Per ogni tecnologia è imprescindibile una *governance* etica

Intervista con Corrado Giustozzi, informatico, consulente strategico, docente e divulgatore scientifico

Informatico, consulente strategico, docente e divulgatore sui temi della cybersecurity, Corrado Giustozzi, è docente nel corso di Laurea magistrale in Ingegneria dei sistemi intelligenti dell'Università Campus Bio-medico; nei Master universitari di 1° e 2° livello in Cybersecurity di LUISS, Campus Bio-medico, Link Campus; nel Master universitario di 2° livello in Homeland Security del Campus Bio-medico; nel Master in Protezione strategica del Sistema Paese della SIOI. È stato esperto supersenior di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT della PA e componente dell'Advisory Group dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA). Giornalista pubblicista, membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge un'intensa attività di divulgazione sui temi della cybersecurity. L'Università di Roma Tor Vergata gli ha conferito la laurea magistrale *honoris causa* in Ingegneria di Internet e delle Tecnologie per l'Informazione e la Comunicazione.

A lui abbiamo chiesto quali sono le principali sfide tecniche e operative che le aziende devono affrontare quando cercano di integrare tecnologie come l'intelligenza artificiale e/o la blockchain, riuscendo a garantire una corretta postura di sicurezza informatica? Come possono superare queste difficoltà?

Premetto che, a mio avviso, Intelligenza Artificiale e blockchain sono tecnologie con pochi punti di contatto in comune, per non dire che sono ortogonali tra loro. Possiamo infatti considerare la IA come una tecnologia "orizzontale", nel senso di "general purpose" o "universale", in quanto può essere applicata a molteplici ambiti di attività in settori eterogenei, ed è in grado di risolvere i problemi più disparati.
La blockchain è invece una tecnologia molto "verticale", che di fatto risolve un unico problema in un ambito molto specifico (ovvero: garantire l'integrità dei dati scritti da molteplici soggetti in un registro distribuito, laddove non vi sia un singolo soggetto affidabile cui affidarne la gestione centralizzata). È probabilmente possibile individuare casi d'uso in cui queste tecnologie possono convivere e magari anche cooperare, ma almeno per il momento mi sembrano più frutto di riflessioni accademiche che di reali esigenze pratiche. Tuttavia, a prescindere da tali considerazioni, è chiaro che oggigiorno, nel momento in cui tecnologie realmente nuove e dirompenti stanno entrando nell'uso quotidiano senza che se ne siano ancora comprese a pieno le grandi potenzialità e gli inevitabili limiti, il mantenimento di una adeguata postura di sicurezza è un aspetto assolutamente cruciale per ogni azienda o impresa, pubblica o privata.

> **"È assolutamente cruciale mantenere un'adeguata postura di sicurezza"**

Le sfide però non sono tecniche ma soprattutto organizzative, e direi addirittura culturali: si tratta infatti principalmente di *governare* nel senso più ampio tali tecnologie, ossia adottare processi che consentano di impiegarle in modo consapevole, trasparente, etico e responsabile; nonché di vigilare affinché vengano evitati abusi e utilizzi impropri, i quali potrebbero creare

indebiti impatti su terzi oltre che ritorcersi contro l'utilizzatore. La sicurezza sul piano tecnico è compito relativamente più semplice, ma deve collocarsi all'interno di questo quadro altrimenti rischia di essere inefficace.

In quali settori ritiene che l'adozione di nuove tecnologie, come ad esempio l'intelligenza artificiale, possa avere il maggiore impatto sulla cybersecurity? Può condividere alcuni esempi pratici di applicazioni innovative che ha osservato o sviluppato?

Del rapporto tra intelligenza artificiale e cybersecurity si parla in realtà da parecchi anni, senz'altro da molto prima che il recente boom portasse gli LLM e le IA generative all'attenzione del grande pubblico. In particolare, è un tema da sempre molto considerato in ambito militare, per le sue evidenti implicazioni sia operative che strategiche; ma in tempi più recenti sta catturando sempre più gli interessi anche commerciali del settore civile. Generalmente esso viene declinato sui due approcci possibili, diametralmente opposti tra loro: quello in cui l'IA può supportare le attività dei difensori, e quello in cui può invece supportare le attività degli attaccanti. È chiaro, infatti, che la tecnologia in sé è neutra, e tutto dipende dall'uso che se ne fa.

> "La tecnologia in sé è neutra: tutto dipende dall'uso che se ne fa„

Per quanto riguarda il primo caso, basta ricordare come già da diversi anni esistono sul mercato prodotti di sicurezza che impiegano tecniche di *machine learning* (le quali, giova ricordarlo, non sono IA di per sé ma piuttosto ne costituiscono un componente) per migliorare le capacità di rilevazione ed analisi di eventi anomali che potrebbero sottendere attività malevole o attacchi; mentre per quanto riguarda il secondo, ci sono purtroppo evidenze del fatto che diversi attori criminali stiano già facendosi aiutare dalle IA per confezionare messaggi di phishing più accurati e credibili, per scrivere *malware* migliore in modo più rapido ed efficace, o addirittura per imitare le voci di reali personaggi famosi e autorevoli al fine di confezionare truffe ed inganni assai verosimili nei confronti di imprenditori o altri soggetti facoltosi.

La vera innovazione sta forse proprio in questa ampia varietà di applicazioni della IA a fini offensivi, cui purtroppo non sembra ancora corrispondere altrettanta creatività e fantasia da parte di chi la usa a fini difensivi. Ma è una legge di natura che i predatori siano sempre un passo più avanti rispetto alle prede, altrimenti si estinguerebbero...

Guardando al futuro, come vede l'evoluzione delle stesse tecnologie nei prossimi cinque anni? Quali trend o sviluppi prevede che possano trasformare il panorama tecnologico e sociale?

L'Intelligenza Artificiale, pur essendo nota ed impiegata da decenni, è diventata la "tecnologia del momento" (per non dire "di moda") grazie alla felice concomitanza di due fattori: la messa a punto di nuovi paradigmi per l'elaborazione di modelli linguistici di grandi dimensioni, mediante i cosiddetti *transformer*; e la disponibilità delle enormi potenze di calcolo necessarie per elaborarli, per merito delle GPU di ultima generazione.
Progressi assai recenti hanno portato a migliorare ulteriormente la combinazione, definendo *transformer* assai più efficaci e sviluppando GPU ancora più potenti, col risultato che le prestazioni dei nuovi sistemi di IA stanno crescendo in modo più che lineare.

> "L'IA è diventata la tecnologia del momento„

Ciò porta diversi analisti a ritenere che nell'arco di pochi anni potremo avere una "reale" intelligenza a bordo di dispositivi relativamente semplici ed economici, con applicazioni potenzialmente dirompenti per la vita di tutti i giorni e conseguenti importanti impatti sulla sfera sociale.

Con l'aumento dell'uso dell'intelligenza artificiale, emergono preoccupazioni etiche significative. Qual è la sua opinione sull'importanza della governance etica nell'implementazione dell'AI?

Come dicevo prima, ritengo che una *governance* etica sia imprescindibile per ogni tecnologia. Nello specifico, il rischio che un sistema di IA fornisca involontariamente risultati affetti da *bias* o pregiudizi è assai elevato; ma

lo è altrettanto che fornisca risultati viziati da *allucinazioni*, ossia contenuti verosimili ma erronei, i quali sono artefatti tipici e purtroppo pressoché inevitabili nelle IA generative. Inoltre, al di là di tali eventualità ascrivibili ad ambiti di errore o casualità, vi potrebbero essere casi di usi *deliberatamente* distorti o impropri dell'IA, al fine di perseguire obiettivi spregiudicati se non esplicitamente illeciti o addirittura criminali. Per prevenire tutto ciò occorre dotarsi di un vero e proprio sistema di gestione che garantisca il rispetto dimostrabile degli irrinunciabili principi etici nell'utilizzo delle tecnologie. Occorre dunque dotarsi innanzitutto di una politica appropriata, e quindi sviluppare un adeguato insieme di processi a supporto della sua attuazione, che si fondino su una attenta analisi del rischio sviluppata in ottica costi-benefici. Ultimo fattore, ma non in ordine di importanza, è fornire a tutto il personale, da quello direttivo a quello operativo, un'adeguata formazione e sensibilizzazione sui temi della sicurezza e della responsabilità nell'uso delle nuove tecnologie.