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

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0137 • articolo non sottoposto a peer review • pubblicato in anteprima il 4 apr. 2024

Antonio Iannuzzi

Considerazioni sul disegno di legge «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)

Audizione informale innanzi alle Commissioni riunite I (Affari costituzionali) e II (Giustizia) della Camera dei Deputati

Si pubblica il testo dell'audizione orale svolta il giorno 28 marzo 2024 presso la Camera dei Deputati, Commissioni permanenti riunite I (Affari costituzionali) e II (Giustizia), sul disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717). Sono qui avanzate considerazioni sull'impianto generale della proposta e su alcune disposizioni del disegno di legge.

Cybersicurezza – Resilienza – Direttiva NIS 2 – Pubblica amministrazione – Reati informatici
Agenzia per la Cybersicurezza Nazionale (ACN)

Notes on the bill on "Provisions on strengthening national cybersecurity and cybercrimes" (AC 1717)

Oral hearing at the Chamber of Deputies, Joint Standing Committees I (Constitutional Affairs) and II (Justice)

The text of the oral hearing held on March 28, 2024 at the Chamber of Deputies, Joint Standing Committees I (Constitutional Affairs) and II (Justice), on the bill on "Provisions on strengthening national cybersecurity and cybercrimes" (AC 1717) is published. The text suggests some considerations about the general outline of the proposal and some provisions of the bill are advanced here.

Cybersecurity – Resilience – NIS 2 – Public Administration – Cybercrimes – Italian Agency for National Cybersecurity

L'Autore è professore ordinario di Istituzioni di diritto pubblico presso l'Università degli Studi Roma Tre

Onorevole Presidente, onorevoli Deputati,

1. Il disegno di legge «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (A.C. 1717) è stato presentato come una risposta sostanziale all'aumento delle minacce derivanti da attacchi cibernetici e, dal Presidente del Consiglio dei ministri, come una risposta politica al grave c.d. "caso dossieraggi", emerso a seguito del fatto che la Procura di Roma ha accertato che un ufficiale della Guardia di finanza, distaccato presso la Direzione nazionale antimafia, era responsabile di numerosissime interrogazioni al Sistema dell'Agenzia delle entrate riguardanti diversi politici italiani.

2. La prima parte del provvedimento è sostanzialmente un'anticipazione della normativa di recepimento della Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS 2) all'interno dell'ordinamento italiano, con l'obiettivo di «sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici». Alcune previsioni sono significative e senza dubbio da apprezzare positivamente: le nuove norme, infatti, vanno ad individuare un "superperimetro" che comprende al suo interno sia i soggetti destinatari delle misure previste dalla Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS 1), sia i soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica, sia altre entità che vengono esplicitamente elencate e che non appartengono a queste categorie. Proprio questo elemento ulteriore è molto interessante perché affronta alcune linee di presidio attualmente scoperte (anche se in prospettiva coperte dalla Direttiva NIS 2): i comuni sopra i 100.000 abitanti, e, comunque, i comuni capoluoghi di regione, e le rispettive *in-house* e poi le società di trasporto pubblico locale con analogo bacino.

2.1. Con riguardo all'obbligo per i Comuni con popolazione superiore ai 100.000 abitanti e, comunque, dei comuni capoluoghi di regione, soggetti all'obbligo di segnalare e notificare gli incidenti indicati nella tassonomia di cui all'art. 1, co. 3-*bis*, del d.l. 21 settembre 2019, n. 105, aventi impatto su reti, sistemi informativi e servizi informatici di rispettiva pertinenza, sono da segnalare due ordini di questioni.

La prima cosa da osservare è, secondo i dati statistici disponibili, che i Comuni oltre i 100.000 abitanti sono oltre 40; ad essi andranno ad aggiungersi i capoluoghi di regione con popolazione inferiore. Sulla reale capacità dei Comuni di far fronte, con rapidità ed efficienza, a quest'obbligo si possono nutrire dei dubbi, alla luce peraltro della presumibile carenza in organico di figure con simile professionalità. Il depauperamento della dotazione organica dei Comuni e delle Città metropolitane che si è determinato negli ultimi anni si rende ancora più evidente per i profili ad alta specializzazione tecnica. In conseguenza di queste criticità, si potrebbero incentivare sia una gestione associata, nella forma di convenzioni, sia la possibilità di gestione come "unione di comuni", nel caso di Comuni limitrofi, stante il fatto che la disciplina legislativa in tema di unione di comuni, l'art. 32 del TUEL a livello statale e le leggi regionali, non dettano limiti specifici relativamente agli ambiti di intervento. Si potrebbe, anche, pensare di valorizzare l'assistenza fornita dall'ANCI.

Consentitemi, però, di rilevare criticamente che il ddl prevede la clausola dell'invarianza finanziaria che mal si concilia con le enormi esigenze di formazione sia di nuove professionalità esterne all'amministrazione sia di personale amministrativo già nei ruoli che potrebbe essere riqualificato all'uopo. La mancanza di formazione sulla sicurezza cibernetica, che è parte di un deficit di conoscenze digitali dei cittadini italiani, deve essere assunta come un'emergenza democratica ed una questione costituzionalmente rilevante. Il *Digital*

Economy e Society Index (DESI) 2022 – indice che misura lo sviluppo dell'economia e della società digitale stilato annualmente dalla Commissione europea – colloca l'Italia nell'indecorosa posizione del 25° posto fra i 27 paesi aderenti all'Ue alla voce capitale umano, con un disarmante tasso di analfabetismo digitale pari a più della metà della popolazione, in quanto solo il 46% degli italiani risulta in possesso di competenze digitali di base. Oggi il PNRR sta investendo nell'acquisizione di competenze digitali, ma occorre preoccuparsi di assicurare una formazione continua dopo la fine del PNRR, non solo garantendo investimenti finanziari, ma anche reimmaginando i soggetti che saranno deputati ad erogare tali saperi, tenendo in considerazione che la formazione professionale è da lungo tempo un elemento di criticità in Italia.

Sotto questo profilo è da apprezzare l'iniziativa dell'Agenzia per la cybersicurezza nazionale (ACN) che con l'Avviso n. 8/2024 ha avviato una procedura per la selezione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente. Si tratta, comunque, di risorse stanziate «a valere sul PNRR», per cui resta la mancanza di previsione di risorse ordinarie per la formazione del personale e per favorire il percorso di accompagnamento delle amministrazioni all'adeguamento agli obblighi previsti.

La seconda cosa da osservare riguarda la circostanza che i Comuni indicati all'art. 1 dovranno anche individuare, ai sensi dell'art. 6, comma 2, «il referente per la cybersicurezza», selezionandolo «in ragione delle qualità professionali possedute». In merito occorre segnalare che la previsione normativa, così come genericamente formulata, non consente di individuare con sicurezza i requisiti professionali di cui dovrà essere in possesso detto referente (attestazioni, certificazioni, pregressa esperienza, che tipo di formazione accademica?) Se si pensa di individuare una figura equivalente al *Chief Information Security Officer* (CISO) previsto dalla NIS 2 per le aziende, allora occorre far mente che il CISO deve possedere una competenza solida e consolidata nel campo delle tecnologie informatiche e dei concetti basilari della sicurezza informatica. Di solito, il CISO ha una formazione accademica in informatica, ingegneria informatica o un settore affine. Deve aver accumulato esperienza pratica nella supervisione della sicurezza informatica ed aver acquisito una conoscenza approfondita delle normative e degli standard di sicurezza, quali principalmente la certificazione ISO 27001. Non è neppure chiaro, stante la laconicità della norma, se l'amministrazione dovrà istituire una struttura interna, con il coordinamento del referente per la cybersicurezza. Questi dubbi probabilmente consigliano l'inserimento di una previsione che demanda ad un successivo decreto la chiarificazione di questi aspetti, che appaiono di primaria importanza se si pensa alle funzioni attribuite al referente ed alle sanzioni in cui possono incorrere i Comuni. Occorre tenere in considerazione che di una chiarificazione relativa alle qualità professionale del referente beneficerebbero tutte le amministrazioni individuate all'art. 1 del ddl in discussione, che sono soggette al medesimo obbligo.

Ancora, sarebbe opportuno valutare se dal punto di vista funzionale tale referente possa essere inquadrato come dirigente, sia in ragione dei maggiori poteri di intervento, sia per attivare la connessa responsabilità dirigenziale in caso di inadempienza.

2.2. In riferimento all'inclusione delle società *in house* appare necessario chiarire il tema delle *in house*, anche in prospettiva NIS 2. La mera partecipazione azionaria, infatti, non è un criterio efficace per l'inserimento nel perimetro di sicurezza nazionale, che invece è più influenzato dal settore di attività e dall'oggetto del servizio più che dalla forma giuridica che connota il rapporto tra comune e soggetto imprenditoriale (*in house*). In particolare, si dovrebbe far riferimento a tutti i servizi esternalizzati, a prescindere se essi siano esternalizzati nella formula dell'*in house providing* o meno. Peraltro, la dicitura «in house» rischia di essere equivoca e di non richiamare in maniera definita una precisa ed unica fattispecie. Meglio sarebbe riferirsi alle società affidatarie o concessionarie di servizi essenziali, escludendo invece società *in house* che potrebbero essere affidatarie di servizi non particolarmente critici o comunque non inclusi nella direttiva NIS 2.

3. Relativamente ai poteri dell'Agenzia per la cybersicurezza nazionale ed ai successivi obblighi per i

soggetti di cui all'art. 1, comma 1 il ddl prevede, in particolare all'art. 2, che i soggetti destinatari degli obblighi «in caso di segnalazioni puntuali dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultino *potenzialmente* [corsivo mio, n.d.a.] esposti, provvedono, senza ritardo e comunque non oltre quindici giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia».

Il secondo comma aggiunge che «La mancata o ritardata adozione degli interventi risolutivi di cui al comma 1 comporta l'applicazione delle sanzioni di cui all'articolo 1, comma 5, salvo il caso in cui motivate esigenze di natura tecnico-organizzativa, tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale, ne impediscano l'adozione o ne comportino il differimento oltre il termine indicato al comma 1».

Tale formulazione normativa merita di essere chiarita.

In primo luogo, potrà essere valutata l'opportunità di espungere il riferimento alla potenziale esposizione («potenzialmente esposti») giacché la sottoposizione a sanzione sembra presupporre l'accertamento di una condizione certa di esposizione al pericolo.

In secondo luogo, non appaiono sufficientemente determinate le «motivate esigenze di natura tecnico-organizzativa», che se «tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale», possono comportare il differimento del termine o finanche la mancata adozione delle misure risolutive indicate dall'ACN. Il rischio è che una formulazione così generica possa essere troppo facilmente addotta finendo per stemperare, fino a vanificare, l'imposizione dell'obbligo. È vero che l'ACN potrà sindacare le motivazioni, ma la formula non contiene alcuna specificazione riguardo alle esigenze di natura organizzativa che giustificano il tardivo o mancato intervento, tuttavia essa appare foriera di contenzioso. Avverso la sanzione, infatti, entro 30 giorni dalla sua notificazione l'interessato può presentare opposizione all'ordinanza ingiunzione (che, di regola, non sospende il pagamento), inoltrando ricorso all'autorità giudiziaria competente (artt. 22, 22-*bis*, l. 24 novembre 1981, n. 689).

4. Sia consentito, a questo punto, un breve inciso sull'impianto generale del disegno di legge, che è scritto con un metodo tutto incentrato sull'individuazione di obblighi a cui corrispondono sanzioni, ora più severe. Questa impostazione a mio avviso non favorisce l'acquisizione di una cultura della cybersicurezza che presuppone la maturazione della consapevolezza che il rafforzamento della sicurezza cibernetica è un vantaggio per il Paese e che è interesse comune adoperarsi per la sicurezza delle reti. È importante notare che diverse disposizioni incluse in questo ddl, ma lo stesso vale per molte disposizioni presenti anche nella Direttiva NIS 2 che si andrà presto a recepire, riflettono le pratiche di sicurezza informatica che la maggior parte delle organizzazioni pubbliche o private dovrebbe implementare per proteggere sia i dati dei cittadini sia, per le aziende, il proprio business. Di conseguenza, le amministrazioni, in questa fase, dovrebbero progressivamente mirare a elevare i requisiti minimi in materia di sicurezza informatica, dedicando risorse finanziarie e competenze necessarie a tale scopo. La capacità di riconoscere rapidamente la natura di un attacco e di adottare misure efficaci per mitigare il rischio diventa un aspetto cruciale per garantire l'efficacia dei sistemi di sicurezza informatica e la preparazione dei dipendenti, i quali dovrebbero essere costantemente formati per sviluppare e migliorare le loro pratiche di sicurezza informatica nel tempo. Pertanto, in un mercato con limitate risorse professionali come quello della sicurezza informatica, diventa sempre più decisivo orientare le strategie e gli investimenti verso la formazione di personale qualificato e sempre aggiornato.

5. La seconda parte del ddl è relativa all'incremento delle pene per i *cyber crime* oltre a creare nuove fattispecie di reato. Tra queste particolarmente rilevante è il tema di cui all'art. 1, lettera *p*), che introduce l'art. 635-*quater*.1 del Codice penale, per la disciplina del reato di «Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico».

L'articolo rischia di determinare, nella formulazione attuale, alcuni problemi interpretativi.

Mi soffermo sulla questione principale: è necessario che venga meglio chiarito e specificato il concetto "danneggiare illecitamente", che indurrebbe a pensare che esista – e che quindi sia legittima – l'ipotesi di "danneggiare lecitamente".

In molti casi l'attività di cybersecurity potrebbe portare a svolgere talune delle attività di sopra richiamate, ma non a scopo malevolo, bensì a

scopo difensivo. Tuttavia, se questo era l'intento del proponente, la formulazione non è certamente delle più chiare ed immediate, soprattutto se pensiamo al fatto che, nell'ordinamento italiano, non è prevista la legittima difesa cibernetica.

Proprio questo può essere il punto di svolta del provvedimento: il riconoscimento del legittimo ricorso all'uso del mezzo informatico per difendersi da una azione violenta che metta a rischio la sicurezza del singolo o di altri ovvero i beni ovvero il domicilio, sebbene digitale. L'esempio concreto è quello di un *Red Team* (difesa attiva) che agisca per far cessare un attacco informatico, che potrebbe incorrere nel reato – non essendo disposta la fattispecie del "danneggiamento lecito" – per danneggiamento illecito delle capacità dell'*hacker*. Ancora, il servizio di *Cyber Threat Intelligence* che recupera nel dark web informazioni che consentono di sventare un attacco informatico potrebbe incorrere nella fattispecie dell'"abusivamente si procura", anch'essa prevista dal ddl, non essendo definito quando sia invece consentito il "procurarsi" dati, informazioni ecc. E così di seguito.

L'assetto normativo nuovo, soprattutto, potrebbe mettere a rischio la professione e l'attività di *penetration testing*. Quella cioè in cui un soggetto viene ingaggiato per testare, attraverso un attacco concordato, le difese di un sistema informatico. Anche in quel caso vi sono condotte "offensive" non supportate però da un intento doloso. Certamente non si vuole vietarle, ma il rischio è quello di determinare un'inversione dell'onere della prova in relazione allo "scopo" per il quale si detiene una determinata capacità o si effettua una determinata azione.

Mi chiedo se in tal modo il legislatore intenda estendere la portata dell'art. 52 del Codice penale in tema di legittima difesa. A mio avviso, nel solco della giurisprudenza costituzionale più recente, è possibile ampliare interpretativamente la tutela costituzionale e legislativa del domicilio, di modo che domicilio analogico e digitale possano essere tutelati allo stesso modo dalla legge, così come avviene per la nozione di corrispondenza. La sentenza n. 170/2023 della Corte costituzionale ha esteso, infatti, la nozione di "corrispondenza", nel caso di specie proprio per l'estensione delle prerogative dei parlamentari *ex* art. 68, co. 3, Cost., alle «forme di scambio di pensiero a distanza (…), costituenti altrettante "versioni contemporanee" della corrispondenza epistolare e telegrafica. Sostenere il contrario, in un momento storico nel quale la corrispondenza cartacea, trasmessa tramite il servizio postale e telegrafico, è ormai relegata, nel complesso, a un ruolo di secondo piano, significherebbe d'altronde deprimere radicalmente la valenza della prerogativa parlamentare in questione». Insomma, muta lo spazio di applicazione, non il diritto in oggetto.