Giornata della sicurezza in rete. Difendersi dalla privatizzazione del web e dalla IA non controllata

di Rodolfo Marchisio

Tra le varie “giornate” ricorrenti e celebranti c’è quella fondamentale **della sicurezza in rete**, **6 febbraio**. Però quest’anno va integrata, perché non è solo più la giornata della sicurezza necessaria in merito a **dipendenza** (in un paese in cui 1/3 dei bambini tra i 5 e gli 8 anni ha un profilo social ed uno smartphone con seri danni e nella indifferenza dei “grandi” e 2 adolescenti su 3 usano IA e chat Gpt senza saper come funzionano) e **privacy**, **controllo dati**, **odio e violenza nel web**, **violazione di diritti**. Temi fondamentali con radici simili.
Ci sono importanti novità; da come difendersi dalla **Scuola 4.0** a come difendersi **dalla moda e dalla operazione di marketing della IA generale non controllata**. Cominciamo da questa, troppo di moda per essere vera. L’IA è un mondo di attività, proposte diverse che andrebbero conosciute ed analizzate separatamente. Con alcune attenzioni comuni. Questa rubrica sta dando conto di questo e fornendo dati, riflessioni, stimoli.

IA ACT. Cos'è.

Sta per essere messo a punto l'atto di regolamentazione sulla IA approvato dalla UE. Gli USA come al solito vanno per i fatti loro, pur avendo le maggiori imprese che si occupano con alterne vicende di IA, secondo le logiche del *libero mercato* e della *libertà di espressione*. Interesse individuale contro la responsabilità sociale richiesta ad es. dalla nostra Costituzione.
L'UE, dopo avere cercato con scarsi risultati di far pagare le tasse a costoro, ha provato e sta mettendo a punto, si spera per giugno, una serie di regole nello sviluppo della IA.

1- La strada delle regole

- **Usi proibiti perché pericolosi e lesivi.**
- ***Tecnologie subliminali per manipolare i comportamenti*** *di una persona; quelli che abusano di persone vulnerabili e fragili; la* ***categorizzazione biometrica che fa riferimento a dati personali sensibili,*** *come il credo religioso, l'orientamento politico o sessuale; la* ***pesca a strascico (scraping) da internet di volti,*** *come fece anni fa la contestata* ***startup*** *Clearview AI; il* ***riconoscimento delle emozioni sul posto di lavoro*** o a ***scuola****; i sistemi di punteggio o* ***social scoring****. Il testo* ***vieta anche la polizia predittiva****, ossia usare informazioni come tratti della personalità, nazionalità, situazione familiare o economica,* per stabilire la probabilità che una persona ***compia un reato****.*
  Tenendo conto che l'IA si nutre di tutto quanto c'è in rete, a partire dai nostri **pregiudizi.**
  Le donne, i meridionali, i migranti sono tutti…
- **Riconoscimento facciale.**
  Come noto sta funzionando male soprattutto per i non bianchi, maschi, caucasici. Crea problemi di identificazione (dai viaggi, alla identificazione di presunti colpevoli).

Riguarda **l'impiego di sistemi di riconoscimento facciale e biometrico in tempo reale**. Applicazione proibita, perché può portare "*a risultati marcati da pregiudizi e provocare effetti discriminatori*". Salvo in tre "*situazioni*", nelle quali il riconoscimento facciale "*è necessario per raggiungere un pubblico interesse, la cui importanza supera i rischi*". E i tre casi sono: la ricerca di vittime di reati e di persone scomparse; minacce certe alla vita o alla **sicurezza** fisica delle persone o di attacco terroristico; localizzazione e identificazione dei presunti autori di una lista di 16 reati**. Terrorismo, traffico di armi** e Wired

È comunque richiesta l'autorizzazione del magistrato. Come farà l'Italia in cui si stanno "abolendo" anche le intercettazioni? E che sta **affidando la regia del controllo sull'IA Act** non a Enti di controllo "super partes", ma ad un fedelissimo del Presidente del Consiglio?

- **Ad alto rischio** (c'è anche la scuola ed i suoi sistemi di valutazione).
  Sono considerati ad alto rischio sistemi di identificazione e categorizzazione biometrica *o per il riconoscimento delle* ***emozioni****; applicativi di sicurezza di infrastrutture critiche;* ***software educativi o di formazione,*** *per* ***valutare i risultati di studio, per assegnare corsi*** *o per* ***controllare gli studenti durante gli esami****. E poi vi sono gli* ***algoritmi usati sul lavoro****, per valutare curriculum o distribuire compiti e impieghi; quelli adoperati dalla* ***pubblica amministrazione*** *o da enti privati per distribuire sussidi, per classificare richieste di emergenza, per smascherare frodi finanziarie o per* ***stabilire il grado di rischio quando si sottoscrive un'assicurazione.*** Infine algoritmi usati dalle forze dell'ordine, dal potere giudiziario e dalle **autorità di frontiera per valutare rischi,** scoprire **flussi di immigrazione**

illegale o stabilire pericoli sanitari.

- **Di uso generale**
  Il testo regola anche i **sistemi di AI per uso generale**, in grado di svolgere compiti diversi (come creare un testo o un'immagine) e allenati attraverso **un'enorme mole di dati non categorizzati**, come GPT-4, alla base del potente **chatbot ChatGPT**, già sanzionato dal nostro garante della privacy, o LaMDA, dietro **Google Bard**. Gli sviluppatori devono assicurarsi che i **contenuti siano marcati in un sistema leggibile da una macchina** e siano riconoscibili come generati da un'AI. **Un utente deve sapere se sta interagendo con una chatbot.** E i contenuti **deepfake** devono essere etichettati come tali. Precauzioni che, tuttavia, **non** è detto siano **sufficienti a impedire la diffusione di fake news**, che la IA può, e di molto, potenziare e raffinare, **violando i diritti alla informazione, alla espressione, al voto libero e informato**. Ma anche il diritto alla **formazione dell'opinione pubblica**, non a caso sempre più orientata a credere a cose non provate. (Nichols).

Unica eccezione: **l'impiego di questi sistemi per perseguire reati**. Il regolamento fissa una soglia per identificare i sistemi ad alto impatto, che hanno **maggiori effetti sulla popolazione** e perciò devono rispettare obblighi più stringenti.

2. **La strada della conoscenza e della consapevolezza**

Come cerchiamo di dimostrare e documentare in questa rubrica, un'altra strada, quella che più interessa la cittadinanza e le scuole è quella di **conoscere di più per capire meglio**. In questo senso la introduzione piuttosto superficiale della IA nella formazione dei docenti e delle scuole (sinora superiori) con corsi, seminari e dimostrazioni, **resta deviante rispetto al fatto che "nuovo" non è sempre sinonimo di meglio,** di definito, di motivato, di provato e utile.
Che "tecnologico" non è automaticamente sinonimo di certo,

sicuro, efficace, risolutivo. Di **progresso.**
Le tecnologie non vanno solo conosciute prima ma **vanno compresi *i sistemi economici, sociali, politici che ne sono alle spalle*** (Soro) **e che le propongono:** perché, a quali condizioni, per quali interessi (in genere guadagnare soldi o scambi col potere politico che **non** le controlla); **le conseguenze sui diritti e sulla educazione che stanno dietro a queste iniezioni forzate di tecnologie,** fra "modernismo" e dominio **degli oligopoli economici** che ce le impongono.

Da dove arrivano, chi le controlla e chi non potrà mai controllarle, quali diritti sono in ballo e prima di tutto **quale è la reale influenza sulla formazione dei nostri ragazzi e sulla formazione di una cultura e cittadinanza digitale?**
Purtroppo i dati delle ricerche confermano che gli adolescenti sono già dentro la IA, ma in modo superficiale. *Se 2 adolescenti su 3 hanno già fatto uso di applicazioni basate sull'intelligenza artificiale "generativa" come ChatGpt, in genere per usare le Ai come assistenti personali per **generare testi**, non mancano le **criticità**;* se le nuove generazioni di "nativi" sembrano essersi evolute tecnicamente, i rischi esistono*. **Oltre 8 giovani su 10, infatti, accettano di buon grado che siti web e piattaforme possano influenzare il loro modo di conoscere il mondo** con il 44,7% tendenzialmente d'accordo e il 37,8% fortemente d'accordo. Per non parlare **dei fake, messi in circolazione grazie all'aiuto dell'AI,*** che solo avendo imparato si possono smascherare*. Un'opera di discernimento che, purtroppo, la stragrande maggioranza dei giovani utenti è impreparata a fare: **appena il 27% degli intervistati dice di conoscere il funzionamento del "deep learning" generativo** e di saperlo illustrare perlomeno a grandi linee*. Skuola.net

Ma la scuola è solo l'anticamera della industria? La scuola, in particolare dalla Buona Scuola ad oggi, ha delegato la sua ricerca di strade e modelli nuovi e più adatti, fondati pedagogicamente, alla tecnologia ed a quella parte che è in

mano ai privati. Di IA e programmazione open, controllabile anche dal basso si parla sempre meno.
La scuola che si intravede è tecnologica, privatizzata, controllata dall'esterno e dall'alto.
Come la sanità.

Se la scuola è la formazione di cittadini, di persone consapevoli, futuri lavoratori (anche nella IA spesso sfruttati e sottopagati, mentre i posti di lavoro come programmatore che la "Buona scuola" aveva ipotizzato si sono rivelati per quello che erano: una bufala) la **inerzia di fronte alle mode ed al dominio di 10 ricchi monopolisti tecno/economici** (molti dei quali come Zuck e Musk oggi già in crisi) è **molto preoccupante**. La mentalità, gli atteggiamenti, la consapevolezza che deriva dalla conoscenza e dalla riflessione sono quelli che interessano la scuola come ente formativo in cui le tecnologie entrano non perché di per sé valide (gli studi dimostrano il contrario) ma perché inserite in un progetto di conoscenza, riflessione, **consapevolezza del mondo da cui arrivano ed in cui tutti viviamo.** Compresi bambini con social e smartphone e adolescenti utenti passivi.

Una osservazione. Nelle proposte della "IA" le iniziative open, libere, gestite dal basso non sono mai citate. Mentre la scuola si abbassa a diventare l'anticamera della industria che la programma. Una industria che sfrutta, controlla, cui ci stiamo assuefacendo. Come nel PNRR Scuola 4.0. Ma di questo, se volete, parliamo altrove.