# Cybersecurity, cosa prevede il PNRR? Quali sono i compiti dell'Agenzia per la cybersicurezza nazionale?

*intervista a Valentina Procopio, laureanda in Giurisprudenza, socio giovane ANSSAIF*

**Ci può riassumere i contenuti del Next Generation EU riguardanti la trasformazione digitale?**

L'Unione Europea ha risposto alla crisi pandemica con il Next Generation EU, programma di investimenti e riforme per accelerare la transizione ecologica e digitale; migliorare la formazione delle lavoratrici e dei lavoratori e conseguire maggiore equità di genere, territoriale e generazionale. I due principali strumenti del NGEU sono il "Recovery and Resilience Facility" (RRF) e il "React-Eu".

Il dispositivo RRF richiede agli Stati membri di presentare un pacchetto di investimenti e riforme: l'Italia ha presentato il Piano Nazionale di Ripresa e Resilienza (PNRR). Il Regolamento RRF richiede che i piani presentati dagli Stati dedichino almeno il 20% della spesa complessiva per investimenti e riforme alla transizione digitale, comprendano la razionalizzazione e digitalizzazione della pubblica amministrazione e lo sviluppo dei servizi pubblici digitali, migliorino la connettività, prevedano costi sostenibili per gli utenti e un aumento della velocità di realizzazione della rete, e infine sostengano la ricerca e lo sviluppo nelle tlc, l'adozione delle tecnologie digitali da parte delle imprese, l'aumento delle competenze e la capacità di accesso a strumenti e servizi digitali di cittadini e lavoratori.

**Quali sono le risposte che il PNRR prevede al riguardo?**

Nel PNRR troviamo risposte alla richiesta del Regolamento RRF nella Missione 1 *("Digitalizzazione, innovazione, competitività, cultura e turismo")*, articolata in tre componenti.

La Componente 1 incoraggia la digitalizzazione della Pubblica Amministrazione. La digitalizzazione della PA viene attuata agendo da un lato su aspetti di infrastruttura digitale: si prevede la migrazione al cloud delle amministrazioni e l'accelerazione dell'interoperabilità tra gli enti pubblici, si contempla lo snellimento delle procedure secondo il principio "once only" (per cui le pubbliche amministrazioni devono evitare di chiedere a cittadini e imprese informazioni già fornite in precedenza) e si considera il rafforzamento delle difese di cybersecurity.

Dall'altro lato, vengono estesi i servizi ai cittadini, migliorando l'accessibilità e adeguando i processi prioritari delle amministrazioni centrali agli standard condivisi da tutti gli stati membri dell'Unione.

La Componente 2 promuove l'innovazione e la digitalizzazione del sistema produttivo attraverso diversi interventi: vengono incentivati investimenti tecnologici, ricerca e sviluppo e promossa una riforma del sistema di proprietà industriale, vengono introdotte misure dedicate alla trasformazione delle piccole e medie imprese e misure a supporto

dei processi di internalizzazione e competitività delle filiere industriali. Infine vengono inclusi importanti investimenti per garantire la copertura di tutto il territorio con reti a banda ultra-larga.
La Componente 3 rilancia i settori economici della cultura e del turismo, tramite interventi di valorizzazione di siti storici e culturali per migliorarne capacità attrattiva, sicurezza e accessibilità.

**Come viene affrontato il problema della cybersecurity nella PA?**
La trasformazione digitale della PA contiene misure di rafforzamento delle difese cyber del Sistema Paese, a partire dalla piena attuazione della disciplina in materia di "Perimetro di Sicurezza Nazionale". Il quinto investimento previsto per la Componente 1 della prima missione del PNRR è destinato alla cybersecurity ed è organizzato su quattro aree di intervento : in primo luogo, vengono rafforzati i presidi di front-line per la gestione degli alert e degli eventi a rischio intercettati verso la PA e le imprese di interesse nazionale; in secondo luogo, vengono costruite e consolidate le capacità tecniche di valutazione e di audit della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale per lo Stato; in terzo luogo si investe nell'immissione di nuovo personale nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e investigazione del crimine informatico; infine sono irrobustiti gli asset e le unità cyber incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber.

**Quali sono stati i passaggi costitutivi dell'Agenzia per la Cybersicurezza Nazionale?**
Negli allegati tecnici al PNRR si prevede, tra l'altro, l'individuazione di un nuovo organismo per la sicurezza informatica nazionale che guidi l'architettura nazionale generale della cybersicurezza. Alla luce di tale previsione con il decreto-legge 82 del 2021 è stata disposta l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN). Il Dpcm 16 settembre del 2021 definisce i termini e le modalità del trasferimento di funzioni, beni strumentali e documentazione dal Dipartimento delle informazioni per la sicurezza all'Agenzia.

**Quali sono i suoi compiti?**
Finalità ultima dell'Agenzia è la promozione della cultura della sicurezza cibernetica e la consapevolezza nei settori pubblico e privato e nella società civile dei rischi e delle minacce cyber. Tra i principali compiti affidati all'Agenzia dall'art 7 del decreto-legge 82 del 2021:
• esercizio delle funzioni di autorità nazionale in materia di cybersecurity, a tutela degli interessi nazionali e della resilienza dei servizi e delle funzioni essenziali dello Stato da minacce cibernetiche;
• prevenzione, monitoraggio, rilevamento e mitigazione, per far fronte agli incidenti di sicurezza informatica e agli attacchi informatici, anche attraverso il Computer Security Incident Response Team (CSIRT) italiano e l'avvio operativo del Centro di valutazione e certificazione nazionale;
• innalzamento della sicurezza dei sistemi di Information and communications technology (ICT) dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, delle pubbliche amministrazioni, degli operatori di servizi essenziali (OSE) e dei fornitori di servizi digitali (FSD);
• supporto allo sviluppo di competenze industriali, tecnologiche e scientifiche;
• funzione di interlocutore unico nazionale per i soggetti pubblici e privati in materia di misure di sicurezza e attività ispettive negli ambiti del perimetro di sicurezza nazionale cibernetica, della sicurezza delle reti e dei sistemi informativi (direttiva NIS), e della sicurezza delle reti di comunicazione elettronica.

**Quali sono i tempi previsti per la sua piena operatività?**
Si prevede la piena operatività dell'Agenzia dal primo gennaio 2022. Alcune operazioni sono già state effettuate: inglobate le prime competenze dal Dis (60 esperti), ed è operativo l'NCS (Nucleo per la Cybersicurezza Nazionale) e direzione del CSIRT (Computer Security Incident Response Team – Italia).