AI, un rischio rimosso

written by Luca Ricolfi | 4 Maggio 2026

Quanti posti distruggerà? Quante nuove professioni nasceranno? Quante professionalità dovranno ristrutturarsi? Quanto drastiche saranno le riorganizzazioni aziendali?

Queste, grosso modo, sono le macro-domande che ci facciamo quando proviamo a immaginare come sarà il mondo allorché l'intelligenza artificiale lo avrà completamente riplasmato.

C'è però una conseguenza dell'AI, e più in generale della iper-connessione, di cui si parla pochissimo: la potenziale distruzione della fiducia. Della fiducia si parla pochissimo perché – per un sistema sociale – è un po' come l'aria per un individuo: non te ne accorgi perché è una condizione minima di sussistenza. Nessun individuo può sopravvivere se smette di respirare, nessun sistema sociale può sopravvivere se viene meno la fiducia fra i suoi membri.

Naturalmente per fiducia non intendo la benevolenza, l'empatia, la solidarietà, bensì una condizione più asettica e fredda, ampiamente studiata dai sociologi e dagli economisti: la convinzione che gli accordi saranno rispettati e le transazioni non saranno inquinate da inganni, sotterfugi, informazioni false, frodi, truffe.

Ebbene, questo presupposto minimo della vita sociale sta progressivamente venendo meno perché le possibilità di inserirsi subdolamente nel flusso comunicativo in cui ormai quasi tutti viviamo sono enormemente cresciute, e si stanno ulteriormente espandendo e affinando. Le cronache ne riferiscono raramente, ma ogni giorno migliaia di persone vengono manipolate (per indurle a fare un versamento o cambiare un contratto) o subiscono assalti alla propria identità, alla propria privacy, ai propri dati, al proprio conto corrente. Grazie all'intelligenza artificiale e

all’iper-connessione, oggi è facilissimo simulare di essere una banca, un’assicurazione, un assessorato, un’azienda erogatrice di servizi, un’autorità di regolazione, un ufficio di polizia, persino – con l’imitazione della voce – una determinata persona che si conosce personalmente e di cui ci si fida. E questo avviene per una ragione ben precisa: negli ultimi anni – grazie a internet, all’informatica e all’AI – si è enormemente abbassato il costo di produzione di segnali al tempo stesso credibili e falsi, ma è rimasta sostanzialmente intatta la fiducia del pubblico verso interlocutori sconosciuti. Fingersi un funzionario di banca attraverso una videata ben costruita, o facendo apparire sul nostro telefonino il numero telefonico della banca custodito in rubrica, è enormemente più facile di 10 anni fa. A dispetto di ciò la maggior parte di noi si comporta sostanzialmente come 10 anni fa, ossia continua a concedere fiducia ai propri interlocutori, come se il rischio di essere ingannati fosse trascurabile.

Ma quel rischio, contrariamente a quanto ci piacerebbe credere, è in vertiginosa ascesa (più della chirurgia estetica, che è una delle industrie leader del nostro tempo). Un buon indicatore del rischio di essere ingannati è l’aumento delle truffe on line e delle frodi informatiche, che secondo una recente indagine FABI (Federazione Autonoma Bancari Italiani) stanno crescendo a un ritmo annuo dell’ordine del 30%, e sottraggono centinaia di milioni di euro ai cittadini (un trend favorito dal crollo delle transazioni in contanti). Quanto ai dati più generali della delittuosità, colpisce il fatto che la voce “truffe e delitti informatici” stia al secondo posto (dopo i furti) come numero assoluto di delitti segnalati (oltre 300 mila nel 2024), e in fatto di velocità di crescita contenda il primato alle violenze sessuali (la classe di delitti maggiormente cresciuta fra il 2019 e il 2024). Né le cose vanno meglio nel confronto internazionale dove – in materia di truffe e frodi – siamo al 9° posto su 41 società avanzate (paesi Oecd o UE), ed “eccelliamo”

precisamente in questo tipo di delitti.

La fase in cui siamo è ancora quella dell'euforia, in cui prevale l'entusiasmo per il progresso tecnologico e i suoi indubbi vantaggi. Ma rischia di essere solo una fase. Nell'istante in cui il sistema informatico di una grande banca venisse violato, e migliaia di correntisti perdessero i loro risparmi, quella fase finirebbe e si passerebbe istantaneamente da un regime di (prevalente) fiducia a un regime di sfiducia generalizzata, con conseguente caos (se non paralisi) delle transazioni on line.

Fantascienza?

Tanto poco fantascienza che quell'istante ha già ricevuto un nome: si chiama Q-day, ossia giorno in cui un computer quantistico riuscirà a violare i codici di sicurezza di qualche grande istituzione. Nessuno sa quanto vicino sia quel giorno (qualcuno ritiene che possa essere già nel 2029), ma sappiamo che da tempo gli esperti di crittografia stanno lavorando ad algoritmi capaci di scongiurare quella catastrofe, proteggendo le basi di dati dall'imminente assalto dei quasi-onnipotenti computer quantistici.

Nel frattempo si naviga a vista. Il grosso del pubblico si muove sulla rete come in un immenso luna park, con scarsa consapevolezza dei pericoli. Una frazione più istruita, più esperta, più informata o semplicemente più diffidente, già ora adotta precauzioni e sistemi di auto-protezione come le VPN (Virtual Private Network). Con la conseguenza di aggiungere una nuova fonte di diseguaglianza alla già lunga lista dei fattori che creano marginalità, esclusione, vulnerabilità.

Un bel paradosso per chi credeva e crede che internet sia una sorta di paradiso egualitario.

[articolo uscito sul Messaggero il 3 maggio 2026]