, lett. h), d.P.C.M. 14 aprile 2021, n. 81). L'art. 2 del ddl disciplina gli obblighi di adeguamento a «segnalazioni puntuali» dell'ACN «circa specifiche vulnerabilità a cui essi risultino potenzialmente esposti», mediante l'adozione al più tardi entro quindici giorni dalla comunicazione delle misure richieste, anche qui con la previsione di oneri informativi e sanzioni per inosservanza. In entrambi i casi, si tratta di misure legislative che possono porre problemi di compatibilità in termini di ordinamento e autonomia organizzativa degli enti ad esse sottoposti, laddove la protezione della sicurezza nazionale rischia di sconfinare nell'autonoma gestione dei sistemi e servizi informativi, veri e propri strumenti di governo delle amministrazioni regionali. Mancando gradualità, tali prescrizioni stridono con l'impostazione cooperativa, verso l'alto e verso il basso, che è determinante per il rafforzamento della cybersicurezza e della resilienza informatica complessiva del sistema Paese. Ciò anche in considerazione del fatto che l'approccio alla sicurezza informatica è un approccio multi rischio, che mira cioè a proteggere dagli incidenti i sistemi informatici e di rete, ma anche il loro ambiente fisico.

Più in particolare, le disposizioni citate chiamano in causa anche aspetti di coordinamento tecnico-informatico, che imporrebbero un approccio condiviso e collaborativo quantomeno con le amministrazioni regionali, nell'ottica di "concorrere" alla definizione del percorso legislativo sulle misure organizzative e strumentali per il rafforzamento della resilienza digitale (per una declinazione della soluzione del "concorso di competenze" in tema di coordinamento orizzontale dei sistemi informativi di amministrazioni statali e regionali, tra le altre, v. Corte cost. n. 50/2005). La questione della base giuridica viene in rilievo proprio in considerazione del carico regolatorio e del meccanismo sanzionatorio previsto dal ddl, che mal

si attaglia alla garanzia della sicurezza nazionale come esigenza anche di unità e indivisibilità di una Repubblica coesa e più (cyber)sicura. Si ricorda al proposito che a partire dal 2005 le regole sulla sicurezza dei sistemi informativi sono state ricondotte agli interventi statali di coordinamento tecnico-informatico che servono a definire le regole tecniche necessarie "per garantire la *sicurezza* (corsivo aggiunto) e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime" (v. l'art. 14, d.lgs. 7 marzo 2005, n. 82). Come noto, questo coordinamento è oggi affidato a una agenzia della Presidenza del Consiglio, che progetta e monitora l'evoluzione strategica dell'intero sistema informativo pubblico, puntando su infrastrutture e standard comuni o condivisi "che riducano i costi sostenuti dalle amministrazioni e migliorino i servizi erogati" (cfr. *Piano triennale per l'informatica pubblica 2024-2026* cit., p. 10). Con un approccio alla transizione digitale che sin dalle origini considera il sistema informativo pubblico come unitario, strutturato come architettura policentrica e federata, e che oggi risponde peraltro al principio del cloud-first. Un modello in cui stride particolarmente quindi la previsione di interventi verticali posti interamente a carico delle amministrazioni, alle quali non sono destinate risorse specifiche (se si eccettuano quelle "eccezionali" del PNRR già veicolate agli enti mediante gli avvisi dell'ACN). Un vulnus ricorrente in tutte le riforme sulla digitalizzazione pubblica adottate nei decenni passati.

Sotto il profilo della sostenibilità amministrativa, merita attenzione anche l'articolo 6 che disciplina il "rafforzamento della resilienza delle pubbliche amministrazioni". Esso prevede l'istituzione di una nuova "struttura preposta alle attività di cybersicurezza" (co. 1), che potrà essere individuata anche tra quelle esistenti. Al proposito, occorre ricordare che non poche sono le figure che insistono sull'area delle attività connesse al settore digitale: tra queste, il responsabile per la trasparenza, il responsabile per la protezione dei dati personali, il responsabile per la transizione digitale. Quest'ultimo presidia una struttura già normata e dunque l'introduzione di una nuova e autonoma struttura costituirebbe un aggravio organizzativo; sarebbe quindi auspicabile ricondurre ad essa le attività del nuovo referente per la cybersicurezza. Alla nuova struttura sono assegnati compiti sia di indirizzo (v. lett. a): "sviluppo delle politiche"; lett. d): "produzione di un piano programmatico per la sicurezza") sia di carattere tecnico altamente specializzato (v. lett. g): monitoraggio e valutazione continua delle minacce informatiche"). Non sono meglio precisate le competenze del referente per la cybersicurezza, figura peraltro già prevista nell'ultimo "Piano triennale per l'informatica nella PA 2022-2024" adottato dall'Agenzia per l'Italia digitale, a cui quindi la disciplina legislativa nulla aggiunge a proposito dei requisiti professionali. In ogni caso, qualora la competenza fosse altamente specializzata – per ora si può solo intuire – non sarebbe scontato né immediato reclutarla all'interno delle amministrazioni. Al riguardo, oltre al raccordo con le funzioni delle altre strutture menzionate, sarebbe auspicabile la previsione di una fase transitoria e di una "clausola formativa" per programmare un percorso di formazione del personale interno. Frattanto, per far fronte tempestivamente ai numerosi obblighi di legge potrebbe essere consentito il ricorso a figure esterne (come per il Data Privacy Officer) o a un team esterno coordinato da un referente interno all'amministrazione. Una ulteriore soluzione per consentire alle amministrazioni di rispettare le nuove prescrizioni potrebbe essere l'esercizio in forma associata, specie per gli enti di minori dimensioni, o l'affidamento a società in house. Tale ultima ipotesi è stata introdotta di recente anche per lo svolgimento delle attività del referente per la transizione digitale (cfr. l'art. 17, co. 1-*septies*, d.lgs. n. 82/2005), modificato dal d.l. n. 19/2024). Sulle società in house, su cui gravano gli stessi obblighi di notifica e adeguamento previsti dagli artt. 1 e 2, occorrerebbe poi sviluppare nel ddl una disposizione autonoma (un comma aggiuntivo), che precisi la formula opaca "rispettive società in house" inserita in coda all'elenco delle pubbliche amministrazioni obbligate, dettagliando anzitutto i settori merceologici di attività su cui insistono i servizi da esse erogati.

Infine, a proposito di sistema integrato di cybersicurezza, si sottolinea l'assenza di un espresso e chiaro riferimento ai team di risposta agli incidenti di sicurezza informatica (CSIRT) istituiti a livello regionale nell'ambito della struttura nazionale CSIRT Italia (cfr. l'art. 8, d.lgs. 18 maggio 2018, n. 65), che invece potrebbero costituire un raccordo ulteriore con l'istituenda nuova struttura

regionale, ponendosi al contempo come interlocutori degli enti locali: un livello intermedio tra la regione e l'ACN. Tema questo presente nella delega per il recepimento della NIS 2 in cui si prevede di sviluppare e rafforzare la «collaborazione tra tutte le strutture pubbliche con funzioni di Computer Emergency Response Team (CERT) coinvolte in caso di eventi malevoli per la sicurezza informatica» (art. 3, co. 1, lett. e), legge n. 15/2024). Resta poi sullo sfondo la natura giuridica del CSIRT regionale, per chiarire il rapporto con gli enti regionali (le misure organizzative e le risorse) e standardizzare il procedimento costitutivo.

Per concludere su questi profili, una struttura così complessa avrebbe imposto anzitutto una valutazione della sostenibilità amministrativa, che manca nella documentazione a corredo dell'atto, ma – come detto sopra – avrebbe giovato alla definizione di misure per molta parte "rimesse" quindi nel breve periodo alla capacità o incapacità dei singoli enti.

4. Nota finale sulla governance

Dal quadro sopra appena tratteggiato, e da altre disposizioni del ddl qui non approfondite, pare delinearsi anche una rinnovata governance della cybersicurezza, sempre più imperniata sulle (sole) agenzie governative della Presidenza del Consiglio. L'ACN acquisterebbe poteri in materia di cybersicurezza più penetranti di natura accertativa e sanzionatoria, ma anche nuove funzioni in relazione per esempio allo sviluppo delle applicazioni di intelligenza artificiale (IA) quale "risorsa per rafforzare la cybersicurezza" (art. 7, co. 1). Un innesto che trova ampio seguito anche nel draft del ddl governativo sull'intelligenza artificiale (approvato dal Consiglio dei Ministri il 23 aprile 2024) nel quale la cybersicurezza è indicata come "precondizione essenziale" dell'IA e l'ACN si troverebbe a condividere con l'Agenzia per l'Italia digitale il ruolo di Autorità nazionale per l'intelligenza artificiale (art. 18). Anche le attività di coordinamento e raccordo con le amministrazioni pubbliche e le autorità indipendenti, pure previste (al comma 2 dell'art. 18), sono appannaggio della Presidenza del Consiglio presso cui si prevede di costituire un apposito Comitato di coordinamento, che sarà appunto interno alla Presidenza e si comporrà dei direttori delle due Agenzie e del Capo del Dipartimento PCM per la trasformazione digitale. Questa linea parrebbe confermare quell'approccio accentratore e verticalizzante di cui si è detto al principio a proposito del ddl 1717. Resta fermo che per meglio valutare gli esiti di entrambe le proposte legislative occorrerà attendere che si concluda l'esame parlamentare appena avviato.