Audizione Anitec-Assinform Confindustria Digitale

1° luglio 2021

DECRETO-LEGGE 14 giugno 2021, n. 82, "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"

Commissioni riunite I e IX (Affari Costituzionali e Trasporti) Camera dei Deputati

- Come Confindustria Digitale e Anitec-Assinform abbiamo seguito e supportato nel tempo l'evoluzione della normativa nazionale sulla cybersecurity, guidata negli ultimi anni dal Nucleo di Sicurezza Cibernetica, e giudichiamo positivamente le molte iniziative_che si sono succedute, fino alle ultime norme sul Perimetro Nazionale di Sicurezza Cibernetica.
- Riteniamo che con questo DL il Governo riconosca, come in passato sempre evidenziato da Confindustria Digitale, che non è possibile procedere a una trasformazione digitale pervasiva in assenza di cybersicurezza e che è quindi indispensabile disporre di meccanismi normativi e organizzativi tali da garantire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza nonché lo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza.
- Questa collaborazione assume ovviamente ancora maggiore rilievo alla luce della necessità di implementare la digital transition quale parte del Piano nazionale di ripresa e resilienza, azione a cui il piano alloca il 27% dei fondi stanziati dalla Recovery and Resilience Facility.
- In questo contesto, le azioni per l'adozione di un approccio "*cloud first*" (ad esempio lo sviluppo del Polo Strategico Nazionale) e la razionalizzazione dei processi delle amministrazioni in ottica di interoperabilità, per giungere a soluzioni "*once only*" sono una priorità che il settore vede con estremo favore, e per cui apprezziamo che l'importanza della cybersicurezza sia confermata dall'allocazione a questo capitolo di investimento del 10% dell'importo per la digitalizzazione delle PA.
- La stessa attenzione dovrà certamente essere posta anche all'allocazione degli investimenti in cybersecurity per quanto concerne la trasformazione digitale del tessuto produttivo, superando, ad esempio, nell'investimento per Transizione 4.0, le logiche che avevano inizialmente escluso la cybersicurezza - ma anche altri servizi innovativi - dall'implementazione di Industria 4.0. La situazione continua a non essere chiara, con ricerche che portano risultati contrastanti (sono state rese note in questi giorni due ricerche che dichiarano, da un lato, che Industria 4.0 ha interessato soprattutto medie e grandi aziende e, dall'altro invece, che le PMI durante la pandemia hanno continuato ad investire nella trasformazione industriale, con un 26% in tecnologie digitali, tra cui il top è cybersicurezza).
- È evidente che la digitalizzazione è ormai una componente trasversale di qualunque settore di attività e porta in tutti i settori rischi e vulnerabilità condivisi e caratteristici del mezzo digitale stesso. La frammentazione delle competenze di cybersicurezza costituisce, in generale, una

limitazione per il contrasto alle minacce e la risposta agli attacchi, ed è quindi positivo che la si superi sia a livello pubblico che a livello privato e che si attivi un coordinamento che possa meglio indirizzare le problematiche esposte.

- Le aziende del settore dispongono di capacità significative che possono essere messe a disposizione di una governance integrata della cybersicurezza nazionale, in termini sia di capacità progettuali, sia di piattaforme, sia di servizi: dal test, alla formazione, al monitoraggio alla gestione degli incidenti.
- È in effetti necessario fare ancora passi significativi per riuscire a portare la cultura e la pratica della cybersicurezza in un tessuto economico come quello italiano, caratterizzato dalla presenza di un numero elevatissimo di PMI, che, per natura e dimensioni, incontrano difficoltà nell'agganciare i temi della transizione digitale e l'indispensabile tema della sicurezza ad essa collegato. In questo senso auspichiamo che l'Agenzia svolga, come previsto, un ruolo significativo e siamo disponibili come federazione ed associazioni confindustriali a collaborare con l'Agenzia, anche proseguendo attività che già svolgiamo mediante le strutture territoriali di Confindustria ed i Digital Innovation Hub.
- In conclusione, consideriamo positivamente la razionalizzazione proposta, già peraltro effettuata in altri paesi come Francia e Gran Bretagna, creando una singola struttura, con unitarietà di intenti ed azioni, che consente di rendere più agevolmente operative le decisioni e le strutture definite. Auspichiamo che l'Agenzia possa realmente costituire il punto di contatto dell'industria per la gestione delle problematiche di cybersicurezza, come previsto dai diversi articoli del DL che includono l'industria ed il settore privato tra gli interlocutori dell'Agenzia, anche attraverso l'istituzione di un tavolo permanente che consenta un adeguato confronto e approfondimento dei temi rilevanti, nonché consenta di limitare le distorsioni e le incertezze nella fase di prima applicazione delle disposizioni, con riferimento ad esempio alla data da cui decorre l'obbligo di comunicazione al CVCN, a tutela soprattutto delle PMI.
- Riteniamo, da ultimo, che le tempistiche di attuazione, unitamente alla piena disponibilità del personale destinato dal DL, così come il ruolo individuato per l'Agenzia quale *Centro nazionale di coordinamento italiano*, che si interfaccerà con il *Centro europeo di competenza per la cybersecurity nell'ambito industriale, tecnologico e della ricerca,* saranno dunque essenziali per garantire il raggiungimento degli obiettivi prefissi. e, con essi, la creazione di un ecosistema che consenta al nostro Paese di poter competere alla pari degli altri sul piano della cybersecurity – e delle ricadute dirette e indirette – contribuendo, così, al rafforzamento del mercato unico europeo.