L'istituzione della figura del "referente per la cybersicurezza" nel d.d.l. 16 febbraio 2024 ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" – A.C. 1717)

di Stefano Rossa - pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale, 8 maggio 2024

È attualmente in discussione al Parlamento italiano il disegno di legge del 16 febbraio 2024, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (A.C. 1717). Fra le varie norme, il d.d.l. prevede l'introduzione del referente per la cybersicurezza, figura volta a colmare un vuoto organizzativo importante in una Pubblica Amministrazione in cui il rischio cyber *assume di giorno in giorno maggior centralità.*

È evidente a tutti che il tema della *cybersecurity* stia assurgendo con insistenza alle cronache. Se fino a qualche anno addietro gli attacchi *cyber* erano diretti prevalentemente verso imprese e privati per finalità criminali, le recenti **tensioni geopolitiche** mondiali stanno invece ponendo gli Stati – e più in generale i soggetti pubblici – al centro dell'azione degli attaccanti. La ragione è intuibile: la (relativa) semplicità di un attacco virtuale, se rapportata con gli enormi danni fisici che esso è in grado di causare – si pensi ai danni di un *malware* al funzionamento della rete di una centrale nucleare – rende l'attacco informatico un'efficace e performante arma bellica da impiegare unitamente a quelle "tradizionali".
Se questo aspetto lo si somma alla **pervasività e alla enorme diffusione della tecnologia digitale** nella società civile, che richiede necessariamente che essa sia sicura sul piano informatico, emerge con forza la crescente centralità del c.d. rischio *cyber*. Il quale si traduce nell'esigenza di avere un ciberspazio sicuro e resiliente e, prima ancora, di giungere a una consapevolezza minima generalizzata della *cybersecurity*.
Contezza che tendenzialmente le imprese possiedono già, soprattutto quelle più grandi e strutturate. Ma che, invece, non è ancora pienamente maturata nella cittadinanza (come evidenziato dai livelli di alfabetismo digitale presenti in Italia, come emerge dal DESI 2023) e, di converso, nella Pubblica Amministrazione.
A testimonianza di ciò, si pensi che il **CISO** (*Chief Information Security Officer*) è una figura essenziale nell'organizzazione aziendale delle imprese, ma **non compare invece nella compagine organizzativa delle Amministrazioni Pubbliche**, in cui la responsabilità per i profili di sicurezza informatica è attribuita a figure differenti individuate negli specifici casi, in base al principio di auto-organizzazione, le quali però non sono istituite con tale preciso fine (si pensi, ad esempio, al responsabile della transizione digitale, il quale *ex* art. 17 co. 1 lett. *c*) del d.lgs. n. 82 del 2005 svolge *anche* la funzione di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture).
Anche per colmare questa criticità il 16 febbraio 2024 è stato presentato alla Camera dei Deputati il Disegno di legge ordinario contente "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (A.C. 1717), attualmente in corso d'esame alle Commissioni riunite Affari Costituzionali e Giustizia della Camera (è possibile consultarne il testo qui, mentre la pagina relativa ai lavori preparatori del progetto di legge sul sito istituzionale della Camera dei Deputati è consultabile qui).
Fra le diverse novità normative previste, il d.d.l. introduce all'art. 6 l'obbligo di individuare nella struttura organizzativa delle maggiori Amministrazioni (fra cui: Regioni, Province autonome di Trento e Bolzano; Comuni con più di 100 mila abitanti; Comuni capoluogo di Regione; società di trasporto pubblico urbano con bacino di utenza superiore a 100 mila abitanti; ASL) **un'apposita struttura, preposta alle attività di cybersicurezza,**

istituita *ex novo* oppure individuata fra le strutture già esistenti. Tale struttura sarà chiamata a sviluppare politiche e procedure di cybersicurezza; a elaborare e aggiornare il piano per il rischio *cyber*, nonché il documento interno relativo all'organizzazione e ai ruoli del sistema per la cybersicurezza informativa; pianificare e attuare interventi di potenziamento della capacità gestionale del rischio *cyber* e delle misure previste dalle linee guida emanate dall'Agenzia per la cybersicurezza nazionale (ACN); nonché monitorare e valutare le minacce alla cybersicurezza dei propri sistemi informativi.
Il d.d.l. prevede altresì l'obbligo di individuare, all'interno della citata struttura per la cybersicurezza, la figura del **referente per la cybersicurezza**. Questi rivestirà il ruolo di punto unico di contatto fra la specifica Pubblica Amministrazione di appartenenza e l'ACN, alla quale deve essere pertanto comunicato il nominativo del referente *cyber*. In considerazione della delicatezza dei compiti affidatele, tale figura deve essere necessariamente selezionata o individuata in considerazione dell'elevata professionalità tecnica richiesta.
Posto che sono sottratti a tali obblighi, da un lato, il DIS, l'AISE e l'AISI, e dall'altro, i soggetti ricompresi nell'ambito del Perimetro di sicurezza nazionale cibernetica, è doveroso però sottolineare come il disegno di legge non preveda lo stanziamento di apposite risorse finanziarie, stabilendo all'art. 18 la clausola di invarianza finanziaria.
Proprio quest'ultimo profilo rappresenta un freno evidente alla concreta realizzazione di quanto previsto dal d.d.l., condizionando negativamente le novità previste dal testo che – almeno per quanto attiene all'introduzione della figura del referente per la cybersicurezza – sono correlate al disegno dell'organizzazione amministrativa. Come è stato sottolineato nelle audizioni informali al disegno di legge, fra gli altri dal Prof. Francesco Cardarelli (audizione consultabile qui, in particolare al min. 1:39:06 ss.), per il quale l'**invarianza finanziaria prevista dal d.d.l. in relazione ai profili organizzativi della PA** rappresenterebbe «un'araba fenice», e dal Dott. Luigi Garofalo (audizione consultabile qui al minuto 1:05:32 ss.), proprio **la mancanza della previsione di apposite risorse finanziarie ostacolerebbe la possibilità di attrarre, e dunque assumere nella Pubblica Amministrazione, figure professionali dotate di elevate competenze tecniche**. Un'altra criticità emersa, ed evidenziata sempre durante le audizioni informali, in particolare dall'Avv. Stefano Mele (audizione consultabile qui al minuto 58:59 ss.), concerne l'assenza nel testo del d.d.l. di un periodo temporale transitorio per dare attuazione a queste nuove norme, soprattutto qualora dovesse servire formare professionalmente chi sarà chiamato a rivestire il ruolo di referente per la cybersicurezza. Infine, un ulteriore profilo critico, come è stato puntualmente messo in luce nell'audizione informale dal Prof. Erik Longo (audizione consultabile qui al minuto 3:03:51, di cui il cui testo in esteso è invece consultabile qui) è legato alla **mancata previsione di una struttura di coordinamento decentrata sul territorio nazionale** – come nel caso dei *Security Operations Center* (SOC) regionali o della rete dei *Computer Security Incident Response Team* (CSIRT) – la quale potrebbe aiutare i costituendi referenti per la cybersicurezza a svolgere al meglio le proprie funzioni.
Essendo ancora un disegno di legge, è probabile che l'A.C. 1717 subirà modifiche prima di diventare legge dello Stato. Se le intenzioni del legislatore sono chiare e sono finalizzate a rendere il più resiliente possibile il sistema di cybersicurezza pubblica, è auspicabile che nelle successive fasi legislative le osservazioni emerse, così come quelle che emergeranno, siano fatte proprie dal Parlamento onde correggere i profili critici evidenziati. E proprio in questa direzione si collocano i recentissimi emendamenti al testo del disegno di legge proposti per superare la clausola dell'invarianza finanziaria e prevedere apposite risorse finanziarie (emendamenti consultabili qui inserendo gli estremi del d.d.l.).