

## Gli italiani «Mhackeroni» vincitori del Hack-a-sat

Molto prima che la Casa di Carta sconvolgesse le nostre fragili menti sussurrandoci all'orecchio che non esiste baluardo inespugnabile, nemmeno (forse soprattutto) la Zecca di Stato spagnola, nel 1993 un diciottenne americano per gioco o per scherzo fondò il «Def Con», la conferenza che ogni anno riunisce a Las Vegas professionisti del mondo

Cyber Security, ricercatori, giornalisti, studenti appassionati di software, computer, hardware e fondamentalmente qualsiasi cosa, dato, informazione, piattaforma o sistema che possa essere... hackerato. Durante l'edizione appena conclusa, è stata lanciata una competizione, l'Hack-A-Sat, dietro bando diretto del Governo degli Stati Uniti,



con l'obiettivo di verificare la resistenza dei sistemi informatici di un satellite in orbita; protagonisti della gara ovvia-

mente i più titolati a scoprire vulnerabilità di galassie in apparenza non decodificabili e non attaccabili. A vincere

il capture-the-flag una squadra italiana di hacker etici, i Mhackeroni, formata da ricercatori e studenti delle università di Milano, Torino, Roma, Padova, Venezia, Genova, Parma, Pisa e Perugia, da professionisti di istituzioni quali Tu Wien, Eth Zurich, Eurecom e da aziende come Facebook, Google, Apple e CrowdStrike. La sfida finale della competizione prevedeva di prendere il controllo del Moonlighter, un vero satellite orbitante, decodificando sistemi criptati dalle stesse autorità gover-

native; in questo modo, gli esperti di sicurezza valutano l'effettiva tenuta e l'eventuale permeabilità dei protocolli, mettendosi in condizione di porre rimedio, evitare azioni ostili e testare le potenzialità offensive degli alleati. I Mhackeroni hanno conquistato il primo gradino del podio, vinto 50mila dollari messi a disposizione dalla Space Force e dalla Air Force statunitensi e ottenuto il plauso dei rispettivi rettori. Italiani, popolo di santi, poeti e navigatori (anche digitali).

I.P.

# APOSTOLATO DIGITALE

condividere codici di salvezza

ESPERIMENTO – ALL'AI LA RICHIESTA DI INDICAZIONI PER FAVORIRE LA PARTECIPAZIONE A MESSA

**L**a ChatGPT può rivelarsi uno strumento per ricevere spunti utili nell'ambito pastorale? Spinto da tale curiosità, in qualità di responsabile del Gruppo Liturgico della parrocchia di San Sebastiano, situata in un quartiere di Thiene (Vi) che conta circa 3.600 abitanti, di cui il 17,5% provenienti da Africa, Est Europa e mondo musulmano e che registra una partecipazione media annuale alle celebrazioni intorno al 9%, ho interpellato la ChatGPT con l'intento di raccogliere indicazioni per aumentare la partecipazione alla Santa Messa, sottoponendo il risultato al vaglio del Consiglio Pastorale. Naturalmente, all'interno dello stesso Consiglio non sono mancate proposte interessanti, ma si faticava a individuare un terreno comune di azione. Di contro, la risposta della ChatGPT è stata percepita come fornita da un «soggetto neutro» (che, in realtà, neutro non è!), e accolta come piattaforma di confronto che ha indotto a interrogarsi sul proprio approccio al problema. Prima di procedere, una precisazione in merito al prompt inserito, ovvero la frase attraverso cui dare istruzioni specifiche al fine di ottenere

## Se il Consiglio Pastorale si consulta con ChatGpt...



  
**La sensazione è di essere dinanzi ad una possibile nuova alleanza tra strumenti di intelligenza artificiale, discernimento umano e azione dello Spirito Santo**

una risposta pertinente. La domanda è stata introdotta da una descrizione della popolazione a cui avrebbe dovuto riferirsi. Inizialmente indicando di tener conto che è formata anche da persone atee, non cattoliche e di altre religioni. Successivamente, focalizzandosi solo sulla popolazione cattolica, con particolare riguardo agli anziani e ai giovani. Nei due casi ho ottenuto risposte attinenti e diversificate, sottoponendo al momento solo la seconda al Consiglio Pastorale. Le indicazioni fornite hanno offerto un «piano d'azione» motivando ogni punto con pratici suggerimenti, volti a compiere i primi passi (da approfondire con ulteriori domande nella stessa chat),

incentrati sulla comunicazione efficace, l'accoglienza, il coinvolgimento delle persone nella liturgia, le omelie, lo spazio dedicato alle testimonianze, la necessità di effettuare periodicamente monitoraggi e feedback per adattare anche le altre attività parrocchiali. Posto che, fino al periodo precedente la pandemia, la parrocchia ha già praticato numerosi suggerimenti tra quelli indicati, purtroppo non interamente ripristinati alla ripresa definitiva, l'impressione ricavata da un primo confronto è quella di spunti validi sui quali confrontarsi e agire, calandoli nella specifica realtà. Allo stesso tempo, consapevoli che l'addestramento

della ChatGPT si basa su un insieme di dati costituiti da testo, audio o immagini e raccolti da diverse fonti (libri, articoli, conversazioni, siti, ecc.) soprattutto in lingua inglese, abbiamo riflettuto sulla qualità della risposta fornita. Essa, infatti, sembra prendere origine da un approccio derivante più dal marketing che dalla pastorale liturgica. Concorde o meno con le provocazioni di Bruno Ballardini (celebri i suoi libri su cristianesimo e marketing), rimane la curiosità di conoscere quanti e quali fonti specifiche di pastorale liturgica, che non siano tra l'altro solo inglesi, sono state prese in considerazione ed eventualmente come implementarne la presenza nel web. Unanime, inoltre, la conclusione: sono proposte «intelligenti», che tuttavia hanno bisogno di essere vagliate e supportate dall'intelletto inteso come dono dello Spirito Santo. La sensazione è di essere dinanzi ad una possibile nuova alleanza tra strumenti di intelligenza artificiale, discernimento umano e azione dello Spirito Santo. La ChatGPT ci

ha fornito in pochi minuti, in forma schematica ed effettivamente applicabile, una serie di indicazioni che avrebbero richiesto una fatica maggiore per essere raccolte. Ora, però, sarà ancor più necessario attivare il discernimento comunitario, guidato e sostenuto dallo Spirito Santo, affinché quanto indicato diventi l'agape di una parrocchia, e non semplicemente una serie di modalità per scovare nuovi clienti.

Andrea NAVARIN



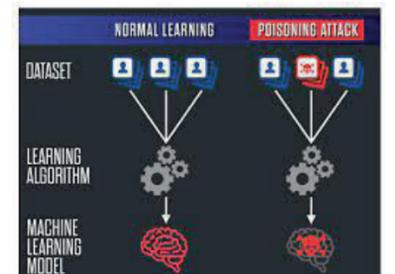
### Fake news

Come nascono? Dinamiche e difese con Paolo Attivissimo - TEDxToranoNuovo.

RISCHI – IL DATA POISONING

## Intelligenza Artificiale avvelenata?

L'intelligenza artificiale deve processare un'ingente quantità di dati per poter ottenere soluzioni accurate. Questa grossa mole di dati, però, può essere «inquinata» con la conseguenza che l'intelligenza apprende comportamenti che si rivelano essere dannosi. Il processo di avvelenamento dei dati viene definito «data poisoning» e la sua durata può variare a seconda del ciclo di addestramento della tecnologia. Ad oggi esistono due categorie principali di questi attacchi: la prima mira alla compromissione del modello di apprendimento, la seconda



intende contaminare l'integrità dei dati. Quest'ultima è più complessa e maggiormente dannosa, rispetto alla prima, e consiste nella creazione di una backdoor – ovvero righe di codice informatico grazie alle quali un utente può entrare come amministratore all'interno di siti web e computer, senza avere alcun accesso autorizzato – la quale consente agli aggressori di poter controllare la macchina senza intaccare la database. Così facendo, in apparenza, la tecnologia continuerà a funzionare «adeguatamente». Recentemente, un gruppo di ricercatori di Google, Nvidia e Robust Intelligence ha pubblicato uno studio che, indagando su questi attacchi, ne ha identificato due tipologie: il primo è lo split-view poisoning in cui l'aggressore agisce ottenendo il controllo di una risorsa web indicizzata da un particolare set di dati; nel secondo, definito front-running poisoning, l'aggressore non ha il pieno controllo dei dati ma ha la possibilità di inquinarli poco prima che vengano raccolti. Questo studio propone anche delle accortezze per contrastare gli avvelenamenti: distribuire hash crittografici per tutti i contenuti indicizzati, così da assicurare che i clienti ricevano gli stessi dati annotati dai manutentori, e randomizzare l'ordine in cui i dati vengono archiviati negli insiemi. Purtroppo però contrastare il data poisoning richiede molto tempo e denaro poiché, in caso di riuscita nel ripristino della situazione pre-avvelenamento, il computer dovrà essere completamente riaddestrato.

Anna SBARDELLATI