Commissioni riunite, I Affari costituzionali e II Giustizia,

Camera dei Deputati

**Osservazioni e proposte**

Audizione del 28/03/2024

**Fernanda Faini**

**ricercatrice in *tenure track* e docente di informatica giuridica**

**Università Telematica Pegaso**

**Disegno di legge C. 1717 Governo, recante**

**"Disposizioni in materia di**

**rafforzamento della cybersicurezza nazionale e di reati informatici"**

Onorevole Presidente, Onorevoli Deputati,

ringrazio per l'invito; mi onora poter portare il mio contributo.

Premesso che:

il disegno di legge in esame e la *ratio* di rafforzamento della cybersecurity, incidendo sull'ambito amministrativo pubblico e aggravando il trattamento sanzionatorio per i reati informatici meritano un apprezzamento generale anche in considerazione della sensibilità della tematica affrontata e alla luce dell'incremento degli attacchi informatici;

Considerato che:

in specifico, con il disegno di legge si intende conseguire una più elevata capacità di protezione e risposta a fronte di emergenze cibernetiche anche alla luce dell'attuale

contesto geopolitico, intenti assolutamente condivisibili e pregevoli;

al fine di superare le criticità attuali, l'ottica del disegno di legge è tesa ad un rafforzamento di obblighi e strutture dedicate alla cybersecurity, accompagnate dalla presenza di procedimenti dedicati e sanzioni al fine di garantirne efficacia ed effettività;

proprio al fine di realizzare questi obiettivi e garantire effettività alle norme, il disegno di legge incide su diverse dimensioni che caratterizzano l'*agere* pubblico, afferenti alle competenze, alla *governance*, all'organizzazione e ai procedimenti delle pubbliche amministrazioni;

di conseguenza, le osservazioni, le integrazioni e i suggerimenti di seguito proposti vanno proprio nel senso di una puntuale attuazione delle finalità e obiettivi che si prefigge il presente disegno di legge;

tanto premesso e considerato si suggerisce quanto segue
prevalentemente in relazione al Capo I del disegno di legge stesso:

1) per quanto riguarda l'art. 1 e l'art. 2 del disegno di legge recanti gli obblighi di notifica di incidenti a carico di pubbliche amministrazioni e altri soggetti indicati, la previsione di ispezioni e sanzioni previste (oltre alla responsabilità disciplinare e alla responsabilità amministrativo-contabile) e gli obblighi di adozione di interventi risolutivi indicati dall'Agenzia per la cybersicurezza nazionale (di seguito anche ACN) in caso di inosservanza delle previsioni, proprio al fine di garantire l'attuazione in modo effettivo, efficace e completo delle disposizioni, si suggerisce di **superare la prevista clausola di invarianza finanziaria** di cui all'art. 18, secondo cui le amministrazioni pubbliche competenti provvedono all'adempimento dei compiti derivanti dalla presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, e, al contrario, di prevedere risorse dedicate.

Tale osservazione vale anche in considerazione dell'art. 6, che prevede l'individuazione di una struttura dedicata da parte delle amministrazioni pubbliche e degli altri soggetti cui le disposizioni sono rivolte e di un Referente per la cybersicurezza con gli articolati obblighi previsti a loro carico. Il suggerimento scaturisce anche alla luce delle problematiche già insorte per altre disposizioni afferenti all' applicazione delle

tecnologie informatiche in ambito pubblico come il Codice dell'amministrazione digitale (d.lgs. 82/2005), che ancora sconta inattuazioni proprio a causa della mancanza di risorse che permettano anche un'adeguata formazione e cultura interne alle pubbliche amministrazioni (profilo su cui tornerò più avanti). A tal proposito richiamo l'attenzione sui ritardi e sulle inattuazioni che ha scontato la nomina del Responsabile per la transizione digitale previsto dall'art. 17 d.lgs. 82/2005. Il rischio è anche in tal caso l'inattuazione oppure un'attuazione formale e non sostanziale, con il pericolo che le disposizioni rimangano solo mere pregevoli dichiarazioni di intenti, ma non si traducano nella realtà in norme effettive ed omogeneamente attuate;

2) in merito all'art. 2, comma 2, si pone un'**eccezione alle sanzioni** in caso di mancata o ritardata adozione degli interventi risolutivi indicati dall'Agenzia per la cybersicurezza nazionale in caso di "**motivate esigenze di natura tecnico-organizzativa**": data la genericità e indeterminatezza del concetto si suggerisce di integrare la disposizione, prevedendo che tali esigenze siano definite nelle apposite linee guida predisposte da ACN (previste all'art. 1), al fine di non creare criticità e difformità applicative della stessa norma;

3) per quanto riguarda l'art. 6, commi 1 e 2, e la relativa individuazione, anche tra quelle esistenti, di una struttura dedicata alla cybersicurezza nel cui alveo si colloca il **Referente per la cybersicurezza** si suggerisce di integrare la disposizione prevedendo che tale **figura operi d'intesa e in collaborazione con le figure già esistenti** nelle pubbliche amministrazioni quali il Responsabile per la transizione digitale (previsto dall'art. 17 del d.lgs. 82/2005) e il *Data Protection Officer* (DPO) o Responsabile della protezione dei dati (RPD) (previsto dall'art. 37 ss. del regolamento europeo 2016/679), in considerazione anche delle necessaria collaborazione e cooperazione tra queste figure alla luce delle precipue e correlate competenze delle stesse. Inoltre si suggerisce di integrare la norma di cui all'art. 6, comma 2, che prevede l'individuazione della figura del Referente per la cybersicurezza "in ragione delle **qualità professionali possedute**", dettagliando quali siano: al riguardo si suggerisce che tali qualità professionali siano specificate nelle linee guida adottate da ACN (richiamate nel comma 4 dell'art. 1 del disegno di legge), in modo da garantire profili di competenza solida e omogenea nelle

diverse realtà amministrative pubbliche coinvolte;

4) per quanto riguarda l'art. 7 in materia di **intelligenza artificiale** mostro alcune perplessità per l'indeterminatezza e l'ampiezza di alcuni termini impiegati, quali in specifico la locuzione "favorire un uso etico e corretto dei sistemi basati su tale tecnologia"; inoltre si suggerisce di integrare che tale promozione e sviluppo avvenga in sinergia con Agenzia per l'Italia Digitale (AgID), che dovrebbe avere funzione di vigilanza e controllo in materia di intelligenza artificiale, e gli altri soggetti istituzionali che abbiano un ruolo in relazione all'intelligenza artificiale, al fine di realizzare strategie condivise in modo orizzontale, evitando verticalizzazioni.

In merito a tale disposizione di cui all'art. 7 del disegno di legge ritengo inoltre debba essere presa in considerazione anche l'intelligenza artificiale come oggetto di attacchi informatici, oltre che come risorsa per il rafforzamento della cybersicurezza;

5) si suggerisce di integrare il Capo I del disegno di legge, prevedendo disposizioni dedicate alla **formazione**, alla **ricerca e** allo **sviluppo di adeguate competenze afferenti alla cybersicurezza, valorizzando il ruolo dell'Università**; in specifico si suggerisce l'introduzione di una norma con cui si obbligano i soggetti interessati dalle disposizioni ad attivare una specifica **formazione delle proprie risorse umane**, funzionale a garantire l'effettiva e corretta applicazione delle norme stesse e una solida cultura in materia di cybersicurezza. Al riguardo mi permetto di suggerire anche la formulazione, ossia prevedere lo sviluppo di adeguate "competenze tecnologiche, di informatica giuridica e manageriali" per la figura del Referente per la cybersicurezza e per coloro che opereranno nelle strutture che le amministrazioni dovranno costituire ai sensi dell'art. 6, anche grazie a partenariati tra soggetti pubblici e privati in particolare con le Università, che possono vantare competenze e linee strategiche in materia, anche al fine di creare quella consapevolezza, parte integrante e indispensabile della cultura digitale (come emendamento si suggerisce di integrare l'art. 6 con un comma che preveda quanto proposto). Preme precisare che la locuzione suggerita è già in uso nel nostro ordinamento giuridico, specificatamente nell'art. 17 del d.lgs. 82/2005 (CAD) per quanto attiene al Responsabile per la transizione digitale e garantisce, pertanto, omogeneità tra le disposizioni e tra figure che devono necessariamente collaborare e che devono essere

dotate di competenze specifiche al fine di svolgere il proprio ruolo.

Ritengo che parimenti sia opportuno prevedere **azioni di cultura digitale rivolte alla collettività** per elevare la consapevolezza generale in materia e rafforzare la sicurezza nella dimensione digitale di tutti e ciascuno e non solo nella realtà analogica (la formulazione può avvenire sul modello dell'art. 8 del d.lgs. 82/2005, Codice dell'amministrazione digitale); anche in tal caso ruolo di primo piano possono svolgere le Università;

6) si suggerisce di integrare il Capo I del disegno di legge, prevedendo che il personale impegnato nelle strutture per la cybersicurezza, di cui all'art. 6, sia valutato ai fini del processo di **misurazione e valutazione della performance** anche in base al rispetto e all'attuazione di quanto previsto nell'art. 6 e al corretto adempimento degli obblighi ivi previsti, a fini di effettività ed efficacia;

7) in considerazione del fatto che le disposizioni si applicano parimenti ad amministrazioni pubbliche profondamente diverse (nazionali, regionali e locali) si suggerisce di integrare il Capo I del disegno di legge con la previsione di puntuali **meccanismi istituzionali atti a garantire il solido coinvolgimento delle Regioni, degli enti locali e dei diversi livelli istituzionali** in linea con il modello partecipato, federato e non gerarchico, che caratterizza il nostro ordinamento, e atta ad assicurare omogeneità territoriale nell'applicazione delle disposizioni stesse;

8) in merito al Capo II del disegno di legge, in considerazione della diffusione e del cruciale ruolo che svolgono le **firme elettroniche** si suggerisce di rafforzare le sanzioni previste nell'art. **640-quinquies sulla frode informatica del soggetto che presta servizi di certificazione di firma elettronica**, che prevede per il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, la reclusione fino a tre anni e la multa da 51 a 1.032 euro;

9) si suggerisce, infine, di intervenire sul **trattamento illecito di dati personali e**

**altri illeciti penali relativi alla protezione dei dati personali**, di cui all'art. 167 ss. d.lgs. 196/2003, che risultano invariati, in particolare alla luce dell'**uso massivo di *big data*** possibile con sistemi di intelligenza artificiale. Si reputa opportuno considerare il profilo ed inasprire le sanzioni in tali fattispecie, anche in considerazione dei possibili destinatari delle sanzioni stesse.

Resto a disposizione per approfondimenti e ringrazio per l'invito e per l'attenzione.

Fernanda Faini, PhD

Ricercatrice in *tenure track* e docente di informatica giuridica

Università Telematica Pegaso