

Come superare le fragilità digitali

23 Maggio 2025

Innovazione, regole chiare e cultura del dato per creare infrastrutture sicure e al servizio dei cittadini.

Fondazione Bruno Kessler, PagoPA, Istituto Poligrafico Zecca dello Stato, Synapsed e lo Studio Legale Lisi hanno affrontato la questione alla XX edizione del Festival dell'Economia nell'incontro intitolato "[*Fragilità delle infrastrutture digitali: cosa fare? Opportunità e sfide*](#)", moderato da Filomena Greco, giornalista de Il Sole 24 Ore.

*"L'obiettivo della Provincia autonoma di Trento è di creare un ecosistema digitale amministrativo che sia efficiente, integrato e interoperabile – ha affermato **Achille Spinelli, Vicepresidente e Assessore allo sviluppo economico, lavoro, famiglia, università e ricerca** – e in questo senso abbiamo già attivato diversi progetti grazie a fondi della programmazione europea e PNRR. Guardiamo alla semplificazione e alla velocità come veri valori. Ma guardiamo con grande favore e accompagniamo progetti importanti sul nostro territorio, come quello di Università di Trento e Fondazione Bruno Kessler relativo a una infrastruttura – una vera "miniera" – che renderà i nostri dati ancora più sicuri, ampliando capacità di calcolo e possibilità di fare ricerca".*

Ad aprire gli interventi è stato Roberto Viola, **Direttore Generale della DG CONNECT (Direzione Generale Comunicazione, Reti, Contenuti e Tecnologie) della Commissione Europea**: *"Tecnologie emergenti come il cloud-edge computing, l'IA e il 5G e 6G, aprono le porte ad enormi opportunità, ma comportano anche sfide significative per garantire la cybersicurezza. Gli investimenti e le normative UE sulla sicurezza delle catene di approvvigionamento basate su fornitori affidabili, sulla certificazione dei prodotti e sulla protezione delle nostre infrastrutture più importanti spianano la strada ad un futuro tecnologico sicuro".*

Esistono infrastrutture pubbliche digitali – ad esempio quelle sviluppate da PagoPA con il suo sistema di pagamento o l'app IO – che sono utilizzate quotidianamente da milioni di cittadini e

migliaia di enti. Alla base di questi ecosistemi c'è una visione strategica incentrata **sull'interoperabilità, sulla modularità delle soluzioni, sull'usabilità e, soprattutto, sulla sicurezza**. Questo è quanto ha spiegato **Maurizio Fatarella, Direttore Generale di PagoPA**, raccontando l'arrivo di un nuovo strumento: *l'IT-Wallet, il portafoglio digitale italiano*, pensato non solo per semplificare l'accesso ai servizi, ma anche per rafforzare l'identità digitale e la protezione dei dati personali, con benefici evidenti in termini di sicurezza e tutela della privacy.

Anche **l'Istituto Poligrafico e Zecca dello Stato (IPZS)** gestisce servizi digitali critici per la vita del cittadino e del Paese e sta lavorando alla definizione e alla realizzazione della nuova piattaforma di identità digitale, nell'ottica della sicurezza interoperabile e della centralità del cittadino. Nel progetto IT-Wallet, ha spiegato **Andrea De Maria, Innovation manager per IPZS**, l'istituto contribuisce con la creazione e la gestione delle componenti del sistema che garantiscono sicurezza, affidabilità e integrabilità con le infrastrutture esistenti, fornendo ai cittadini un controllo consapevole sulla propria identità digitale.

Ma dietro a questi sistemi c'è sempre un enorme lavoro di ricerca tecnico-scientifica, oggetto di studio del **Centro Cybersecurity della Fondazione Bruno Kessler**. Il **Direttore Silvio Ranise, Professore Ordinario dell'Università di Trento**, ha infatti messo in luce le principali vulnerabilità che caratterizzano gli ecosistemi digitali complessi, oggi sempre più pervasivi e interconnessi. *“Rendere questi sistemi affidabili richiede un lavoro coordinato su almeno tre livelli: identità digitale, protezione dei dati e affidabilità dell'intelligenza artificiale”*. Sul primo fronte, è importante adottare un approccio “zero trust” nella gestione dell'identità: **ogni richiesta di accesso, sia essa di un utente o di un sistema, deve essere esplicitamente verificata**. La delicata fase di emissione delle credenziali digitali, ad esempio nel caso dei wallet europei per la gestione dell'identità digitale, rappresenta un punto di vulnerabilità strategica e necessita di garanzie crittografiche forti. Occorre poi **bilanciare facilità d'uso e sicurezza**, implementando **misure che rendano questi servizi resilienti**. E infine **il lavoro di protezione dei dati per garantire trasparenza ed accuratezza dei risultati**.

*“La **Fondazione Bruno Kessler** – ha concluso **Ranise** – ha istituito al suo interno un laboratorio congiunto sulla cyber-sicurezza, per accrescere l'impatto pratico della propria ricerca e allo stesso tempo migliorare la propria postura di sicurezza e guidare la trasformazione per la conformità alla direttiva europea NIS2 supportando le organizzazioni trentine, nazionali ed internazionali”*.

A riportare la prospettiva delle imprese che operano nel settore della sicurezza IA è stato **Matteo Meucci, CEO di Synapsed**, che ha condiviso i risultati di uno studio recentemente condotto su dieci modelli di intelligenza artificiale generativa, tutti rivelatisi vulnerabili a diverse forme di attacco. **Meucci** ha evidenziato quanto l'IA, pur promettendo enormi benefici, necessiti di un **quadro operativo rigoroso**, in cui le organizzazioni siano in grado di **testare, monitorare e**

correggere attivamente i propri sistemi.

E dunque, non può mancare la parte regolatoria e legale: **l'avvocato Andrea Lisi** ha spostato l'attenzione sulle implicazioni giuridiche e politiche della gestione delle infrastrutture digitali, specie quando affidate a soggetti esterni, spesso extraeuropei. **Lisi** ha sollevato il rischio di una eccessiva frammentazione normativa, suggerendo un ritorno ai fondamentali: **mettere al centro il dato, inteso non solo come risorsa tecnica ma come bene politico e culturale**. Servono quindi **formazione continua, alfabetizzazione digitale dei cittadini e nuove figure professionali capaci di coniugare diritto, etica, tecnologia e governance**.

Affrontare la fragilità delle infrastrutture digitali è quindi possibile, con uno sforzo collettivo che abbracci competenze tecniche, capacità regolatorie, visione strategica e sensibilità sociale in una governance condivisa.



Gli interventi di Roberto Viola – Direttore Generale della DG CONNECT della Commissione Europea e Accademia di Scienze Economiche, lavoro, famiglia, università e ricerca

LINK

<https://magazine.fbk.eu/it/news/come-superare-le-fragilita-digitali/>

TAG

- #cloud

- #crowd strike
- #cybersicurezza
- #dati
- #festival economia
- #festivaleconomiatreto2025
- #identità digitale
- #infrastrutture digitali
- #intelligenzaartificiale
- #it wallet
- #pagopa
- #poligrafo
- #wallet
- #wallet digitale
- #zecca

MEDIA COLLEGATI

- Videointervista a Silvio Ranise, Direttore per il Centro Cybersecurity di FBK:
https://youtu.be/vq5UWbBY_OE