CONFERENZA DELLE REGIONI
E DELLE PROVINCE AUTONOME

24/43/CR08/C14

POSIZIONE SULLO SCHEMA DI DISEGNO DI LEGGE RECANTE "DISPOSIZIONI IN MATERIA DI REATI INFORMATICI E DI RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE

La Conferenza delle Regioni e delle Province autonome, nel corso della seduta odierna, con riferimento allo schema di disegno di legge in epigrafe ha condiviso le proposte emendative e le osservazioni di seguito riportate, quale utile contributo all'iter parlamentare del provvedimento.

Proposta additiva

1.1
All'Art. 1, comma 1, dopo le parole "*rispettive società in house*" aggiungere quanto segue:
"che operano nel settore ICT, per gli incidenti che le riguardano direttamente. Nel caso di società in house l'obbligo di segnalazione si estende anche agli incidenti occorsi ai soggetti pubblici soci che non rientrano tra i soggetti di cui al primo periodo del comma 1".

Relazione illustrativa
La proposta cerca di chiarire l'ambito di applicazione:

- le società in house di cui si parla sono quelle del settore ICT, e non quelle che operano per servizi in settori diversi (formazione, finanziamenti, ecc);
- l'in house può essere soggetto sia ad incidenti diretti che ad incidenti nell'ambito dei servizi che erogano per soggetti pubblici soci, quindi la modifica cerca di evitare che per uno stesso incidente ci siano due soggetti che fanno la relativa segnalazione (sia l'amministrazione che la rispettiva società in house di cui l'amministrazione si avvale);
- l'in house può erogare servizi anche ad enti non ricompresi tra quelli elencati nel primo periodo del comma 1 e, in caso di incidenti, risulta fondamentale che la società in house, nel rafforzare il suo ruolo di gestore e di presidio della cybersicurezza verso le PA socie, venuta a conoscenza di incidenti che riguardano i propri servizi erogati, sia tenuta alla segnalazione indipendentemente dalla dimensione o dalla connotazione del soggetto pubblico socio.

Proposta emendativa

1.1
All'Art. 1, comma 1, dopo le parole "*e le aziende sanitarie locali*" aggiungere le parole "*ed ospedaliere*"

Relazione illustrativa
Le aziende ospedaliere fanno parte del servizio sanitario regionale al pari delle aziende sanitarie locali e per questo si ritiene debbano essere annoverate anch'esse tra i soggetti di cui all'art. 1 comma 1 per garantire gli stessi livelli di cybersicurezza.

Proposte emendative sulle segnalazioni

Proposta additiva

1.2
All'articolo 1, comma 2, dopo le parole *"I soggetti di cui al comma 1 segnalano senza ritardo"* inserire le seguenti *"per il tramite del Referente per la cybersicurezza di cui al successivo art. 6 comma 2"*.

Relazione illustrativa
Si chiarisce che ad effettuare le segnalazioni è il referente di cui al successivo articolo 6 comma 2.

Proposta ablativa

2.1
All'Articolo 2, comma 1, la parola "*potenzialmente*" è soppressa.

Relazione illustrativa
Dal momento che tale previsione prevede applicazione di sanzioni per inadempienza, si propone di espungere la parola "potenzialmente" in modo da far ricadere in questa fattispecie di segnalazioni puntuali dall'ACN solo quelle su cui ci sono effettive evidenze di esposizione da parte dell'Ente ricevente tale segnalazione.

Proposta emendativa

6.1
All'articolo 6, comma 1, dopo le parole *"I soggetti di cui all'articolo 1, comma 1, provvedono a individuare, laddove non già presente, una struttura"* aggiungere le seguenti: "*dirigenziale unica, denominata Ufficio per la cybersicurezza,*" e dopo le parole "*che provvede*" aggiungere le seguenti: "*sotto gli indirizzi dell'Ufficio RTD, come previsto dall'art. 17, comma 1, lett. c), del d.lgs. 7 marzo 2005, n. 82, ai compiti relativi:"*.

Relazione illustrativa
La proposta mira a chiarire che la struttura prevista dall'art.6 sia unica e di livello dirigenziale, al fine di garantire presidio ad un opportuno livello organizzativo rispetto ad un tema così rilevante per gli enti e per l'adeguata implementazione agli interventi previsti in ambito PNRR Misura 1 investimento 1.5.
Inoltre viene chiarito che il nuovo "Responsabile per la Cybersicurezza" dovrà seguire gli indirizzi più generali dettati dal "Responsabile per la Transizione Digitale" (RTD) per via delle funzioni riconosciute dal vigente D. Lgs. n. 82/2005.

Proposta ablativa

6.1
All'articolo 6, comma 1, le parole "*nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente*" sono soppresse.

Relazione illustrativa
Si ritiene che la locuzione, limitativa, induca le amministrazioni a privilegiare il mero adempimento (un po' come avvenuto con la figura del Responsabile per la Transizione Digitale - Ufficio RTD) e non la funzionalità, lo sviluppo di nuove competenze ed il rafforzamento dell'organizzazione in tema cybersicurezza.

Comma aggiuntivo

6.1 bis
All'articolo 6, dopo il comma 1, viene aggiunto il seguente comma:
"1-bis. Il responsabile della struttura di cui al comma 1 è dotato di adeguate competenze tecnologiche, di cybersicurezza e manageriali".

Relazione illustrativa
La proposta mira a chiarire che il dirigente responsabile della struttura prevista dall'art.6 deve avere specifiche competenze in materia, al fine di garantire presidio con competenze opportune di un tema così rilevante per gli enti e per l'adeguata implementazione agli interventi previsti in ambito PNRR Misura 1 investimento 1.5.

Proposta emendativa

6.2
All'articolo 6, comma 2, sostituire la frase "*Il predetto referente svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale*" con la seguente: "*Il predetto referente svolge la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale, e con i CSIRT regionali eventualmente istituiti,"*.

Relazione illustrativa
Si ritiene che il referente debba fare da punto di contatto anche con lo CSIRT di livello regionale quale raccordo intermedio fra gli enti locali del territorio regionale e ACN.

Proposta emendativa

6.2
All'articolo 6, comma 2, dopo la frase "*A tal fine, il nominativo del referente per la cybersicurezza è comunicato all'Agenzia per la cybersicurezza nazionale*" aggiungere le seguenti parole: "*unitamente ai nominativi dei delegati del referente stesso per garantire la reperibilità della funzione. Il referente può essere alle dipendenze della struttura del comma 1 oppure operare sulla base di un contratto di servizio, anche avvalendosi della rispettiva società in house*".

Relazione illustrativa
Si chiede di valutare la possibilità di inserire figure delegate/supplenti del referente al fine avere una garanzia di opportuna reperibilità, in caso di indisponibilità o irraggiungibilità del referente, nell'ottica di ottemperare allo stringente requisito di segnalazione di un incidente entro le 24 ore e/o eventuale notifica entro 72 ore. Il referente potrà operare anche in base ad un contratto di servizio, come nel caso del DPO, e tale ruolo potrà essere svolto anche dalle società in house per conto delle rispettive amministrazioni socie.

Comma aggiuntivo

6.2 bis/ter
All'Art. 6, dopo il comma 1, aggiungere i seguenti commi:
"2-bis. *Le Regioni e le province autonome di Trento e di Bolzano, sulla base di accordi con l'Agenzia per la cybersicurezza nazionale, possono istituire CSIRT regionali operanti in raccordo con lo CSIRT nazionale.*
"2-ter. *L'organizzazione e l'attività degli CSIRT regionali istituiti sulla base del precedente comma, sono definiti attraverso la stipula di intese in sede di Conferenza Stato-Regioni"*.

Relazione illustrativa
Si ritiene che tale previsione sia in linea con quanto previsto nella Strategia Cyber nazionale e nelle progettualità in ambito PNRR Misura 1 investimento 1.5 promosse dall'Agenzia per la Cybersicurezza Nazionale, che prevedono appunto l'istituzione di CSIRT di livello regionale.
Si ritiene, inoltre, che l'organizzazione e le attività degli CSIRT regionali siano elementi di carattere strategico tali da essere oggetto di intesa in sede di Conferenza Stato-Regioni.

Proposta emendativa

6.3 a)
All'art. 6, comma 3, lettera a) dopo le parole "*ai soggetti di cui*" aggiungere quanto segue: "*all'articolo 3, comma 1, lettere g) e i), del decreto legislativo n.65 del 2018, e a quelli"*

Relazione illustrativa
È necessario precisare che la sfera di competenza del referente cybersicurezza non ricomprende i soggetti, facenti parte della medesima organizzazione, già individuati ai sensi della direttiva NIS in modo uniforme a quanto escluso nell'art.1.

Proposta ablativa

8.1
All'articolo 8, comma 1, le parole "*anche in deroga all'art. 17 della legge 23 agosto 1988, n. 400*" sono soppresse.

Relazione illustrativa
Si ritiene che la deroga al procedimento di formazione dei regolamenti previsto in via generale dall'art. 17 della legge 400 del 1988 possa costituire una potenziale fattore contrastante il riparto di competenze tra Stato e Regioni ex art. 117, comma 6, Cost.

OSSERVAZIONI

Osservazioni di carattere generale

La Conferenza delle Regioni e delle Province autonome sottolinea, in linea generale:

1. la necessità di prevedere un intervento – nel DDL o in altro provvedimento ad esso collegato - di normazione di attività di *penetration testing* a scopo di *ethical hacking* e nell'ambito di attività preventiva.
2. che l'impianto della norma appare analogo ad altre che presentano uno schema adempimento-sanzione. Tale approccio si scontra con l'esigenza operativa di intervento

   richiesta dalla cybersicurezza. È necessario uno sforzo per realizzare un sistema che, superando la mera teoria normativa, si concentri sulla messa in atto degli adempimenti. Nel caso di specie, l'introduzione di un Responsabili/Referente per la Cybersicurezza in ogni Amministrazione dimostra un'attenzione alle nuove sfide presentate dalla cybersecurity, 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. È fondamentale che ACN, oltre a introdurre novità normative in merito, lavori a stretto contatto con i Responsabili/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. Si ritiene che, 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 verso soggetti terzi, si debbano adottare misure in grado di incidere efficacemente e tempestivamente. Tra le ipotesi, si potrebbero introdurre pareri obbligatori da parte del Responsabile/Referente per la Cybersicurezza su ciascun atto dell'Ente e la possibilità di emanare linee guida e raccomandazioni interne.
3. che per rendere efficace l'intervento, considerando anche la già consolidata normativa in tema di cybersicurezza, servirebbe un'impostazione analoga a quella prevista dal GDPR, dal D.Lgs. 81/2008 o dalla L. 190/2012 in particolare in relazione alla definizione gerarchica dei ruoli e delle responsabilità (da cui le proposte sopra che chiariscono meglio il rapporto Responsabile e Referente); sarebbe necessario creare un collegamento, in coerenza con quanto previsto dalla Direttiva UE 2022/2555 NIS2, tra l'organo politico di indirizzo e la struttura amministrativa di gestione, nonché chiarire meglio che il Referente è una figura di garanzia, interna o esterna, analoga al DPO previsto dal GDPR, al RSPP di cui al D.Lgs. 81/2008 o al RPCT di cui alla L. 190/2012, alla quale siano garantite autonomia e indipendenza.
4. che il disegno di legge pone maggiormente l'accento sulla risposta e sulle sanzioni in caso di attacchi informatici. È però altresì importante rivolgere l'attenzione verso la prevenzione di tali attacchi. Questo implica non solo miglioramenti nell'ambito normativo, ma soprattutto un impegno continuo nella formazione e all'aggiornamento delle competenze del personale e delle nuove figure introdotte di cui non si ritrova traccia nel testo.

<u>Osservazioni di carattere specifico</u>

La Conferenza delle Regioni e delle Province autonome, inoltre, rappresenta le seguenti osservazioni specifiche relativamente ai punti del provvedimento indicati di seguito.

1. **Capo I art. 1, comma 4**
   Si chiede di chiarire la figura dell'"interessato" e se coincida con i soggetti di cui all'art.1 comma 1.
2. **Capo I art. 1, comma 5**
   "nel rispetto delle disposizioni di cui all'articolo 17, comma 4-quater, del decreto-legge 14

giugno 2021, n. 82": non si rinviene il riferimento al comma 4-quater. Si chiede di chiarire se la sanzione venga applicata al soggetto di cui all'art.1 comma 1 o al soggetto di cui all'art.6 comma 2, ove nominato.

3. **Capo I Articolo 2 comma 1 lettera i)**
   Si richiede di precisare se i 15 giorni indicati siano da considerarsi come "solari" o "lavorativi". -> se non specificato di norma dovrebbero essere solari. Si richiede altresì di precisare se tale tempistica è da considerarsi valida per qualunque grado di gravità della vulnerabilità segnalata dall'Agenzia o se debba essere considerata da un certo grado di gravità in su e, nel caso, quale.
4. **Capo I Art. 2, comma 1**
   Da un punto di vista pratico si potrebbe migliorare l'efficienza organizzativa consolidando le notifiche da effettuare al Garante Privacy (entro 72 dal momento in cui il Titolare ne viene a conoscenza come previsto dall'art.33 GDPR) e al CSIRT in un unico punto centrale. Questo consentirebbe di gestire in modo ottimale tutte le comunicazioni relative a una violazione, riducendo il tempo e le risorse necessarie per gestire separatamente ciascuna notifica entro i tempi richiesti. Si rappresenta che, in momenti di elevata criticità, come quelli legati ad un incidente di cybersicurezza, la moltiplicazione degli oneri, tra i quali la denuncia ai sensi dell'art. 331 del codice di procedura penale, a carico dei singoli Enti rischia di ritardare la messa in atto delle principali contromisure. Si osserva inoltre come, nelle prime fasi di un incidente, durante le quali non è di norma ancora completamente chiara la natura dello stesso, la notifica preliminare all'Autorità per la Protezione dei Dati Personali rappresenti una prassi consolidata a tutela dell'Ente.
5. **Capo I Art. 2, comma 1**
   Si utilizza il termine segnalazione riferito a quanto inviato da ACN, a differenza dell'art.1 nel quale la segnalazione è riferita a quanto inviato dalle amministrazioni. Si suggerisce di modificare la terminologia per rendere il testo maggiormente chiaro.
6. **Capo I Art. 6, commi 1 e 2**
   Con l'avanzare della digitalizzazione delle Pubbliche Amministrazioni e dei soggetti coinvolti nella sicurezza nazionale informatica aumenta la superficie di esposizione agli attacchi informatici. All'opposto, si rileva una crescente criticità nel reclutare le specialisti ICT (risorse umane) dotate di competenze avanzate specifiche in ragione di una diffusa carenza nel mercato anche privato delle competenze ICT e in particolare di formazione nel campo della Cybersecurity. In tal senso si profila una potenziale criticità nell'individuazione delle risorse umane di cui al comma 1 e 2, che potrebbe comportare, come avvenuto per gli RTD, l'individuazione di personale privo delle necessarie competenze e un conseguente mancato rafforzamento delle Amministrazioni.
7. **Capo I Art. 6, comma 2**
   Potrebbe essere opportuno, al fine di agevolare in particolare gli enti di minori dimensioni o quelli che utilizzano sistemi informativi erogati dalla società in house o dalla Regione come aggregatore, considerare la possibilità che il ruolo di referente sia svolto direttamente dalla in house (vedi proposta emendativa) oppure in subordine che sia possibile una nomina associata del referente di cui al comma 2, in analogia a quanto previsto dall' art. 17 comma 1 *septies* del CAD (Codice dell'Amministrazione Digitale) che prevede anche la possibilità di esercitare le funzioni di RTD in forma associata. Tale previsione potrebbe rispondere all'ampliamento dell'ambito soggettivo di applicazione della Direttiva 2022/2555 NIS2 con riferimento ai soggetti pubblici.

8. **Capo I Articolo 6 comma 2**
   Si chiede di precisare se il referente per la cyber sicurezza debba essere necessariamente una risorsa interna all'Ente o possa essere un soggetto esterno delegato dallo stesso. Vedere

anche proposta emendativa fatta in tal senso.

9. **Capo I Art. 6, comma 1**
   L'art. 17 comma 1 lett. c) del CAD prevede che il Responsabile per la Transizione Digitale svolga compiti di "indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1". L'attribuzione di detto compito si sovrappone a quelli spettanti alla struttura di cui all'art.6 del DdL e richiede un raccordo tra le figure. Vedere proposta emendativa in tal senso
10. **Capo I**
    L'art. 24 rubricato "Esclusione dal diritto di accesso" della legge 7 agosto 1990, n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*" individua un elenco dei casi per i quali non può essere esercitato il diritto di accesso. A tale elenco si potrebbe aggiungere una specifica disposizione che escluda dall'accesso anche tutte le informazioni relative agli incidenti di sicurezza informatica. Le informazioni fornite relativamente agli incidenti possono infatti rendere noti dati relativi ai sistemi informativi, alla loro configurazione e comportare l'aumento dell'esposizione e del rischio di ulteriori attacchi.
11. **Capo II Art.18, comma 2**
    "I proventi delle sanzioni di cui all'articolo 1, comma 5, confluiscono tra le entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera f), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109." Si potrebbe considerare, anche al fine di evitare conflitti di interesse tra l'Ente chiamato ad irrogare le sanzioni e il beneficiario delle stesse, che i proventi confluiscano in un fondo, eventualmente gestito da ACN stessa, le cui risorse annualmente siano messo a disposizione delle Amministrazioni, ad esempio attraverso dei bandi, ai fini dell'implementazione delle politiche di cybersicurezza.

Roma, 4 aprile 2024