Digeat N.3 - 19 Settembre 2024

Il doppio volto della fiducia

Di Isabella Corradini

Abstract

La fiducia nelle innovazioni digitali costituisce un tema sempre più di largo interesse, dal momento che la costruzione della fiducia dell'individuo passa attraverso l'accettazione e il corretto uso delle tecnologie digitali, elemento chiave per favorire la cittadinanza digitale consapevole. Ma la fiducia è anche strumento utilizzato dai cybercriminali per i loro scopi. In questo articolo si vuole evidenziare una duplice chiave di lettura della fiducia in ambito digitale e gli aspetti che la caratterizzano.

Indice

- Fiducia, tra cybercrime ed esigenze di privacy
- Le aspettative degli utenti
- Coinvolgimento e consapevolezza digitale
- Bibliografia e sitografia

In quest'epoca caratterizzata da rapidi e intensi cambiamenti, la fiducia nella relazione tra esseri umani e tecnologie digitali costituisce un tema centrale, che può essere considerato in una duplice prospettiva: da un lato, come elemento che favorisce l'accettazione e l'uso dei dispositivi digitali da parte dell'utente, con la finalità di **promuovere una cittadinanza digitale consapevole**; dall'altro, come **strumento usato dai cybercriminali** per acquisire un vantaggio economico, il che pone il delicato problema della sicurezza dei dati.
Ad ogni nuovo progresso tecnologico, ecco che si ripropone la questione della fiducia. Il caso più recente riguarda l'Intelligenza Artificiale (IA), argomento immancabile in questo periodo in ogni conversazione social o mezzo di informazione, che finisce con il creare veri e propri "partiti" di sostenitori e contrari.

> In quello dei sostenitori, c'è chi – partendo dalla convinzione che non si può fermare il progresso – esprime una grande fiducia nelle potenzialità di questa tecnologia, rassicurando l'utente sul fatto che anche nel passato ci sono stati rilevanti progressi tecnologici, ma in fin dei conti gli esseri umani sono sopravvissuti a tutti i cambiamenti e ne hanno comunque beneficiato. Nel partito dei pessimisti, invece, c'è chi anticipa un futuro catastrofico, dove gli esseri umani saranno dominati dalle macchine, le quali finiranno con il sostituirli sul lavoro.

Evitando di lanciarci in previsioni sul futuro, spesso scarsamente attendibili, conviene sempre aspettare che la ricerca faccia il suo lavoro, **superando la visione riduttiva dell'IA come buona o cattiva**, considerato che gli attori e gli elementi in gioco sono molteplici.

Fiducia, tra cybercrime ed esigenze di privacy

Si potrebbe parlare di fiducia contesa, vista l'importanza che essa riveste non solo per gli utenti, ma anche per i cybercriminali: in molti casi, infatti, è proprio la conquista della "fiducia" dell'utente a decretare il successo di alcune minacce informatiche. Esempio a tutti noto è quello dell'ingegneria sociale (*social engineering*), tecnica alla base dei messaggi di *phishing*, che agisce sulla sfera psicologica dell'utente, cercando di conquistare la sua fiducia manipolandone la percezione, al fine di indurlo a condividere informazioni riservate o a fare azioni imprudenti, come aprire un file allegato o un messaggio WhatsApp.
Di questi tipi di minacce se ne parla da anni. Tuttavia, nonostante le misure messe in campo, **non è un mistero che esse continuino a mietere successi, perché fanno leva su comportamenti ed emozioni che sono connaturati all'essere umano, ma che nell'ambito della sicurezza informatica si declinano in vulnerabilità**, come quando ad esempio, per pura curiosità o per paura di incorrere in problemi legali, si aprono link o allegati di dubbia provenienza.

> I cybercriminali sanno come sfruttare queste caratteristiche, e sono fiduciosi del fatto che gli esseri umani commettono comunque degli errori o compiono azioni imprudenti, soprattutto quando sono scarsamente consapevoli dei rischi. Ed è noto come il fattore umano rappresenti ancora il maggiore elemento di vulnerabilità della sicurezza informatica, purtroppo scarsamente considerato (molto a parole, poco nei fatti).

La questione si complica con l'intelligenza artificiale, in particolare quella generativa, capace di sviluppare massive campagne di *phishing* e testi sempre più perfezionati. Senza contare che i *deepfake*, creati ad arte con l'Intelligenza artificiale, rendono la realtà sempre meno distinguibile dalla finzione. Questo uso distorto (e indiscriminato) dell'IA può minare la fiducia degli utenti nelle potenzialità di questa tecnologia, anche per effetto dell'incapacità di controllarne gli impatti nel quotidiano.
Secondo un sondaggio condotto dal Pew Research Center su una popolazione di oltre undicimila soggetti per investigare l'influenza dell'intelligenza artificiale nella loro vita, **emerge un sentimento di diffidenza generale verso questa tecnologia**, in particolare per quanto riguarda l'impatto sulla privacy (Tyson e Kikuchi, 2023).
Si tratta indubbiamente di preoccupazioni umane che non possono essere trascurate, perché a ben vedere l'accettazione delle tecnologie digitali e il loro corretto uso passano dal rapporto di fiducia che viene ad instaurarsi con le persone, alla quale contribuiscono la trasparenza informativa e la facilità del loro uso (Corradini, 2023).
Va comunque osservato come, per quanto la regolamentazione dell'IA sia un passaggio fondamentale per promuovere la fiducia dei cittadini nei sistemi di IA, **la soluzione non può essere quella di imbrigliare tutte le tecnologie e le loro applicazioni in normative e regolamenti**. Le preoccupazioni, infatti, richiedono innanzitutto risposte di tipo educativo, in grado di favorire la consapevolezza necessaria a comprendere rischi e vantaggi delle tecnologie.

Le aspettative degli utenti

Lo sviluppo della fiducia richiede sempre più di **non trascurare le effettive esigenze degli utenti** e le loro preoccupazioni, superando quell'ossessione di voler a tutti i costi decantare le meraviglie delle tecnologie digitali e il tutto per un bene superiore, quello dell'umanità.

> Il paradosso di questo presupposto miglioramento della vita dell'essere umano è che si delegano ormai alle macchine le attività più banali, con il rischio di produrre un graduale impigrimento mentale (questo è uno dei timori emersi relativamente all'uso del chatbot ChatGPT in ambito scolastico).

Fermo restando che sulla motivazione del miglioramento ci sarebbe ampiamente da dibattere – sul punto vale la pena richiamare le acute osservazioni del sociologo Evgenij Morozov nei suoi vari testi pubblicati – la riflessione che qui vorrei fare è che questa visione ha portato gli esseri umani, nel corso

degli anni, a svolgere sempre più un ruolo di secondo piano, al punto da essere concepiti come semplici (ma necessari) consumatori e fruitori di servizi, ma non purtroppo consapevoli dei processi sottostanti.

Eppure, guardando alla **definizione del costrutto di fiducia**, ne dovrebbe conseguire un ruolo attivo dell'essere umano. Secondo il vocabolario online della Treccani, la fiducia viene infatti definita come un "atteggiamento, verso altri o verso sé stessi, che risulta da una valutazione positiva di fatti, circostanze, relazioni, per cui si confida nelle altrui o proprie possibilità, e che generalmente produce un sentimento di sicurezza e tranquillità".
Per costruire fiducia nelle tecnologie digitali, vale a dire un atteggiamento positivo, è quindi necessario **far incontrare l'innovazione con i valori dell'individuo**.

Nell'ambito del World Economic Forum (WEF) del 2024, in un panel dedicato alle tecnologie, è emerso come **la crisi di fiducia nelle tecnologie non sia da attribuire al fatto che gli individui non capiscono come usarle, ma alla scarsa convinzione che queste tecnologie stiano lavorando a loro favore o che stiano supportando le loro aspettative e i loro valori** (Dobrygowski, 2024). Lo stesso WEF ha lanciato un'iniziativa di ricerca ad hoc e sviluppato il "Digital Trust Framework", con l'obiettivo di rimettere al centro dimensioni importanti per lo sviluppo della fiducia, come sicurezza, protezione, affidabilità, uso etico, inclusivo e responsabile delle tecnologie.

Coinvolgimento e consapevolezza digitale

Il processo di costruzione di fiducia non è semplice. Le persone hanno bisogno di **comprendere gli impatti che le innovazioni (come, ad esempio, l'IA) hanno sulle loro vite**, dando loro la sensazione di poterle controllare. Ascoltare i loro timori ed essere in grado di dare risposte esaustive fa parte di tale processo, così come la convinzione che le principali istituzioni sappiano gestire le innovazioni in modo adeguato: secondo il sondaggio condotto da Edelman in 28 paesi con 28.000 intervistati (Edelman Trust Barometer 2024), emerge invece una scarsa fiducia in questa capacità, mentre vengono ritenute necessarie le valutazioni degli scienziati e di esperti di etica.

> La fiducia è un elemento chiave per favorire la cittadinanza digitale consapevole, vale a dire la comprensione delle opportunità e dei rischi (anche di tipo etico e sociale) connessi alle innovazioni e che permettono al cittadino di poter interagire in una società che sarà sempre più digitale. Ma è importante che il cittadino abbia un ruolo attivo e non sia un semplice spettatore o, peggio, un mero consumatore passivo.

Allo scopo, non bastano efficaci strategie di comunicazione (anche se rilevanti), ma **serve un cambio di approccio e di mentalità** capace di rimettere davvero al centro le persone e i loro bisogni, non solo a parole, ma nei fatti. Questo significa ridare dignità all'essere umano, superando il paradosso secondo cui si procede da un lato ad una graduale spersonalizzazione degli individui tramutati in identità digitali, dall'altro all'umanizzazione di assistenti virtuali e chatbot, i quali, ad esempio, vengono addestrati in modo che le persone abbiano la sensazione di parlare con altri esseri umani (Corradini, 2024).

E visto che con l'intelligenza artificiale uno degli aspetti più discussi è quello dell'etica, **un buon punto di partenza potrebbe essere proprio quello di superare la visione riduttiva dell'utente-consumatore e di promuovere quella dell'essere umano pensatore**, anche critico, in grado di valutare e scegliere il suo futuro digitale.

Bibliografia e sitografia

Dobrygowski D., *Were the Luddites right? Why building digital trust is key to technological innovation*, consultabile qui.

Corradini I., *Intelligenza Artificiale: aspetti psicologici, sociali e di consapevolezza*, in Rivista Elettronica di Diritto, Economia e Management, numero 2023/4, consultabile qui.

Corradini I., *Crimini relazionali nell'era digitale. Aspetti psicologici e sociali per un uso consapevole delle tecnologie*, Edizioni Themis, 2024.

Edelman, *2024 Edelman Trust Barometer*, consultabile qui.

Tyson A. and Kikuchi E., (2023), Growing public concern about the role of artificial intelligence in daily life, consultabile qui.

Treccani, *Fiducia*, consultabile qui.

WEF, *Digital Trust Framework*, consultabile qui.