La strategia nazionale sulla Cybersecurity e la competitività

Vittorio Calaprice Rappresentanza in Italia della Commissione Europea
Stefania Ducci Agenzia sulla Cybersicurezza Nazionale
Agostino Santoni Vicepresidente di Confindustria con delega per il digitale
Marco Pierpaoli Giunta Camera Commercio delle Marche delega alla digitalizzazione
Roberto Basso Director External Affairs & Sustainability Wind Tre S.p.A.
Laura Castelnovo Samsung Electronics Italia
Rodolfo Mecozzi Cybersecurity e Digital Protection EY Advisory S.p.A.
Moderatore Marco Baldi Univ. Politecnica delle Marche

La sessione sulla Cyber Security è intitolata alla Strategia Nazionale sulla Cyber Security e la competitività, infatti realizzare prodotti ha un costo, utilizzare prodotti sicuri, anche dal punto di vista Cyber, ha un costo maggiore e quindi sicuramente ha un effetto sulla competitività a qualunque vincolo o qualunque requisito che serva a garantire la Cyber Security ha un effetto sui costi e quindi sulla competitività stessa. Emerge quindi il tema di trovare un punto di equilibrio tra la necessità di garantire sistemi dispositivi, infrastrutture sicure a livello nazionale, internazionale e però garantire, salvaguardare la competitività del nostro sistema produttivo. Quindi sono due esigenze che possono in qualche modo convivere o sono destinate a confliggere?
L'Unione Europea sta costruendo un'architettura di governance della e per la Cyber Security e la sta costruendo in particolare a partire dal 2020 attraverso tre strumenti che sono a sua disposizione.
Il primo è quello legato al coordinamento delle politiche e quindi l'insieme delle strategie dei singoli paesi, guidate dalla Commissione Europea, così come anche il rafforzamento o la nascita di alcune strutture, che da qui a breve avranno anche il compito di coordinare l'insieme di queste strategie, come l'agenzia ISA o la nuova Cyber-competence Center. Il secondo una definizione regolatoria normativa formata dagli atti come il Cyber Security Act, che ha dato l'impulso al tema delle certificazioni, al rafforzamento della direttiva NIS, con la NIS2, DORA (Digital Professional Resilience Act) e da qualche settimana anche la proposta di un Cyber Resilience Act. Questo è l'apparato normativo che sta accompagnando la costruzione dell'architettura Cyber Security della dell'Unione Europea.
Il terzo aspetto si interviene anche la parte del supporto finanziario degli investimenti e attraverso appositi programmi uscito solo il programma Digital Europe che per la prima volta nella programmazione 2021-2027, ha il compito anche di rafforzare il sistema della competitività delle imprese Cyber e della ricerca che viene anche supportato dal programma Horizon Europe e coordinato anche da insieme dei bandi dall'agenzia AIDEA. È stato appena pubblicato un importante bando per quasi 170 milioni di euro, proprio nel campo della Cyber Security.
La competitività è parte di questo processo anzi anche il fine, per la necessità di costruire l'autonomia strategica nel campo dei prodotti e dei processi di Cyber dell'Unione Europea. Questo è un obiettivo politico che passa attraverso la collaborazione di tutti enti pubblici diciamo strutture pubbliche e strutture private appartenevano pubblico privato è un'altra parte fondamentale di questo processo ed è chiudo la parte che dovrà coniugarsi con le competenze e con il capitale umano è stato messo in evidenza sin dall'inizio ho ascoltato alcuni interventi questa mattina ed è anche su questo la competitività passa cioè su un rafforzamento la qualità del capitale umano. Il prossimo anno il 2023 sarà l'anno europeo delle competenze. La

presidente Ursula Von den Leyen ha chiesto agli Stati membri e tutte le autorità di lavorare sulla definizione di un quadro anche di rafforzamento delle competenze. Tra queste sicuramente le competenze digitali e quelle Cyber saranno non solo necessarie, ma saranno sempre più richieste.
A livello nazionale, il programma elaborato dell'agenzia per la Cyber sicurezza nazionale a supporto dello sviluppo di nuove imprenditorialità innovativa la valorizzazione dei risultati della ricerca pubblica partendo innanzitutto dalla strategia nazionale di Cyber sicurezza e analizzando poi quali sono i filoni tecnologici di interesse, partendo dall'innovazione tecnologica non solo dell'Industria, ma dell'intero sistema paese. I filoni tecnologici di interesse per l'agenzia e su cui si vanno a focalizzare poi le successive due aree di intervento sono: Cyber Security propriamente inteso, ma anche la data Science e la blockchain, e le componenti Cyber negli ambiti robotica, automotive e spazio, l'intelligenza artificiale, i quantum computer, la crittografia e le criptovalute.
Al fine di implementare le iniziative del piano di implementazione della strategia, l'agenzia ha elaborato due aree di intervento:
l'area di intervento 1 già diciamo così programmato nel breve periodo, che già in qualche modo anche partita;
mentre l'aria di intervento 2 intervento programmato, nel medio periodo che partirà invece nella primavera del prossimo anno.
La prima area di intervento prevede lo sviluppo di nuove imprenditorialità innovative, start up principalmente e spinoff in collaborazione con programmi di incubazione e accelerazione. Mentre l'area di intervento 2 prevede il supporto e la valorizzazione dei risultati della ricerca pubblica in collaborazione con quelli che sono i Technology Transfer Office delle Università, enti pubblici di ricerca.
Innanzitutto, l’obiettivo è quello di costruire un ecosistema stabile un Innovation network, per sviluppare nuove realtà imprenditoriali, sotto forma di startup e spin-off e al fine di aiutarle utilizzandole la valorizzazione e lo sviluppo delle tecnologie emergenti. Vengono sostenuti con contributi a fondo perduto sia per progetti di validazione fino a un massimo di 25 mila euro che per progetti di sviluppo fino a un massimo come vedete di 175 mila euro per cui i fondi che potranno essere erogati per singola startup, non potranno superare nel complesso i 200 mila euro.