Poliziamoderna

Un mondo nuovo

Anno 1947. Isaac Asimov nel racconto *Il robot scomparso* scriveva: “Un robot non può recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno”. Questa è una delle tre leggi della robotica che uno dei padri del genere fantascientifico coniò, ambientandola nel 2058… ad oggi, mancherebbero solo 35 anni. Che dire, il grande scrittore russo, così come tanti dopo di lui, tra i quali Philip Dick o gli ideatori di saghe di fantascienza come *StarTrek*, ci avevano visto lungo, perché quel che decenni prima avevano ipotizzato nei loro romanzi, oggi sta pian piano diventando realtà: dai computer parlanti ai telefoni cellulari, dai tablet (chi non ricorda la tavoletta su cui prendeva appunti il capitano Kirk? Era il 1968) a macchine che ragionano da sole e si autoriparano. Tutto questo, ovviamente, per supportare, alleviare e velocizzare le attività quotidiane dell’essere umano.

Oggi siamo tutti affascinati, chi più chi meno, da questo nuovo mondo che ci si sta aprendo davanti, grazie all’avvento dell’intelligenza artificiale. Su Internet si possono trovare centinaia di siti capaci di catapultarci in questo universo parallelo, per comporre un testo, generare immagini fornendo come base semplici input, modificare foto o video, parlare un’altra lingua e via via scorrendo. Elementi di IA sono stati inseriti anche in molti degli applicativi che quotidianamente utilizziamo su computer o sui telefoni cellulari, magari senza neanche accorgercene. Il tutto, come già detto, per aiutare, semplificare, velocizzare la nostra quotidianità; ma c’è anche chi ipotizza che, con il suo “naturale” evolversi, l’intelligenza artificiale potrà sostituire l’uomo in alcune attività, come generare attori virtuali in un film o addirittura scrivere sceneggiature originali (ricordate lo sciopero che questa estate ha paralizzato Hollywood con attori e autori sulle barricate?) o ancora scrivere articoli come quello che state leggendo… Confessiamo che la tentazione di farlo è stata tanta, anzi è stato fatto ma (fortunatamente per la professione) il risultato non è stato proprio dei migliori; quindi vogliamo rassicurarvi: queste righe sono state scritte da un essere umano in carne ed ossa.

Dunque, verrebbe da dire “tutto molto bello, ma…” Ebbene sì, c’è sempre un “ma” in questi casi, anzi, un rovescio della medaglia, quello che potremmo definire, prendendo spunto sempre dalla fantascienza, come un “lato oscuro”, un risvolto che alletta chi sfrutta la tecnologia per scopi illeciti; e quando si tratta di reati informatici entra in campo la polizia postale e delle comunicazioni. Di questo argomento ne abbiamo parlato con Ivano Gabrielli, il direttore del Servizio.

«Il tema è complesso e come polizia postale abbiamo iniziato ad approcciarlo da tempo – dice Gabrielli – In questo momento storico non ci sono tecnologie che ci permettano, perlomeno in prima battuta, di capire cosa sia e cosa non sia prodotto dall’intelligenza artificiale, ossia cosa è immediatamente identificabile come *fake*». Ed è proprio questo il problema principale nell’individuare se un filmato o una fotografia possa essere originale o creata da zero da un computer, soprattutto perché, passando di mano in mano, subiscono variazioni tali da far perdere completamente le tracce; pensiamo ad esempio a un video inoltrato più e più volte tramite app di *instant messaging* come Whatsapp che, durante i vari passaggi, perde risoluzione, viene modificato nelle dimensioni e nell’audio che pian piano perde di qualità: in pratica, lungo la sua strada, ha perso così tante “informazioni”, in sostanza dei bit, da non riuscirne più a rintracciarne la messa in Rete originaria. Un problema non di poco conto per chi deve indagare.

«Oggi sicuramente il mondo delle frodi e delle truffe è prevalente – prosegue il direttore – Pensiamo a quelle online attivate attraverso telefonate che simulano una voce, o a quelle che possano in qualche modo essere generate attraverso l’esposizione di un contenuto audio-video o foto che possano in qualche modo trarre in inganno, come nel caso delle *romantic scam*: un fenomeno ricorrente e, tra l’altro, di difficile denuncia perché la vittima, fintanto che è dentro la truffa, pensa di vivere una storia sentimentale particolarmente importante. Quando ne esce se ne vergogna a tal punto da non denunciare. Prima dell’avvento dell’IA una persona poteva essere rintracciata facendo una ricerca per volto o per foto, invece oggi si può costruire da zero un’immagine che simuli un volto del tutto nuovo e quindi, di fatto inesistente».

Un problema, dunque, quello dei *deep fake*, ossia così “profondamente falsi”…tanto da poter risultare

reali, che possono addirittura indirizzare l'opinione pubblica «attraverso la proposizione di finti video, di finte interviste, che comunque ancorché smentite poi hanno prodotto un effetto su una quota parte di persone che non si affidano al *mainstream*, o comunque giudicano sempre le informazioni *mainstream* come false – continua Gabrielli – una dinamica che può portare a generare anche fenomeni particolari, dall'innocuo terrapiattismo fino ad arrivare alle teorie cospirazioniste di gruppi come Qanon».

Quindi, un pericolo reale, ancora allo stato embrionale, ma che non per questo non ha fatto "alzare le antenne" agli specialisti delle indagini online, destinati a stare "sempre sul pezzo" a causa del continuo evolversi della tecnologia e dell'informatica: «Il bene giuridico tutelato, cioè la libertà sessuale (come nel caso di reati quali ad esempio *revenge porn* o le *sex extortions*) piuttosto che la dignità umana, viene comunque a essere leso e quindi il tema è anche questo: quello che fino a qualche tempo fa poteva essere considerato un reato impossibile, oggi va riconsiderato nell'ottica nell'utilizzo di un'intelligenza artificiale che è in grado di prendere un'immagine e rielaborarla in maniera realistica tanto da poterla considerare reale». Da questo punto di vista, il nostro Paese ha già fatto passi in avanti dal punto di vista legislativo, soprattutto nella tutela della dignità dei minori; infatti in Italia viene punita anche la detenzione di pedopornografia virtuale, ossia la realizzazione con software di immagini pedopornografiche.

All'inizio di questo articolo, abbiamo parlato dell'IA come di un supporto all'attività umana e quindi anche per l'attività di polizia, così come conferma Ivano Gabrielli: «Si pensi al supporto che potrebbe dare l'IA allo svolgimento di indagini complesse in cui è necessario analizzare una gran mole di dati. Stiamo lavorando a un progetto per l'analisi e il riconoscimento di materiale pedopornografico che, in fase di test, ha dato risultati congrui al 98%. L'utilizzo di una tecnologia del genere porterà un triplice vantaggio: il primo nella velocità di analisi del materiale, il secondo la mancanza di "stanchezza" in cui incorre l'essere umano, il terzo, non di poco conto, nell'evitare al nostro personale che indaga su questo tipo di reati rischi di *burnout* significativi piuttosto che di sofferenza psicologica, connessa per l'appunto alla visione ripetitiva di immagini di un certo tipo. Stiamo sperimentando alcuni sistemi nei processi di analisi di grandi quantità di dati: attualmente, ad esempio in caso di un attacco informatico, gli operatori, ancorché aiutati da software, devono osservare migliaia di righe di codice (o centinaia di righe di chat) per individuare il log dell'attività anomala; avere un sistema di intelligenza artificiale che fa questo lavoro per noi e che dia in tempi brevissimi anche l'idea di quello che è accaduto, è un grande aiuto per chi fa il nostro lavoro».

Nel dibattito sull'intelligenza artificiale, il problema principale resta quello etico e della tutela dei diritti come il diritto d'autore, i diritti civili e la privacy: «Deve essere urgentemente creato un substrato normativo, un *framework* internazionale sull'intelligenza artificiale: non possiamo permetterci di avere norme diverse in Stati diversi. L'Unione europea sta lavorando ad un "AI-act", ma anche in questo caso si dovrà fare in modo che le regole che valgono in Europa debbano valere per tutto il mondo in generale, altrimenti troveremo ancora una volta le stesse difficoltà che abbiamo avuto con l'esplosione dei social, con legislazioni diverse che non permettono di attivarsi in tempo e chiedere attività di cooperazione. E nel settore IA, dovrà essere tutto pronto in tempi congrui: non ci possiamo permettere di non avere la possibilità di aggredire un certo comportamento criminoso perché dall'altra parte del mondo non viene considerato tale».

La sfida del Craim

di **Carlo Bui*** e **Tommaso Fornaciari****

Parlare di applicazioni dell'IA in ambito investigativo, significa riferirsi alle tecniche di analisi automatiche di immagini, di video, di audio e di documenti relative ad attività di indagine. Una delle attività svolte dal Craim (Centro ricerca e analisi informazioni multimediali), è quella di estrarre i volti presenti in video pubblicati online o raccolti da telecamere di sorveglianza, e confrontarli con quelli di individui "attenzionati" dagli uffici operativi. Non si tratta di identificazione biometrica, ma di stime di similarità che simulano la percezione di somiglianza che avrebbe l'operatore. Le reti neurali convoluzionali svolgono bene questo compito e non richiedono, per usi personali o limitati, particolari infrastrutture hardware, basti pensare alle capacità di riconoscimento e confronto facciale degli smartphone di fascia medio-alta, cui ormai siamo tutti abituati. Il problema si complica quando l'estrazione o le comparazioni riguardano migliaia di soggetti, oppure filmati che possono contenere settimane o mesi di registrazione e si vuole un risultato in tempi rapidi o in tempo reale.

In questo caso, oltre al potenziamento dell'infrastruttura in termini di unità di calcolo tradizionale, di memoria è necessario aumentare in modo esponenziale il numero di elaborazioni che il "calcolatore" può eseguire al secondo, cioè i cosiddetti *flops*. In effetti, l'elaborazione di algoritmi di *machine learning* e *deep learning* è oggi possibile, in tempi compatibili con le necessità degli uffici, solo ricorrendo a sistemi di *high performance computing*, di cui il Craim si è dotato acquisendo server dedicati che ospitano schede di accelerazione professionali, cioè le cosiddette GPU, solitamente acceleratori grafici, che vengono utilizzate per effettuare calcoli ad una velocità molto superiore a quella delle più potenti CPU tradizionali.

Al Craim sono presenti 4 server dotati di GPU in quantità variabili da 2 a 8 e di tipologie differenti (A100-80GB, K80-24GB), il cui utilizzo è dedicato all'analisi di contenuti multimediali e a all'analisi e interpretazione dei testi. Queste GPU producono un complessivo di 3.700 Tflops, cioè quasi 4 Petaflop (solo a termine di esemplificazione la CPU tradizionale della Intel più potente raggiunge 2,1Tflops). Una potenza di elaborazione come quella realizzata presso il Craim ha di contro due problemi, il primo relativo a temperatura e assorbimento elettrico e il secondo relativo ai costi. Un server con GPU assorbe il triplo di energia rispetto ad un server tradizionale e riscalda circa il doppio; una CPU (la più potente di Intel) ha un costo di circa un terzo della GPU di quelle acquisite dal Craim.

L'applicazione dell'IA al riconoscimento dei volti e degli oggetti, è solo una delle soluzioni offerte dal Craim agli investigatori e sebbene di straordinario impatto sulle attività di indagine, non si può considerare una novità in ambito IA, dove si sta assistendo a una rivoluzione nelle tecnologie del linguaggio, proprio nel campo dell'analisi e interpretazione dei testi. I cosiddetti *Large language models* (Llms), che oggi rappresentano lo stato dell'arte per l'analisi e la produzione automatica di testi, richiedono proprio le risorse hardware di cui abbiamo parlato, grazie alle quali al Craim è possibile analizzare testi di carattere investigativo, estraendo entità e relazioni di specifico interesse per le attività di polizia, grazie all'impiego di modelli customizzati, appositamente addestrati allo scopo. Lo stesso si può dire per la classificazione di documenti per categorie di interesse specifico.

Tutto questo rappresenta il presente. La nuova frontiera dell'IA, su cui si sta concentrando l'attenzione degli esperti del Craim, è, però, l'uso di Llms basati su *Generative pre-trained transformer* (Gpt), che sono i mattoni dei Llms che generano le risposte contestualmente coerenti tra i dati di input e la conoscenza precedentemente immagazzinata in fase di addestramento (*training*). Grazie ai Gpt, è possibile creare sistemi di IA ottimizzati per compiti di domanda e risposta. È il caso di ChatGpt, commercializzata come servizio da OpenAI. I livelli di prestazione raggiunti sono impressionanti: è possibile dialogare con ChatGpt in linguaggio naturale (ovvero, colloquiale), ricevendo risposte plausibili su un insieme di temi vasto tanto quello contenuto nel Web, in più lingue diverse (con traduzioni anche migliori di molti sistemi dedicati tradizionali). Il costo dell'infrastruttura tecnologica richiesta per realizzare un tale sistema è alla portata delle sole grandi aziende tecnologiche di livello mondiale, come Microsoft (che è il principale finanziatore di OpenAI), Google, Facebook, Amazon e pochi altri.

D'altra parte, l'uso di tali sistemi non è possibile e, nemmeno, ipotizzabile per applicazioni di interesse investigativo e, più in generale, per l'analisi di testi riservati, poiché è necessaria la condivisione dei dati con i provider dei servizi che devono averne visibilità per generare risposte pertinenti. Diverso potrebbe essere il caso dei dati raccolti da fonti nitidamente aperte: al Craim sono in corso attività sperimentali che prevedono la condivisione con ChatGpt di contenuti di pubblico dominio.

L'unica soluzione perseguibile per sfruttare a pieno le enormi potenzialità di Gpt per fini di polizia è quello di ipotizzare di internalizzare quanto più possibile queste tecnologie adeguando, anche progressivamente, le capacità di calcolo e gli algoritmi dedicati: questa è la sfida raccolta dal Craim.

**direttore del Craim **direttore tecnico superiore*

04/12/2023