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

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0145 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Matteo Giannelli

Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza

L'Autore è ricercatore a tempo determinato di Diritto costituzionale nell'Università degli Studi di Firenze

La ricerca è stata svolta nell'ambito del Progetto PNRR "Partenariato Esteso" *SERICS - SEcurity and RIghts in the CyberSpace, Spoke 1 – Cyberights* (CUP B83C22004830007), finanziato dall'Unione europea - Next Generation EU.

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. Il disegno di legge di iniziativa governativa recante *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* (A.C. 1717) in discussione presso la Camera dei deputati ha l'obiettivo di consolidare sia la risposta penale alle minacce alla sicurezza informatica quanto la resilienza della pubblica amministrazione. Sotto quest'ultimo profilo le disposizioni contenute nel testo rispondono a due necessità che si sono manifestate sempre di più negli ultimi anni: da un lato, far emergere in modo puntuale e tempestivo la minaccia informatica diretta ai soggetti della pubblica amministrazione non compresi nel Perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge 21 settembre 2019, n. 105; dall'altro, costituire una sorta di anticipazione a livello nazionale in vista dell'attuazione nel nostro ordinamento della Direttiva (UE) 2022/2555 (c.d. NIS 2), il cui termine per il recepimento da parte degli Stati membri scadrà il prossimo 17 ottobre 2024.

Sul punto occorre preliminarmente ricordare che ai sensi dell'art. 2, par. 5, della Direttiva, le nuove disposizioni si applicano agli enti della pubblica amministrazione a livello centrale, mentre in sede di attuazione i singoli Stati membri decideranno se estenderle anche agli enti a livello regionale e locale. Completano il quadro i paragrafi 6 e 7 del medesimo articolo che, rispettivamente, lasciano impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato e prevedono l'esclusione degli enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati.

Da questa breve rassegna normativa dovrebbe risultare evidente come l'attuazione della Direttiva comporti moltissimi problemi di coordinamento, che possono minare l'efficacia e il risultato atteso dal legislatore europeo e nazionale. Problemi, in una certa misura inevitabili poiché strettamente connessi ai fenomeni di integrazione – non solo

normativa – tra ordinamenti ma che devono esser messi in luce con la dovuta attenzione. In questo breve contributo verranno affrontati, sia consentito l'utilizzo del termine, solamente quelli verso "il basso" (riferiti dunque ai livelli di governo substatali) e, almeno direttamente, non quelli "verso l'alto" (riferiti al tema della sicurezza nazionale e alle sue declinazioni).

2. Le disposizioni contenute nel Capo I si inseriscono nel variegato panorama normativo concernente i temi della sicurezza informatica e dello spazio digitale nel nostro ordinamento, attraverso una serie di misure appositamente congegnate per garantire la resilienza intesa quale capacità di una rete o di un sistema di mantenere la funzionalità e di adattarsi, preservando le proprie caratteristiche, in risposta ad attacchi, perturbazioni o crisi in coordinamento con le autorità competenti. Un panorama che si comporrà definitivamente con l'entrata in vigore dei decreti delegati previsti dell'articolo 3 della legge 21 febbraio 2024, n. 15, "Legge di delegazione europea" e che, come detto, dovranno essere emanati entro il 17 ottobre 2024 con riferimento al recepimento della Direttiva NIS 2.

Nel definire il contenuto di tali decreti il Governo, in raccordo con l'Agenzia per la Cybersicurezza Nazionale (ACN), dovrà «individuare i criteri in base ai quali un ente pubblico può essere considerato pubblica amministrazione ai fini dell'applicazione delle disposizioni della direttiva (UE) 2022/2555, anche considerando la possibilità di applicazione della direttiva medesima ai comuni e alle province secondo principi di gradualità, proporzionalità e adeguatezza» (art. 3, co. 1, lett. a). Dovrebbe a questo punto risultare chiaro il collegamento con il ddl in commento e, in particolare con gli articoli 1, 2, 8 e 13, che, occupandosi anche dei livelli regionali e locali, chiedono al legislatore una visione d'insieme per evitare che nuove disposizioni e i connessi obblighi rimangano sulla carta o, ipotesi peggiore, si risolvano in un fattore di confusione dell'intero sistema.

Una consapevolezza che sembra confermata dalla lettura nell'analisi tecnico-normativa dell'A.C. 1717 (supplemento, pag. 15) dove alla voce *Analisi delle compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali* è possibile leggere che «le disposizioni proposte con il Capo I del presente disegno di legge rientrano tra le materie riservate in via esclusiva allo Stato e, in particolare, tra quelle indicate dall'articolo 117, secondo comma, lettera d), della Costituzione. Non si ravvisano, pertanto, profili di incompatibilità con le competenze e le funzioni delle regioni ordinarie e a statuto speciale, nonché degli enti locali. Tuttavia, in considerazione della incidenza di talune disposizioni previste dal provvedimento – in particolare, gli articoli 1, 2, 6 e 10 – sulle attività delle pubbliche amministrazioni anche locali, sarà necessario un confronto ed un raccordo operativo con i richiamati soggetti in relazione all'attuazione di tali disposizioni». Ancora alla successiva voce *Verifica della compatibilità con i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione* si legge che «le disposizioni contenute nell'intervento esaminato sono compatibili e rispettano i principi di cui all'articolo 118 della Costituzione, in quanto non prevedono né determinano, sia pure in via indiretta, nuovi o più onerosi adempimenti a carico degli enti locali».

Dalla prima affermazione appena riportata sembra emergere chiaramente, specie dal periodo conclusivo, un comune consenso in merito alla circostanza che l'imposizione agli enti locali e regionali di vincoli in materia di cybersicurezza, implichi necessariamente un coordinamento e un concreto supporto volto alla realizzazione di condizioni effettive di resilienza cibernetica. Qualche perplessità si ricava, invece, dalla seconda voce soprattutto con riferimento all'assenza di oneri indicata nella parte finale e che sembra ignorare che uno dei problemi principali della cybersicurezza è quello dei costi, non solo sotto il profilo degli attacchi e delle loro conseguenze ma anche sotto quello, preliminare – o meglio preventivo – della *compliance* dei soggetti pubblici e privati.

3. A questo punto occorre chiedersi in che modo il testo delle disposizioni del ddl rilevanti ai fini della presente trattazione intendono affrontare e risolvere le questioni emerse. L'art. 1 nel prevedere un più ampio obbligo di notifica di incidenti rilevanti per la cybersicurezza per soggetti ulteriori rispetto a quelli già ricompresi nel perimetro di sicurezza nazionale cibernetica e l'articolo 8 nell'occuparsi del rafforzamento della resilienza delle pubbliche amministrazioni e dell'individuazione del referente per la cybersicurezza sembrano trascurare una fattiva collaborazione con gli enti locali e regionali. Una cooperazione che si dovrebbe basare

sul modello CSIRT (*Computer Security Incident Response Team*) – oggetto di parziale intervento nell'articolo 21 – che, ad oggi, costituisce l'ambito privilegiato per identificare i problemi, per offrire una risposta coordinata agli incidenti informatici, per realizzare uno scambio di buone pratiche – come sollecitato in più punti anche dalla Direttiva NIS 2 a partire dell'art. 15 – e, in definitiva, incentivare il rispetto delle disposizioni in materia.

Sembra mancare un riferimento alla possibilità per le Regioni e le province autonome, sulla base di accordi con l'Agenzia per la cybersicurezza nazionale, di istituire CSIRT regionali operanti in raccordo con lo CSIRT nazionale. Una previsione che, peraltro, sarebbe in linea con quanto previsto nella Strategia Cyber nazionale e nelle progettualità in ambito PNRR (Misura 1 investimento 1.5), che prevedono appunto l'istituzione di CSIRT di livello regionale, come sta avvenendo in alcuni contesti territoriali, anche grazie al contributo dei diversi enti, anche non territoriali (si pensi ad esempio al contributo delle Università). Inoltre, l'organizzazione e le attività degli CSIRT regionali costituendo elementi di carattere strategico dovrebbero essere oggetto di intesa in sede di Conferenza Stato-Regioni per garantire la massima condivisione tra livello centrale e livello periferico e favorire meccanismi di raccordo con le Regioni da parte dell'Agenzia per la Cybersicurezza Nazionale ad oggi molto limitati.

In termini più generali, l'impianto delle disposizioni appare analogo ad altre che presentano il classico schema adempimento-sanzione. Una circostanza auto evidente nel Capo II per il versante penalistico ma riscontrabile anche nel capo I, quasi a testimoniare la preminenza di un modello sull'altro a scapito di una concezione (anche) promozionale della sicurezza nel modo digitale. Si tratta di un approccio che si scontra con l'esigenza operativa di intervento richiesta dalle norme in materia di cybersicurezza e, di conseguenza, con la successiva messa in atto degli adempimenti. L'introduzione di un Referente per la cybersicurezza in ogni Amministrazione dimostra un'attenzione alle nuove sfide presentate dalla disciplina anche se, tuttavia, la semplice presenza di figure di riferimento, peraltro in assenza di una chiara definizione del loro livello di inquadramento, non appare sufficiente a garantire i risultati. Diviene, dunque, fondamentale che il livello a centrale, a partire dall'Agenzia per la Cybersicurezza Nazionale, oltre a introdurre novità normative, lavori a stretto contatto con i Referenti nelle varie amministrazioni per garantire che i compiti pianificati siano effettivamente realizzati e che vi sia un chiaro processo di monitoraggio e valutazione dei risultati ottenuti, affiancandoli nell'implementazione di strategie operative e di procedure. In coerenza con l'obiettivo di rendere la cybersicurezza una priorità, vista la natura trasversale e pervasiva della stessa rispetto alla ormai totalità dei servizi di funzionamento delle amministrazioni, ai processi digitalizzati e ai servizi erogati, dovranno esser adottate misure in grado di incidere efficacemente e tempestivamente. Tra le ipotesi, potrebbero esser introdotti pareri obbligatori da parte del Referente per la cybersicurezza su diverse categorie di atti dell'ente e la possibilità di emanare linee guida e raccomandazioni interne, in coordinamento con gli organi previsti dalla normativa vigente.

La configurazione della figura del Referente che si ricava dall'art. 8 sembra essere difficilmente conciliabile con questa impostazione. Sullo sfondo di questa vicenda non bisogna dimenticare le crescenti difficoltà delle amministrazioni nel reclutare specialisti ICT dotate di competenze avanzate specifiche in ragione di una diffusa carenza nel mercato, non solo pubblico ma anche privato, delle competenze ICT e, in particolare, di formazione nel campo della cybersicurezza. Una circostanza che potrebbe tradursi in una potenziale criticità nell'individuazione delle risorse umane previste dall'articolo 8, comma 1 e 2, e che potrebbe comportare, come avvenuto per i Responsabili per la Transizione digitale (RTD) di cui Decreto legislativo 7 marzo 2005 n. 82 (Codice dell'Amministrazione Digitale – CAD), l'individuazione di personale privo delle necessarie competenze e un conseguente mancato rafforzamento delle Amministrazioni.

Una lacuna a cui si è posto parzialmente rimedio attraverso alcune modifiche al testo apportate in sede referente dalle Commissioni riunite Affari Costituzionali e Giustizia. Al fine di agevolare in particolare gli enti di minori dimensioni o quelli che utilizzano sistemi informativi erogati dalle società in house o dalla Regione come soggetto aggregatore, è stata introdotta la possibilità che il ruolo di referente sia svolto da un dipendente di un'altra pubblica amministrazione nel caso in cui non vi siano dipendenti dotati specifiche

professionalità e competenze (comma 2) oppure che sia possibile una nomina associata (comma 4), in analogia a quanto previsto dall'art. 17, comma 1-*septies* del citato CAD che prevede anche la possibilità di esercitare le funzioni di RTD in forma associata. Tale previsione, peraltro, potrebbe rispondere all'ampliamento dell'ambito soggettivo di applicazione della Direttiva 2022/2555 NIS 2 con riferimento ai soggetti pubblici. Di ulteriore interesse è il comma 5, anch'esso introdotto in sede referente, che attribuisce all'Agenzia per la Cybersicurezza Nazionale la possibilità di individuare le modalità e i processi di coordinamento e collaborazione, anche di livello regionale, tra le amministrazioni individuate all'articolo 1, comma 1, e i referenti appena descritti al fine di facilitare la resilienza delle amministrazioni pubbliche.

Nella direzione di un difficile coordinamento in fase di risposta alle minacce sembra muoversi l'articolo 2, comma 1, del ddl quando prevede che le amministrazioni, gli enti pubblici e altri soggetti che forniscono servizi pubblici, qualora siano oggetto di segnalazioni dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultano potenzialmente esposti, debbano provvedere tempestivamente all'adozione degli interventi risolutivi indicati dalla stessa Agenzia. Dal momento che tale previsione prevede applicazione di sanzioni per inadempimento, l'utilizzo del termine "potenzialmente" sembra rischioso per la concreta possibilità di far ricadere in questa fattispecie non solo segnalazioni puntuali proveniente dall'Agenzia ma anche quelle su cui non ci sono, e non sono verificabili, effettive evidenze di rischio da parte del soggetto pubblico che riceve tale segnalazione.

Un'ultima postilla riguarda la previsione, apparentemente marginale, contenuta nell'articolo 11, comma 1, dove sono definiti tempi e modalità per l'adozione del regolamento che stabilisce termini e disposizioni operative per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia. Nella disposizione si precisa che il regolamento può essere adottato «anche in deroga all'art. 17 della legge 23 agosto 1988, n. 400». Quest'ultimo inciso è stato introdotto in sede referente e sarà solo la prassi a dimostrarne l'efficacia, anche se in situazioni analoghe tale previsione non è apparsa sufficientemente apprezzabile. Sul punto è possibile in termini generali osservare che la deroga al procedimento di formazione dei regolamenti previsto in via generale dall'art. 17 della legge 400 del 1988 possa costituire, come avvenuto in particolare a partire dalla Riforma del Titolo V, una potenziale fattore contrastante il riparto di competenze tra Stato e Regioni previsto dall'articolo 117, comma 6, della Costituzione.

Riferimenti bibliografici

E. Longo (2024), La disciplina della Cybersicurezza nell'Unione europea e in Italia, in F. Pizzetti et al. (a cura di), "La regolazione europea della società digitale", Giappichelli, 2024.

S. Poletti (2023), *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, in "MediaLaws", 2023, n. 2

S. Rossa (2023), *Cybersicurezza e Pubblica Amministrazione*, Editoriale Scientifica, 2023

R. Ursi (2023), *La sicurezza cibernetica come funzione pubblica*, in Id. (a cura di), "La sicurezza nel cyberspazio", FrancoAngeli, 2023