ATTUALITÀ

Sicurezza digitale: una, nessuna e centomila

di **Fondazione AIDR** · 2 febbraio 2021, 14:54

di Biagino Costanzo Dirigente d'Azienda e Socio Aidr e Aipsa

La digitalizzazione è ormai divenuta un mantra. Giusto parlarne, ma è anche giusto fare un po' di chiarezza e professione di verità sull'argomento.

Il digitale riguarda e riguarderà un enorme ventaglio di attività umane: pensiamo a quella sanitaria, lavorativa, scolastica, ambientale, energetica o alla Pubblica amministrazione e, ad esempio ai suoi innumerevoli archivi.

Nonostante i buoni propositi di investimenti costanti in nuove tecnologie volti ad una capillare digitalizzazione, questa è ben lontana dall'interessare tutto il territorio nazionale.

In ampie zone del nostro Paese, infatti, non arriva né la banda larga né la fibra ottica e se coniughiamo questo con la scarsa diffusione di competenze digitali, sia di base che avanzate, ecco che l'ostacolo sulla strada di una compiuta digitalizzazione diventa sempre più insormontabile.

L'Italia digitale è, come in molti altri ambiti, letteralmente divisa in due. Da una parte c'è la Sicilia, che sulla banda larga fa appena un po' meglio della Bulgaria, dall'altra ci sono la provincia autonoma di Trento, la Lombardia, il Veneto o il Friuli Venezia Giulia che su internet navigano al livello di città come Vienna o Barcellona. In pratica anche l'Italia 3.0, quella dello smart working e dell'e-learning durante il Coronavirus, ora anche del cash back, viaggia a velocità diverse.

Tutto questo si riflette in Europa dove, purtroppo, il nostro Paese si trova in coda alla classifica degli altri Paesi, oscillando tra la quartultima e terzultima posizione dell'Europa dei ventotto stati membri.

Secondo lo studio e gli indicatori del DESI, (il Digital Economy and Society Index 2020), i punti di debolezza dell'Italia si ravvisano proprio sul fronte del capitale umano, ossia la disponibilità di competenze digitali e dell'integrazione delle tecnologie digitali nei processi organizzativi e produttivi.

Saremo dunque ancora lontani dalla famigerata maturità digitale, fino a quando gli sforzi per amalgamare questi aspetti non saranno seriamente considerati elemento culturale.

C'è da dire, tuttavia, che negli ultimi anni l'Italia ha fatto molti progressi sotto il profilo della connettività: l'avvento del 5G ha dato un impulso senza precedenti, e la speranza è che possa essere sfruttato anche per raggiungere le zone del paese tuttora prive di una connessione veloce e affidabile.

È opportuno segnalare che, ad oggi l'utilizzo di internet è prevalentemente legato ad attività ludiche (fruizione di videoclip, musica, news e videogiochi) ed al commercio on line.

Dunque, al di là del diffuso utilizzo di smartphone e social media, il ricorso a clouding, iOT, big data, telemedicina, realtà simulata, long term forecasting, simulazioni ed altre attività in grado di sfruttare a pieno le potenzialità delle nuove tecnologie, resta molto limitato.

Nella Pubblica Amministrazione vi è moltissimo da fare. È ancora troppo evidente il gap tra gli sforzi messi in campo ora, seppur tardivamente, e l'impossibilità pratica di velocizzare tanti servizi utili alla cittadinanza.

Vi sono in essere programmi d'incentivazione messi a punto dal Mise, quali Impresa 4.0, Transizione 4.0 e ora Impresa 4.0Plus, che attribuiscono alle procedure amministrative gestite dalla burocrazia pubblica un peso decisivo per accelerare la trasformazione del sistema produttivo del Paese ma c'è ancora molta strada da fare.
Volendo poi discutere di dematerializzazione cartacea per quanto riguarda documentazione e archivi, è facile intuire che questo processo si debba necessariamente accompagnare ad una rimodulazione di tutti i processi coinvolti ed è su questo punto che, ci si scontra con una mentalità culturale tutta analogica. Questo è il vero scoglio della pubblica amministrazione.

Internet, digitale e sicurezza, ancora una volta i tre temi che molte volte non coincidono. I casi in Italia

Quando ci affidiamo alle "macchine" e all'intangibilità delle reti, è vitale predisporre una valida e potente politica di sicurezza affinché il digitale non diventi prateria sulle quali imperversa la criminalità in ogni sua forma.

In Italia la casistica, in nome del famoso detto "fatta la legge, trovato l'inganno" è sempre più varia e, per certi aspetti colmi di ironia, interessante.

È successo che a Milano, per il lauto compenso 5 mila euro, fosse possibile procurarsi illegalmente le generalità di alcune donne, per lo più all'oscuro (ma molte volte vi è stato costruito un vero e proprio business), per farle figurare partner in matrimoni misti ai fini di regolarizzazione di

cittadinanza in tutta fretta nei vari comuni. Ecco dunque il fenomeno delle spose digitalmente clonate.

Le frodi riguardanti le carte di credito poi, si arricchiscono di modalità diversificate.

Una prima versione semplice in cui, acquistando via telefono o via web, è sufficiente fornire il numero della carta e la data di scadenza per addebitare la spesa sul conto di malcapitati intestatari.

Laddove invece fosse necessaria fisicamente la carta di credito, ecco pronta una raffinata rielaborazione: gli specialisti della truffa sono in grado copiare la banda magnetica su una carta vergine (le cosiddette "White Card") per poi utilizzarla sino a quando non arriva il primo estratto conto sospetto.

La possibilità di manomettere il digitale per creare identità fittizie o mettere in atto dei furti di dati identificativi, permette facilmente di aprire linee telefoniche a nome di ignari che si vedranno poi recapitare bollette salate o, ancora, in ambito assicurativo ed automobilistico, consente ai malviventi di immatricolare vetture a nome di qualcun altro, cui spetteranno i diversi oneri di regolarizzazione sanzionatoria.

Poi vi è il più classico dei casi di frode fiscale via Internet, anche noto come "phishing".

È quello che ha colpito per esempio anni fa il sito del servizio on line di "Bancoposta" di Poste Italiane, dove con una falsa e-mail si chiedeva ai correntisti di accedere alla homepage del sito e controllare i propri dati, in realtà il link indicato nascondeva un portale pirata gestito dalla Croazia.

Si va da truffe con le carte di credito clonate e quelle on line, fino alle frodi legate all' "home banking", cioè la gestione via internet del proprio conto corrente, e al già citato "phishing", che consiste appunto, nell'appropriarsi dell' "identità bancaria" di un correntista effettuando operazioni a proprio favore.

Tra le frodi on line più diffuse sono quelle attraverso specifiche finestre che fanno comparire nei siti ufficiali delle banche, richiedono, mediante la compilazione di specifici moduli, tutte le coordinate e le relative password del correntista ed ecco fatto, si impossessano dell'identità bancaria ed effettuano liberamente bonifici bancari. Anche per i reati nel campo della telefonia, sia fissa che mobile, la tendenza è in costante crescita. Una tecnica molto in voga è quella dell' "sms esca" dove si annuncia una vincita. Si manda un messaggio sul cellulare annunciando la vincita di una somma per ritirare la quale bisogna chiamare un certo numero. Ovviamente non

esiste nessuna somma da ritirare e la vittima pagherà un conto salato per quella telefonata. In aumento sono anche le ricariche telefoniche clonate dagli hacker da appositi software.

Nel nostro Paese si può parlare di vero e proprio boom di reati tecnologici.

A testimoniarlo è il bilancio negli ultimi anni, dell'attività del **CNAIPIC** (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) della Polizia Postale che monitora e contrasta, tra le altre attività criminose, l'antiterrorismo online, carte di credito e bancomat, cyberstalking, cyberbullismo. e-commerce, pedofilia online, social network, money muling, diritto d'autore, hacking. I dati sono allarmanti.

Capitolo a parte ma sicuramente quello più pericoloso e devastante sono i rischi che corrono le infrastrutture pubbliche e private, se la digitalizzazione non viene adeguatamente protetta.

Non possiamo far finta di nulla e di non sapere che con un semplice click è possibile produrre rischi concreti, si può destabilizzare un sito energetico, nucleare, il sistema dei trasporti pubblici, interrompere le trasmissioni di un satellite, compromettere la distribuzione elettrica e idrica nazionale o se si vuole, manipolare anche i dati di una consultazione elettorale

La sicurezza dei dati da sempre si misura nel tramite di tre direzioni, la *riservatezza* (ovvero la proprietà per la quale solo le persone autorizzate possono accedere ai dati), la *disponibilità* (la proprietà per la quale il dato è utilizzabile quando necessario) e l'*integrità* (la proprietà per la quale solo le persone autorizzate possono modificare i dati).

Si ha un problema di privacy quando un attore malevolo vuole attaccare dei dati, inficiando quindi, in qualsiasi modo, uno dei tre parametri che ne definiscono la sicurezza, custoditi e gestiti da una parte ma proprietà di un'altra parte. Se viene dunque attaccato un sistema che tratta dati di terzi, la privacy di questi dati viene di sicuro messa in pericolo.

È essenziale un'alfabetizzazione estesa dell'uso del web. Stiamo vivendo un periodo pericolosissimo a livello di tenuta collettiva, sociale e sottovalutare questo mutamento epocale può essere devastante: credere che bastino solo slogan o dire di voler fare una cosa e data per fatta quanto questo non è, credere inoltre di essere al centro dell'universo attraverso la rete, considerare questa come la fonte principale delle nostre competenze è illusorio, non corrisponde al vero e, soprattutto, non attenua la solitudine che pregna la stanza dalla quale si digita.

È passato un anno dallo scoppio dell'emergenza sanitaria e visto l'incrementarsi dell'uso digitale è necessario rafforzare con sapienza e competenza lo stesso, onde evitare che si resti fermi o. peggio, si torni indietro. Inoltre abbiamo i fondi dedicati al tema nel Next Generation EU, quindi è,

un’opportunità unica per far progettare, nel Recovery plan, a professionisti ed esperti del settore, soluzioni da finanziare e non semplicemente fare un elenco di buoni propositi senza chiare e certe finalità di sviluppo ad ampio raggio e per lungo tempo.

È questa, a mio avviso, l’ultima reale occasione di passare dalle parole ai fatti concreti.

La soluzione, ancora una volta, non può che essere di tipo culturale e provenire da reali investimenti mirati allo sviluppo delle competenze.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/02/02/sicurezza-digitale-una-nessuna-e-centomila/

© 2026 Istituzioni24