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

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0147 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Pier Giorgio Chiara

DDL Cybersicurezza: tra l'inasprimento della risposta penale del legislatore nazionale e il modello preventivo-amministrativo della direttiva NIS2

L'Autore è assegnista di ricerca in informatica giuridica dell'Università di Bologna, CIRSFID ALMA-AI

La ricerca è stata svolta nell'ambito del Progetto PNRR "Partenariato Esteso" *SERICS - SEcurity and RIghts in the CyberSpace*, *Spoke 8 - Ecocyber* (CUP J33C22002810001), 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

I. Il disegno di legge recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, c.d. DDL Cybersicurezza (da qui in avanti, 'DDL'), presentato il 16 febbraio 2024, consta di due capi, che individuano le due anime principali di questo provvedimento legislativo. Se il capo I individua norme di "cyber resilienza", volte ad elevare, cioè, la capacità di protezione e risposta di fronte a minacce cibernetiche in costante evoluzione, crescita e sofisticatezza, nonché di governance della cybersicurezza nazionale, il capo II inasprisce la risposta penale attraverso disposizioni di natura sostanziale e processuale mirate al contrasto dei reati informatici.

Senza entrare ora nel dettaglio delle singole disposizioni, è opportuno sottolineare in via preliminare come il DDL non operi in un *vacuum* normativo bensì si raccordi – e modifichi – la c.d. "normativa PSNC", ovvero il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 (unitamente ai diversi regolamenti attuativi) e il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

In particolare, si estende ai soggetti rientranti nella normativa PSNC l'obbligo di provvedere entro quindici giorni dalla comunicazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) circa specifiche vulnerabilità cui essi risultino potenzialmente esposti mediante interventi risolutivi indicati dall'Agenzia (art. 2 DDL). Sulla scorta del modello NIS 2 in materia di notifica degli incidenti, i soggetti PSNC dovranno effettuare una segnalazione entro 24 ore dall'avvenuta conoscenza di incidenti aventi impatto su reti, sistemi informativi e servizi informatici di propria pertinenza diversi da quelli 'perimetrati', da completarsi con la relativa notifica entro il termine di 72 ore. Inoltre, qualora i soggetti reiterino l'inosservanza di questa previsione, saranno passibili di una sanzione amministrativa pecuniaria fino ad un massimo di 125.000 euro (art. 3 DDL). Viene poi specificata una modalità di funzionamento del Nucleo per la cybersicurezza (art. 5 DDL); è prevista, come

nuova funzione di ACN, la produzione e diffusione di standard e raccomandazioni in materia di crittografia al fine di rafforzare la cybersicurezza dei sistemi informatici (art. 10 DDL) e, infine, si è prevista l'adozione di un regolamento per la disciplina del procedimento sanzionatorio amministrativo di ACN (art. 11 DDL).

Il presente contributo mira a far luce su un aspetto critico sollevato dal DDL, vale a dire, la risposta del legislatore nazionale in materia di cybersicurezza imperniata *principalmente* sull'aumento ed inasprimento della repressione penale alla luce di un modello, quello della Direttiva (UE) 2022/2555 (c.d. direttiva NIS 2), che, di converso, prevede *inter alia* un complesso quadro di strumenti di prevenzione e gestione del rischio di cybersicurezza di stampo più marcatamente privatistico-amministrativistico. Se è pacifico che la risposta penale sia una prerogativa degli Stati membri, la premessa da cui parte questo elaborato – e che si cercherà di avvalorare – è che il modello anticipatorio delineato dalla normativa NIS 2 sia più efficace di un modello repressivo-deterrente nell'affrontare le sfide poste dalla cybersicurezza, del tutto peculiari rispetto a quelle con cui i sistemi giuridici si confrontano nella dimensione analogica.

In questo contesto, una lettura che è possibile avanzare è che tale 'salto in avanti' del legislatore italiano, nelle more del recepimento della direttiva NIS 2, sia legato ad un più generale problema che caratterizza la regolamentazione della cybersicurezza nell'Unione: la tendenza a declinare questa in termini di sicurezza nazionale o di funzionamento del mercato interno e di cooperazione, a seconda del fatto che l'iniziativa legislativa venga presa rispettivamente dagli Stati membri o dalla Commissione europea.

II. Mentre il panorama delle minacce cibernetiche cresce in estensione e complessità, il legislatore nazionale dedica metà del nuovo provvedimento in materia al rafforzamento delle misure di contrasto di alcuni reati informatici. Si potrebbe obiettare che le disposizioni di cui al primo capo del DDL mirino proprio al rafforzamento di un modello di cyber resilienza simile a quello comunitario, con particolare riferimento alla direttiva NIS 2.

A tal proposito, si pensi all'art. 8, che impone alle pubbliche amministrazioni rientranti nell'ambito del DDL di individuare una struttura (all'interno della quale opererà il c.d. referente per la cybersicurezza quale punto di contatto unico dell'ente) che provvederà allo sviluppo di politiche e procedure di sicurezza delle informazioni (es., definizioni di ruoli e organizzazione del sistema), alla produzione e all'aggiornamento di un piano per la gestione del rischio cyber, nonché alla pianificazione e attuazione di interventi di potenziamento delle capacità di gestione del rischio e dell'adozione delle misure previste dalle linee guida da emanare con determina del direttore di ACN. Oppure, sotto diverso profilo, si pensi all'allineamento dei termini per gli obblighi di notifica di cui all'articolo 1, comma 2, DDL ai termini di cui all'articolo 23 della direttiva NIS 2.

Eppure, per quanto l'articolo 2, comma 5, della direttiva NIS 2 riconosca piena autonomia agli Stati membri nel decidere se la direttiva si applichi alle PA a livello locale (gli enti della PA a livello centrale sono infatti soggetti essenziali NIS 2, ex art. 3, comma 1, lett. d), è legittimo chiedersi perché 'anticipare' in questo provvedimento quanto avrebbe potuto essere disposto nel decreto legislativo di recepimento della NIS 2 (da adottare entro ottobre 2024). Ancorché sia imperativo per il nostro legislatore trovare nel futuro atto di attuazione della norma comunitaria un necessario raccordo con le disposizioni qui menzionate – al fine di evitare duplicazioni degli obblighi per tali soggetti – una scelta di diversa politica legislativa avrebbe portato con sé il beneficio di non frammentare ulteriormente un quadro normativo nazionale che, per quanto recente, risulta essere un "mosaico" di già diversi decreti-legge e decreti legislativi, DPR, DPCM, nonché determine del Direttore di ACN.

Veniamo ora al tema dell'efficacia della deterrenza sanzionatoria di stampo penalistico nell'ambito della cybersicurezza. Il tradizionale modello penalistico, in questo contesto, deve fronteggiare due sfide principali, tra loro correlate: la progressiva marginalità e debolezza della sovranità nazionale e la necessità di una risposta efficace alle minacce ed ai reati informatici. I rischi, le minacce e gli attacchi nel cyberspazio non sono più appannaggio esclusivo di attori statali, che devono riconoscere il potere *de facto* esercitato da attori privati. È opportuno ricordare come già la prima strategia UE in materia di cybersicurezza nel 2013 identificasse in un approccio multi-stakeholder la chiave per una gestione efficace delle sfide della dimensione digitale. Inoltre, la cybersicurezza è

intrinsecamente transnazionale. Ad incidere pertanto negativamente sulla tradizionale risposta penalistica vi sono, in primo luogo, le difficoltà nell'identificare e localizzare criminali informatici – spesso sufficientemente schermati da tecniche di anonimato – che operano in giurisdizioni diverse. Qualora si riuscisse poi ad identificare e perseguire il criminale, vi sarebbero poi delle sfide legate all'estradizione. Un altro elemento di complessità è dato dalla scarsa disponibilità di dati relativi alla criminalità informatica, anche alla luce della bassa percentuale di reati segnalati, ecc.

Peraltro, rimanendo sul piano della risposta penalistica, il DDL potrebbe essere letto come un'occasione mancata per l'introduzione di regole *ad hoc* di natura sostanziale e processuale, per esempio con riferimento all'espletamento di pagamenti da parte delle aziende a seguito di c.d. attacchi *ransomware*, *ethical hacking* o ancora in materia di competenza territoriale dei pubblici ministeri in tema di reati informatici.

Invece, come già ricordato, la direttiva NIS 2 sposta l'attenzione della risposta ai rischi, alle minacce e agli incidenti "a monte", attraverso un modello di governance articolato soprattutto intorno alla dimensione preventiva. Infatti, la direttiva NIS 2 declina il c.d. "approccio al rischio" – che permea la quasi totalità degli atti giuridici UE sul digitale – attraverso un complesso reticolato di quadri coordinati di cooperazione a livello nazionale, comunitario (es., Gruppo di cooperazione NIS; rete di CSIRTs; EU-CyCLONe), e internazionale (accordi internazionali *ex* art. 17 NIS 2); tramite l'incoraggiamento della condivisione di informazioni pertinenti (es., minacce, indicatori di compromissione, tecniche e procedure, ecc.) tra soggetti NIS e delle pratiche di divulgazioni coordinate delle vulnerabilità (attraverso l'istituzione di una banca dati europea delle vulnerabilità mitigate) al fine di aumentare il livello collettivo di cybersicurezza prevenendo così incidenti. Sempre sul fronte della prevenzione, la direttiva NIS 2 delinea poi un quadro di misure tecniche, operative e organizzative di valutazione e gestione dei rischi da parte dei soggetti NIS 2: il c.d. "approccio al rischio" si sostanzia nella responsabilizzazione del soggetto NIS, il quale dovrà adottare misure adeguate e proporzionate al rischio posto alla sicurezza dei suoi sistemi, secondo un approccio multi-rischio (protezione dell'ambiente fisico ed informatico).

Il DDL dovrebbe quindi porre maggiormente l'accento su questi aspetti 'anticipatori' e prevedere, quantomeno, dei regolamenti attuativi in cui vengano definite delle linee guida affinché le pubbliche amministrazioni interessate dal DDL riescano a conformarsi agli obblighi di cui all'art. 8 DDL, permettendo pertanto un rafforzamento effettivo – e non solo "sulla carta" – della cybersicurezza di tali soggetti, anche considerata la clausola di invarianza finanziaria di cui all'art. 23 DDL.

III. L'accento posto dal legislatore italiano sulla risposta repressiva all'accrescere delle minacce e degli attacchi cibernetici può essere letto con la lente dei conflitti di competenza, spesso silenziosi, tra l'UE e gli Stati membri nel regolamentare le questioni legate alla cybersicurezza. La vaghezza delle definizioni e dei concetti cardinali delle politiche di cybersicurezza all'interno dell'Unione è elemento imprescindibile di questa teoria. Infatti, sembra che i perimetri concettuali, nonché gli obiettivi perseguiti dal termine stesso di "cybersicurezza" (oppure ancora, "resilienza") varino a seconda di chi legiferi.

Gli Stati membri tendono a dotarsi di normative in materia di cybersicurezza facendo perno su aspetti di sicurezza nazionale (es., Italia, Estonia, Germania), la quale è competenza nazionale esclusiva di ciascuno Stato membro ex art. 4, paragrafo 2 del Trattato sull'Unione europea. In tal senso, non può stupire che tale riferimento normativo sia richiamato esplicitamente dall'analisi tecnico-normativa del DDL Cyber (A.C. 1717 Supplemento, p. 17). Nel caso italiano, una lettura congiunta del titolo della normativa di cui al decreto-legge n. 105 del 2019 e dell'articolo 1 del medesimo decreto suggerisce la volontà del legislatore di governare un'area specifica della sicurezza nazionale.

A un più basso livello di astrazione, tuttavia, le disposizioni della normativa PSNC si sovrappongono in larga misura – se non addirittura duplicano – con il quadro giuridico della NIS 2. Infatti, la Commissione europea disegna una governance europea della cybersicurezza partendo però da logiche diverse, ossia, di funzionamento del mercato interno e di cooperazione.

Dall'inizio degli anni 2000 possono essere rintracciati diversi "scontri" sulle competenze tra l'UE e gli Stati membri in materia di cybersicurezza: dall'istituzione dell'ENISA nel 2004, che si è vista progressivamente affidare compiti

tradizionalmente di appannaggio degli stati; alle posizioni divergenti tra Consiglio dell'UE, da una parte, e Parlamento e Commissione dall'altra, con il primo pronto a rimarcare la competenza statuale ex art. 4, paragrafo 2 TUE anche in materia di cybersicurezza in dossier legislativi come il *Cyber Resilience Act* (si vedano le posizioni circa una governance centralizzata/decentralizzata degli obblighi di notifica), *Cyber Solidarity Act* (che istituisce meccanismi di coordinamento a livello sovranazionale di gestione delle crisi e incidenti di cybersicurezza su larga scala, terreno che facilmente gli stati riconducono ai perimetri di sicurezza nazionale) o ancora la proposta del 2020 di una *Joint Cyber Unit* (poi mai concretizzatasi).

Connesso a ciò, rimane il difficile compito di tracciare i confini tra "cybersicurezza" e "sicurezza nazionale". Gli stessi eventi avversi descritti come minacce informatiche potrebbero al tempo stesso essere definiti come reati, ossia questione interna per eccellenza. Atteso che il confine tra minaccia cibernetica e crimine cibernetico sia tutt'altro che chiaro, il quadro giuridico sotteso alle competenze e strumenti cambia radicalmente. Se consideriamo la cybersicurezza come una questione di mercato unico digitale (vedi NIS 2, *Cybersecurity Act*, *Cyber Resilience Act*), o di competitività del sistema industriale dell'Unione (*Cyber Solidarity Act*), l'Unione ha competenza per disporre misure regolamentative non solo su standard tecnici comuni, ma anche su meccanismi comuni di indagine e reazione. Se consideriamo la lotta contro le minacce informatiche come una questione di diritto penale, come si è fatto per molto tempo (es., Convenzione di Budapest), tuttavia, il panorama è non solo diverso, ma anche meno efficace rispetto al modello comunitario, come visto sopra.

Senza entrare nel merito di quale ruolo possa (ancora) svolgere *efficacemente* il sistema giudiziario penale in questo contesto, come suggerito da Enrico Letta nel suo report *Much More than a Market* (aprile 2024), dietro incarico della dalla Commissione e dal Consiglio UE, l'imposizione di requisiti aggiuntivi da parte dei legislatori nazionali motivati da logiche connesse alla sicurezza nazionale, come nel caso italiano, rischia di erodere i benefici del mercato unico aumentando i costi e creando incertezza per le imprese. Per affrontare questo problema, è indispensabile garantire che questi requisiti siano in linea con il quadro legislativo europeo generale, adottando misure aggiuntive solo se assolutamente necessarie (p. 59).