‘Salute, Algoritmi e Intelligenza Artificiale’. Il 22 ottobre ore 15,00 il Fubinar

L’utilizzo di tecnologie digitali nel campo della salute è in rapida espansione e riguarda un ampio spettro di attività, dall’organizzazione dei servizi sanitari fino al sostegno al personale medico a livello diagnostico e operativo.

Leggi anche: ‘Teoria dei giochi e matching dei donatori nel trapianto di reni’. Intervista a Roberto Lucchetti

In questo quadro la **Fondazione Ugo Bordoni** presenta il quarto Fubinar del 2020, in programma il prossimo 22 ottobre alle 15:00 dal titolo “*Salute, algoritmi e Intelligenza Artificiale. Tecnologie digitali al servizio di medici e pazienti*”.

Le nuove soluzioni basate su tecniche di Intelligenza Artificiale (AI), su algoritmi di ottimizzazione combinatoria, su reti di comunicazione 5G e sull’IoT, promettono di aumentare produttività, efficienza ed efficacia delle soluzioni per la salute, migliorando l’assistenza e l’esperienza dei pazienti.

Il Fubinar focalizzerà alcune delle tecnologie più innovative sviluppate in ambito sanitario, mettendo a confronto su questo tema di alto rilievo scientifico amministratori ed esperti tecnici e medici.

PROGRAMMA

Introduce

- **Antonio Sassano**, *Presidente, Fondazione Ugo Bordoni*

Keynote

- **Roberto Lucchetti**, *Ordinario di analisi matematica, Politecnico di Milano*

Interventi

- **Giovanni Arcuri**, *Direttore UOC Tecnologie Sanitarie, Fondazione Policlinico Universitario Agostino Gemelli*
- **Pasquale Avella**, *Ordinario di Ricerca Operativa, Università del Sannio*
- **Amedeo Cesta**, *Dirigente di Ricerca CNR, Vicepresidente di AIxIA*
- **Arturo Chiti**, *Ordinario di Diagnostica per Immagini, Università Humanitas*
- **Tommaso Di Noia**, *Ordinario di IA, Machine Learning e Big Data Analytics, Policlinico di Bari e Comitato Scientifico FUB*
- **Marco Marsella**, *Head of Unit "eHealth, well-being, ageing", DG Connect – Commissione Europea*

Modera **Daniela D'Aloisi**, *Ricercatrice, Fondazione Ugo Bordoni*

PARTECIPA

Per saperne di più: AIFUB
'Salute, Algoritmi e Intelligenza Artificiale'. Il 22 ottobre ore 15,00 il Fubinar

USA-Cina. Una guerra Hi-Tech che danneggia tutti e da cui l'Europa deve sfilarsi

Alcuni giorni fa la Cina ha presentato la sua "**Global Initiative on Data Security**" (**GIDS**), un programma attraverso il quale il governo cinese intende proporre un cambio di passo sui temi di interesse internazionale legati alla sicurezza, alla tutela dei dati, al rispetto delle sovranità nazionali.

L'iniziativa, presentata dal ministro degli esteri cinese **Wang Yi**, ha avuto grande eco sulla stampa internazionale, ma è stata del tutto trascurata dai media italiani. Eppure, la proposta cinese si colloca in un contesto di relazioni internazionali tra USA e Cina, tra le due più importanti potenze economiche del pianeta, giunte ai ferri corti e ad un passo da vistose e più gravi rotture.

Come è noto il presidente **Donald Trump** ha lanciato, giusto poche settimane prima dell'iniziativa cinese **GIDS**, il piano "**Clean Network**": un piano nel quale rientrano il blocco alle esportazioni USA verso **Huawei Technologies**, l'ordine a Paesi terzi di non vendere *micro-chips* con tecnologie americane a Huawei ed in cui rientrano anche i percorsi per mettere al bando **TikTok** e **Tencent** negli USA. Il piano Clean Network, a quanto dichiarato dal Dipartimento di Stato, avrebbe raccolto l'adesione di 30 Paesi e di numerose aziende, ma l'amministrazione americana non ha mai specificato alcunché sulle adesioni al Piano. Le ragioni addotte dagli americani sono legate alla sicurezza nazionale e alla raccolta indebita di dati di cittadini americani, accuse che le due società cinesi hanno contestato e rispedito al mittente.

Il contesto dello scontro USA-Cina è, come è noto, ben più ampio, anche se focalizzato sulle tecnologie ICT con particolari punte di intensità sui settori tecnologici del **5G** e dell'**Intelligenza Artificiale** (IA). Si tratta di due aree attigue su cui si giocherà il futuro delle economie mondiali, dal momento che **5G** e **IA** saranno alla base degli sviluppi produttivi dell'**Industria 4.0**, da cui discenderà ogni ricchezza per i prossimi decenni.

Prima di fare ulteriori considerazioni sugli elementi di contesto, vediamo più in dettaglio i termini della proposta cinese, del "**Global Initiative on Data Security**" (**GIDS**), perché gli aspetti che sollecita hanno rilevanza per tutti noi e corrispondono alle esigenze di un comune sentire degli Stati nazionali, dei gruppi di interesse e dei cittadini a livello globale.

La proposta del governo cinese fa riferimento a quattro aree che inevitabilmente si intersecano tra loro: il progresso tecnologico, lo sviluppo economico, la protezione della sicurezza nazionale e, infine, l'interesse pubblico.

L'iniziativa rilancia l'opportunità, per tutti gli Stati, di sostenere e sviluppare un contesto aperto, corretto e non discriminatorio, per consentire il vicendevole beneficio a tutti e la condivisione di ogni sviluppo derivato dall'uso di tecnologie avanzate. Allo stesso tempo, sottolinea il piano cinese, gli Stati hanno la responsabilità e il diritto di assicurare la protezione dei dati rilevanti per il Paese, dei dati personali dei loro cittadini, per la sicurezza nazionale, pubblica ed economica, assieme alla stabilità sociale.

Obiettivo dell'iniziativa?

Auspicare la convergenza di tutte le parti in commedia per la creazione di un terreno di dialogo e cooperazione sulla base del rispetto reciproco e la costruzione di un futuro condiviso nel cyberspazio, capace di portare "…*pace, sicurezza,*

apertura, cooperazione ed ordine", sulla base di 8 azioni operative che, secondo il governo cinese, prevedano che:

1. Gli Stati gestiscano i dati sulla sicurezza in modo completo, obiettivo, basato su evidenze, per mantenere aperta, sicura e stabile, la *supply chain* dei prodotti e dei servizi globali nell'ICT.
2. Gli Stati debbano sostenere atteggiamenti chiari contro qualunque attività che danneggi o sottragga dati importanti per le infrastrutture critiche dello Stato o usi dati nazionali per condurre attività che minino la sicurezza e l'interesse pubblico di altri Stati.
3. Gli Stati debbano prendere ogni iniziativa per prevenire o bloccare ogni attività che metta a repentaglio le informazioni personali raccolte attraverso l'ICT ed opporsi alla sorveglianza di massa di altri Stati o alla raccolta non autorizzata di informazioni personali di altri Stati attraverso strumenti di ICT.
4. Gli Stati debbano incoraggiare le società private a rispettare la legge e le norme degli Stati dove operano. Gli Stati dovrebbero evitare di chiedere ad aziende nazionali di immagazzinare e gestire dati generati e raccolti in territori diversi da quello nazionale.
5. Gli Stati debbano rispettare la sovranità, la giurisdizione e la *governance* dei dati di altri Stati e non raccogliere dati custoditi in altri Stati attraverso l'uso di aziende o individui, senza il permesso dello Stato a cui quei dati appartengono.
6. Se gli Stati hanno bisogno di ottenere dati dall'estero, per esigenze di applicazione di legge, come nel caso della lotta alla criminalità, dovrebbero farlo attraverso apposita assistenza giudiziaria o altri accordi multilaterali e bilaterali pertinenti. Qualsiasi accordo bilaterale sull'accesso ai dati tra due Stati non dovrebbe violare la sovranità giudiziaria e la sicurezza dei dati di uno Stato terzo.
7. I fornitori di prodotti e servizi ICT non dovrebbero

installare *backdoor* nei loro prodotti e servizi, per ottenere illegalmente i dati degli utenti e/o controllare o manipolare i sistemi e i dispositivi degli utenti.

8. Le aziende ICT non dovrebbero perseguire interessi illegittimi, approfittando della dipendenza degli utenti dai loro prodotti, né costringere gli utenti ad aggiornare i propri sistemi e dispositivi. I fornitori di prodotti dovrebbero impegnarsi a informare tempestivamente i loro partner di cooperazione e gli utenti di gravi vulnerabilità nei loro prodotti e offrire rimedi.

Si tratta di 8 punti cruciali per tutti, attraverso cui le autorità cinesi affermano il doppio principio del rispetto della sovranità cyber o digitale o della tutela della localizzazione dei dati. La stessa esistenza del sistema Great Firewall, che impedisce a **Google** e **Facebook** di operare in Cina, si configura come una misura estrema di difesa dei dati dei cittadini cinesi e delle infrastrutture critiche dalla pervasiva azione di due Big Tech di così grande potenza nell'accaparramento dei dati e nel controllo di ogni informazione che transiti attraverso i propri sistemi.

Il fenomeno, come si può immaginare è ben più ampio, e rischia di rientrare nel graduale processo di balcanizzazione della rete, che non si limita alla creazione di gigantesche intranet nazionali (come in Cina o in Russia o in altri Paesi che hanno già fatto questa scelta). Le circostanze dicono che la corda si sta tirando sempre più (anche a causa delle estremizzazioni necessarie a **Trump** nella sua campagna per le presidenziali di novembre), ma non è detto, come è sperabile, che debba per forza rompersi. E, anzi, auspicabile che riprendano corpo le prassi ordinarie degli organismi internazionali il cui ruolo è proprio quello di creare camere di compensazione nelle tensioni tra Stati.

Nel corso della presentazione, il ministro degli esteri cinese

Wang Yi aveva ribadito un preciso riferimento ad uno degli aspetti più critici: "*…L'appello è anche a tutte le aziende produttrici di apparati per non creare backdoors nei prodotti o servizi offerti, ovvero soluzioni nascoste attraverso le quali raccogliere indebitamente i dati personali contenuti nei flussi di informazioni trasportate, evitando qualsiasi forma di sorveglianza indebita sulle informazioni che appartengono ad altri Paesi e riguardano cittadini di altre nazioni*".

E che i toni non siano destinati ad abbassarsi lo ha confermato il tono delle accuse agli USA, accusati da **Wang Yi** di "*bullismo poco diplomatico*", con le decisioni unilaterali di danneggiare le imprese cinesi di Hi-Tech, anzi di danneggiare aziende "*…che esprimono livelli di competitività molto elevati*" (alterando, quindi, le ordinarie dinamiche di mercato) e con un'azione aggressiva tesa a isolare la Cina nella percezione dell'opinione pubblica dei Paesi avanzati.

Come è noto, l'amministrazione Trump ha fatto della vicenda un vessillo elettorale di peso ed ha esercitato nel corso degli ultimi mesi pressioni molto forti sia sui Paesi del cosiddetto raggruppamento **Five Eyes** (oltre a USA, ci sono Canada, UK, Australia e Nuova Zelanda), sia sui Paesi europei.

Il risultato non è stato univoco. La **Germania** ha risposto picche alle pressioni americane. Del resto il Paese è il principale partner commerciale europeo della Cina ed è di qualche giorno fa la pressione della Cancelliera **Angela Merkel**, perché la Cina apra a **Deutsche Telekom**. La **Francia**, ha adottato un atteggiamento analogo, mentre la Spagna ha per il momento chiuso le porte. Situazione *stop-and-go* in Italia, dove non sembra al momento prevalere un atteggiamento più attento agli interessi del Paese, ma si registra una certa resistenza ai diktat dell'amministrazione americana.

Il vero problema è che l'intera architettura della campagna sulla presunta volontà da parte di aziende cinesi di carpire dati di cittadini di Paesi democratici da trasferire in Cina,

per ragioni di sorveglianza globale, non ha alcun riscontro. La stessa *boutade*, presentata qualche giorno fa dal quotidiano ***Il Foglio*** (in Italia e all'estero da altre testate) come uno scoop senza precedenti, ovvero il caso di informazioni su personalità occidentali (tra cui alcune migliaia di italiani) raccolte in Cina, si rifaceva a informazioni anagrafiche disponibili in chiaro su internet.

In tutta questa bagarre, solo pochi ricordano che 5-6 grandi oligarchie di **Big Tech** statunitensi, raccolgono, da oltre 10 anni, miliardi di informazioni e dati personali di centinaia di milioni di persone, informazioni e dati personali in qualche caso molto dettagliati e riservati, comprese enormi quantità di informazioni sanitarie. Oggetto di tali attenzioni tutti i cittadini di tutti i paesi avanzati e non.

Montagne di informazioni e dati personali raccolti attraverso social, acquisti online, sistemi informativi aziendali, comunicazioni tra persone, tracciamenti di centinaia di milioni di telefonini.

Montagne di informazioni e dati personali che vengono spesso custoditi in sistemi Cloud trasferiti ovunque nel mondo e che quando sono custodite in sedi europee sono abbondantemente spiate e analizzate.

Montagne di dati che, se custoditi in apparati Cloud di proprietà americana, possono essere in qualunque momento soggetti a quanto previsto dal **Cloud Act**, norma americana approvata nel febbraio 2018 che consente all'amministrazione americana di avere accesso a qualunque *storage* di dati custoditi presso aziende americane in ogni parte del mondo. Naturalmente si tratta di un obbligo di aziende americane verso il governo del loro Paese, ma si tratta altresì di un obbligo che per non essere rispettato deve esser fatto mantenendo all'oscuro il cliente servito nel Paese d'origine dei dati e le stesse autorità del Paese in questione.

Montagne di informazioni che, una volta raccolte, vengono trattate da sofisticati sistemi di intelligenza artificiale capaci di creare per ciascun profilo, tra centinaia e centinaia di milioni di persone, millimetrici psico-grammi che profilano vita e miracoli di ciascuno, carattere, temperamento e tratti comportamentali.

Montagne di dati che registrano chi siete, come state, quali sono le vostre finanze, i vostri affetti, i vostri difetti e i vostri vizi, ma anche quale aspettativa di vita in base alle vostre condizioni di salute e quale previsione di comportamenti in base a ciò che abitualmente fate. Tutte informazioni che non servono assolutamente solo per orientare i vostri acquisti. Una montagna del genere non partorisce un minuscolo topolino.

https://www.key4biz.it/usa-cina-una-guerra-hi-tech-che-dannegg ia-tutti-e-da-cui-leuropa-deve-sfilarsi/323446/

Synergized search is key to success in the new normal

30-second summary:

- Given that consumers run billions of searches every day – with Google estimated to process 40,000 per second it’s clear marketers need a smart strategy to cut through the competition.
- The question is: Will they drive the highest traffic and

performance with SEO or PPC?
- Head of Paid Media at Tug shares insight on how perfectly balancing these two facets can lead to success in the new normal.

Consumer activity online is at an all-time high. So, it's no surprise many marketers are aiming to make the most of it by hooking their attention early, at the point of search. But deciding how best to do so isn't necessarily easy.

Given that consumers run billions of searches every day – with Google estimated to process 40,000 per second – it's clear marketers need a smart strategy to cut through the competition. The question is: will they drive the highest traffic and performance with search engine optimization (SEO) or pay per click (PPC)?

Both have their own advantages and drawbacks. PPC is a quick win, enabling businesses to rapidly reach consumers and boost visibility. But its lead generation power only lasts while the money flows and, depending on campaign scale and scope, those costs can run high. Meanwhile, SEO delivers more lasting rewards and higher click-through rates (CTRs), often for less investment. Yet marketers might have a long wait before organic searches pay off, and may still fall behind dominant digital marketplaces for certain keywords.

Ultimately, the smartest route lies neither one way nor the other, but in a combination of both. Blending PPC and SEO not only generates stronger results but also balances out their respective shortcomings, offering marketers the best chance of success in the new ever-changing normal.

Utilizing a combination of paid and organic search tactics isn't new – but it's never been clear how marketers can best do this, or a way to visualize the data for optimization. Leveraging PPC and SEO in conjunction with one another can be challenging, but creating the perfect synergy is possible if

marketers focus on the following three factors:

Unify search operations

With consumers spending a quarter of their waking day online, marketers have plenty of chances to spark their interest through search. To outmanoeuvre rivals and capture eyeballs first, brands must make fast yet informed decisions about which approach will produce the ideal outcome.

Achieving this requires holistic insight which, in turn, calls for greater unity. Due to the general view of PPC and SEO as separate entities, teams often operate in silos, but this isolates valuable knowledge around consumer behaviour and the tactics that generate the biggest rewards. Simple as it sounds, removing divisions and encouraging teams to share their insight can significantly improve campaign execution and drive more efficient CPAs.

For example, information from the PPC teams on the best performing keywords and ad copy will help SEO teams to optimize meta descriptions and website content.

Sharing information on what keywords campaigns are covering will also prevent the doubling up of efforts – for example, as organic keyword positions improve, there might be an opportunity to pull back PPC activity and reallocate budget to other keywords to increase the overall coverage. Similarly, updates from the SEO team on keywords that are particularly competitive to rank in top positions are an opportunity for PPC to drive incremental conversions. And, on a more fundamental level, by sharing any new or emerging search terms with each other, both SEO and PPC teams can ensure they are up-to-date and reacting as quickly as possible to opportunities.

Select tech that drives collaboration

The next step is integrated technology. Implementing tools that collate and merge data from multiple sources – including PPC and SEO campaigns – will make collaboration easier. That's not to mention generating a complete overview of collective search operations, performance, and opportunities for businesses.

A holistic and unified dashboard, for example, can provide visibility of combined search performance against KPIs and competitor activity. This enables PPC and SEO teams to identify where there are opportunities and how strategies can be adjusted to leverage them, without duplicating each other's efforts. Marketers can understand where organic rankings are high, and competitor activity low, and vice versa, which means they know when to reduce PPC activity, as well as opportunities where it can drive incremental conversions over and above what SEO can deliver.

All of this, however, depends on accuracy and usability. Information needs to be reliable and actionable, which means simply joining up the data dots isn't enough: in addition to robust cleansing, processing and storage, tools must offer accessible visualization.

Although frequently overlooked, clearly-presented data plays a huge part in enhancing everyday activity. Providing a streamlined picture of keywords and performance data is vital, but to ensure teams can pinpoint prime SERPs, accelerate traffic, and increase conversions, businesses also need tools that allow their teams to quickly find and activate key insights.

Don’t forget human checks

Dialing up tech use, however, does come with a word of warning – no matter how smart platforms may be, they can’t entirely replace human experience and expertise. On their own, sophisticated tools bring a range of benefits that go far beyond translating data into a more cohesive and user-friendly format. The most advanced boast immediate alerts that tell PPC teams where their competitors are bidding – or not – and use artificially intelligent (AI) analysis to deliver a cross-market, sector, and classification perspective on SEO activity.

Human knowledge is still paramount to steering search campaigns in the right direction and picking up on the nuances that machines miss. For instance, problem-solving machines might take the quickest path to objective completion for certain pages or messages, but seasoned search professionals may see the potential for longer-term uses that deliver higher incremental value.

As a result, organizations must avoid the perils of over-reliance on their marketing tools. By persistently applying manual reviews and checking automated conclusions against human knowledge, they can tap the best of tech and people power.

Today’s marketing leaders are grappling with multiple uncertainties, but when it comes to search, the way forward is clear. PPC and SEO are complementary forces; producing deeper insights and higher returns together, as well as minimizing risk. By connecting the two and taking a considered approach to data-driven search strategy, businesses can ensure campaigns are strong enough to succeed in the new normal and take on whatever tomorrow brings.

Asher Gordon is Head of Paid Media at Tug. He leads a multi-disciplined media team who plan, buy, and deliver integrated

media plans for a diverse set of clients. With over 10 years experience working across multiple markets and brands at PHD and Wavemaker, Asher works with clients to better their marketing goals and drive their business forward.

More about:

https://www.searchenginewatch.com/2020/09/28/synergized-search-is-key-to-success-in-the-new-normal/

Navigating a cookieless future

30-second summary:

- On September 16, Apple launched iOS 14, which is a major overhaul of the Apple operating system and would require users to authorize information known as (IDFA).
- This was followed by announcements from Google that they will be following a similar path for Google Chrome, effectively turning off tracking on Safari, which commands 90 percent usage on iPhones, and Chrome, which commands five percent.
- These moves towards user privacy and marketing compliance are effectively a pivot away from the traditional advertising and search marketing industry, which will impact later players like Facebook to national media agencies like GroupM.
- More details on how marketers can navigate in a

cookieless world.

One of the most impactful changes to internet advertising and media has stayed mostly unspoken in agency and SEO chatter. However, like the switch from a desktop landscape to a mobile landscape, there is no reprieve from the coming cookieless world.

On September 16, Apple launched iOS 14, which is a major overhaul of the Apple operating system and would require users to authorize information known as (IDFA). IDFA is used to track user behavior for advertising.

This was followed by announcements from Google that they will be following a similar path for Google Chrome, effectively turning off tracking on Safari, which commands 90 percent usage on iPhones, and Chrome, which commands five percent.

These moves towards user privacy and marketing compliance are effectively a pivot away from the traditional advertising and search marketing industry, which will impact later players like Facebook to national media agencies like GroupM.

Content created in partnership with SherloQ™, Inc.

National TV advertisers and PPC advertisers are not waiting around

Once again led by the advertising and search category of injury law, due to the highly competitive and expensive nature, we are seeing a couple of key movers.

Smith & Hassler, a nationally recognized personal injury law firm that famously uses Judge Alex Ferrer and William Shatner as TV spokespeople, and Mike Slocumb Law, a firm that is known for its use of celebrity spokespeople and a sometimes outrageous style. They are both first use cases of using Natural Language Understanding (NLU) for content and first-

party data extraction, and automatic AI, which assists in marketing automation to Google without the use of cookies.

In both cases, the companies are working with and have implemented SherloQ™, powered by IBM Watson, to implement cookieless changes and compliance to market their websites.

A recent story from AdWeek quoted Andrew Casale about a cookieless future for publishers, who said it best,

> *"Publishers haven't seen a recovery in their CPMs, and similar to Root, believes the focus of online media trading will be publishers' first-party data as such a method of audience targeting will mean less personal information is traded between (comparatively) anonymous ad-tech players."*

The rapid move towards using first-party data and AI automation will not be limited to a single industry. Privacy is a big selling feature and while Apple has allowed an extension to IDFA, mostly due to the time needed for developers to employ these new frameworks, Apple and Google are not going to wait for the advertising industry's input.

If your agency or enterprise wants to learn more about how SherloQ™, powered by IBM Watson, can help navigate a cookieless world, please download our white paper to learn more about our framework.

More about:

https://www.searchenginewatch.com/2020/09/28/navigating-a-cookieless-future/

Algorithmic accountability: il difficile ‘trade off’ fra efficienza e responsabilità degli algoritmi al Fubinar della Fub

Cresce nelle nostre vite la presenza degli algoritmi e di pari passo aumenta anche la preoccupazione per la sensazione di opacità che spesso i sistemi automatici porta con sé. Il funzionamento e soprattutto la responsabilità degli algoritmi sono un tema complesso e multidisciplinare, sempre più urgente su vari fronti a partire da quello giuridico. Questo in sintesi il tema del Fubinar **‘Algorthmic accountability: Affidabilità e responsabilità degli algoritmi”.**

Hanno partecipato **Antonio Sassano**, Presidente, Fondazione Ugo Bordoni; il Professore di Computer Science**Joshua A. Kroll**, Naval Postgraduate School di Monterey, CA (Keynote “A path towards Trustworhy and Responsible AI”); **Fabio Bassan**,Università di Roma Tre; **Giovanna De Minico**, Università di Napoli “Federico II” e Comitato scientifico FUB; **Giuseppe Francesco Italiano**, Università Luiss “Guido Carli”; **Stefano Quintarelli,** European Artificial Intelligence High Level Group; moderatore **Marco Bianchi**, Ricercatore, Fondazione Ugo Bordoni**.**

La domanda di fondo

“La domanda di fondo è quali tecniche debbano essere messe in campo perché gli algoritmi rendano conto delle loro attività”,

ha detto **Antonio Sassano**, presidente della Fub, aprendo i lavori. Ma *"Le logiche che conducono algoritmi sofisticati e in grado di individuare soluzioni ottime o subottime di alta qualità, sono difficilmente spiegabili. Anche da parte dello stesso progettista",* ha aggiunto.

Trade off fra efficienza e accountability

"trade-off" tra efficienza e "accountability": possiamo rendere i nostri algoritmi "spiegabili" riducendo la loro capacità di individuare soluzioni efficienti.

> *#Fubinar @A_Sassano*
>
> *— FondazioneUgoBordoni (@FondBordoni) September 24, 2020*

Ma Chi valuterà il "trade-off" tra riduzione della qualità delle soluzioni e spiegabilità delle logiche algoritmiche? Chi accetterà di ridurre le percentuale di guarigioni pur di poter spiegare ai pazienti perché si è scelta una terapia piuttosto che un'altra?

Algoritmi e sistemi responsabili

L'intervento di **Joshua A. Kroll**, Naval Postgraduate School di Monterey, CA *(Keynote "A path towards Trustworhy and Responsible AI"*), è stato anticipato in questa intervista pubblicata su Key4biz, in cui il professore ricorda come i sistemi di cui fanno parte gli algoritmi sono *"più ampi del software preso nella sua semplicità"*. In altre parole, nell'analisi degli algoritmi è importante considerare l'intero contesto sistemico in cui è calato. Ad esempio, per quanto riguarda la guida autonoma, per valutare il funzionamento dell'algoritmo è necessario prendere in considerazione la velocità, le condizioni dell'asfalto, la luminosità, le curve,

la segnaletica. E’ necessario vigilare sul “corretto” funzionamento degli algoritmi anche da punto di vista etico. *“Bisogna costruire i sistemi in modo che siano responsabili”*, ha detto.

Il beneficio dell’automazione può essere illustrato ad esempio pensando al controllo dei biglietti di un treno. Se il controllo umano, tramite controllore, avviene a bordo, l’utilizzo di tornelli per svolgere la medesima funzione avviene già prima che i passeggeri salgano sulla vettura, eliminando alla radice la necessità che il controllore in carne ed ossa svolga la sua mansione, ottimizzando così il lavoro.

AI e algoritmi difficile applicazione della legge

Difficile, in ambito giuridico, parlare di Intelligenza Artificiale e algoritmi*. “Il termine accountability in ambito giuridico significa sia liability che accountability* – sottolinea **Fabio Bassan**,Università di Roma Tre – *Noi giuristi dobbiamo risolvere entrambi questi profili”*. Si tratta di temi di frontiera, difficili da affrontare. Ed è per questo che secondo Bassan sarà sempre più importante il tema della compliance per la trasparenza degli algoritmi usati dalle aziende, che loro sponte saranno chiamate a dire spontaneamente come funziona l’algoritmo. Un caso concreto, invece, riguarda gli smart contract della blockchain. *“Nella blockchain l’ambito di controllo delle autorità può essere considerato ex ante”,* dice Bassan. Secondo cui l’approccio legislativo deve essere quello di applicare la legge esistente al nuovo che avanza, ammodernando la legislazione. In lacuni settori, infine, serve un sandbox giuridico per affrontare gli OTT che entreranno anche in settori regolati.

Ma non si può dire ‘me l’ha detto la macchina’

Dal canto suo, **Giovanna De Minico**, Università di Napoli “Federico II” e membro del Comitato scientifico FUB, ha ricordato come *“l’evoluzione dei big data ha portato alla destrutturazione di tutte le categorie politiche* – ha detto – *e ha cambiato il concetto stesso di atto pubblico. Se c’è di mezzo l’algoritmo, c’è di mezzo la macchina”.* Un cambiamento radicale che modifica i capisaldi di interi ambiti: dalla privacy all’antitrust.

Cosa resta della responsabilità politica, quando c’è di mezzo una analisi predittiva pensata da una macchina? Chi è responsabile? Il Parlamento?

E’ pur vero che il GDPR fa rientrare ogni decisione in ambito umano, ricreando così un perimetro di “atto pubblico” sulla base di pratiche di risultanze algoritmiche. E quindi nessuno potrà mai dire di aver deciso in un modo o nell’altro adducendo come motivazione *“me l’ha detto la macchina”. “Serve uno spatium deliberandi, uno spazio decisionale che va assicurato all’uomo”*, dice De Minico.

Automazione ridefinisce le regole del sistema

Dal canto suo, **Stefano Quintarelli**, membro dell’European Artificial Intelligence High Level Group, che in questo ambito ha collaborato alla stesura di diversi documenti in materia di AI, ha detto che con il machine learning ridefinisce il perimetro e le regole, modificando di fatto il concetto di intelligenza.

“Con il Machine Learning un sistema non difettoso, ben realizzato e perfettamente funzionante genera, per

costruzione, alcune predizioni errate – ha detto Quintarelli – *Quando queste predizioni fatte dalla macchina possono avere un effetto pregiudizievole sulla vita delle persone è necessario sempre considerare il sistema allargato, non limitandosi solo alla procedura, all'agoritmo, all'addestramento, ai dati. E' necessario considerare anche le procedure che consentono – senza pregiudizio alcuno per la persona – di individuare la predizione errata, correggerla e, ove possibile, migliorare il sistema. Questo tipo di procedure di rimedio formano parte di una vista allargata del sistema di IA, vanno concepite assieme ad esso sin dalla fase di progettazione del sistema, pratica che chiamiamo 'redress by design'".*

"*Con il machine learning affrontiamo i problemi con una velocità e una capacità impensabile in passato* – ha detto – *la scala aumenta ma per sua stessa natura il machine learning farà delle predizioni errate*". Ma in questo caso non si potrà parlare di responsabilità quando il sistema non prevederà questi errori. E' per questo che esistono le "*procedure di rimedio*" perché si sa già che le macchine sbaglieranno. Infine, la guida autonoma potrebbe in futuro abbattere del 90% le vittime della strada. Resta comunque quel 10% di vittime. Ma potremo privare la società dei benefici attesi, in nome di quel rimanente 10% di vittime? In definitiva, l'automazione cambia la natura delle regole; una volta introdotta nel sistema, bisognerà applicare procedure di rimedio; infine, in un sistema non bisogna valutare i casi singoli ma i vantaggi complessivi.

Fattore umano resta determinante

Tornando al tema del trade off fra accountability e spiegabilità degli algoritmi, **Giuseppe Francesco Italiano**, Università Luiss "Guido Carli", dice che molto spesso gli algoritmi sono troppo complessi per essere spiegate tramite semplici alberi decisionali, come ad esempio quelli per il riconoscimento facciale.

Per quanto riguarda l’explainable AI, poi, il fallimento può dipendere a volte in toto dal fattore umano. Ad esempio, emblematico il caso dell’algoritmo che a Boston prometteva di abbattere di 5 milioni all’anno il sistema di scuolabus cittadino, ottimizzando appunto il sistema di trasporto degli studenti cittadini. Un algoritmo perfetto, che però non fu possibile utilizzare per le proteste di una parte dei destinatari. “In questo caso, il singolo che protesta non considera i vantaggi per la collettività” e manda a monte un sistema che la macchina era riuscita a ottimizzare al meglio, ma soltanto sulla carta.

Per saperne di più: AIFUB

> *Algorithmic accountability: il difficile ‘trade off’ fra efficienza e responsabilità degli algoritmi al Fubinar della Fub*

Huawei Connect 2020, i cinque settori strategici per creare valore ICT

Si è aperta oggi a Shanghai una nuova edizione di HUAWEI CONNECT 2020, l’evento annuale di Huawei in cui l’azienda presenta strategie e soluzioni dedicate all’intero settore ICT.

Nel 2016 Huawei ha cominciato a immaginare un mondo intelligente e chiamato i suoi partner globali a collaborare

alla realizzazione di questa visione e di un ecosistema che la supportasse. Nel 2017 Huawei ha quindi annunciato il suo obiettivo di diventare uno dei cinque principali fornitori di servizi cloud al mondo mentre nel 2018 e nel 2019 l'azienda ha svelato rispettivamente la propria strategia IA e computing.

Come creare valore

Quest'anno, con il lancio del 5G su scala globale, connettività, cloud, intelligenza artificiale, computing e applicazioni industriali si combinano insieme per offrire opportunità senza precedenti per il settore ICT. Pertanto il tema dell'evento di quest'anno è *"Creare nuovo valore attraverso la sinergia tra cinque settori tecnologici".*

Huawei si concentrerà sull'applicazione delle tecnologie ICT in ambito industriale e sull'offerta di soluzioni specifiche per ogni scenario, così da contribuire alla crescita delle aziende e supportare i governi nel raggiungimento dei loro obiettivi strategici di rilancio dell'industria nazionale e nel miglioramento della governance statale.

Guo Ping 'Settore ICT registrerà una crescita significativa'

Durante l'evento di apertura, **Guo Ping**, Rotating Chairman di Huawei (nella foto), ha dichiarato: *"Con sempre più governi e aziende che decidono di digitalizzarsi, il settore ICT registrerà una crescita significativa. Non vediamo l'ora di dare inizio a questo nuovo capitolo insieme ai nostri partner".*

Ping ha illustrato il contributo di Huawei nella realizzazione di aziende, campus e città intelligenti, integrando le tecnologie ICT con il know-how dei settori fornendo soluzioni specifiche per ogni scenario così da creare valore per governi e aziende.

Settori strategici

Huawei continuerà inoltre a investire nei seguenti settori:

- **Reti**: Huawei ha proposto il concetto di connettività intelligente, con l'obiettivo di fornire una rete iper-automatizzata, che possa offrire un accesso gigabit onnipresente e un'esperienza deterministica, nonché consentire aggiornamenti intelligenti dei principali sistemi aziendali di governi e aziende.
- **Computing**: Huawei si impegna a fornire ai propri clienti una potenza di elaborazione diversificata, separando il software dall'hardware per adattare il calcolo a seconda delle diverse esigenze di elaborazione, inclusi x86 e Kunpeng.
- **Servizi cloud**: Huawei ha implementato 23 aree cloud in tutto il mondo, con la partecipazione di oltre 1,5 milioni di sviluppatori.
- **Intelligenza Artificiale:** Huawei mira a integrare l'IA all'interno dei principali sistemi di governi e aziende, utilizzando know-how e dati per stabilire le competenze di base dei sistemi basati su IA.
- Connettività, computing, cloud e intelligenza artificiale sono tutti aspetti che devono essere declinati all'interno di **applicazioni industriali** che sono il collante di tutti questi aspetti.

Huawei ritiene che la sinergia tra questi 5 settori tecnologici offrirà enormi opportunità all'intero settore ICT. Insieme ai suoi partner, l'azienda auspica una crescita globale che consenta di trarre beneficio dalla nuova catena di valore.

Sostegno ai partner

Ping ha inoltre ripercorso i tre principi proposti da Huawei nel 2016, quando l'azienda aveva illustrato la sua visione di un ecosistema diversificato e fiorente. Guo ha infine sottolineato che Huawei sosterrà costantemente i suoi partner nel loro impegno per lo sviluppo di applicazioni industriali, per il rafforzamento della catena di approvvigionamento e per la crescita dei propri settori di riferimento.

All'evento è intervenuto anche il sindaco di Shenzhen, **Chen Rugui**. *"Shenzhen sta sfruttando al massimo le opportunità offerte dagli sviluppi in corso nella Greater Bay Area di Guangdong-Hong Kong-Macao e nell'area di Shenzhen dove si stanno svolgendo i trial.. Ci impegniamo ad alzare il livello delle grandi città in tutto il mondo. Usufruendo delle avanzate tecnologie di Huawei e di altre aziende tecnologiche, la nostra città diventa più intelligente di giorno in giorno. Coglieremo le nuove opportunità offerte dal 5G, miglioreremo l'adozione del 5G in più scenari, promuoveremo l'Internet industriale, guideremo l'interconnessione verticale e sosterremo la trasformazione digitale delle PMI. Shenzhen mira a porsi come il gold standard dell'economia digitale cinese. Crediamo fermamente che la tecnologia abbia tutto il potenziale per rendere migliore la vita e più dinamiche le città"*, ha aggiunto il sindaco.

Chen Jinzu, General Manager di Shenzhen Airport Group, e **Tang Shaojie**, General Manager di Shenzhen Metro Group, hanno raccontato la loro esperienza nella costruzione di aeroporti e sistemi metropolitani intelligenti. In questa occasione, Huawei ha anche annunciato il suo slogan per lo sviluppo dell'ecosistema con i suoi partner d'eccellenza in tutto il mondo: *"Innovare, crescere e vincere insieme".*

Zhang Ping'an, Presidente del Consumer Cloud Service, Huawei Consumer Business Group, ha spiegato come i Huawei Mobile

Services (HMS) abbiano consentito l’innovazione digitale in vari settori come finanza, istruzione, e intrattenimento, creando eccellenti servizi di IA per soddisfare le molteplici esigenze degli utenti.

https://www.key4biz.it/huawei-connect-2020-i-cinque-settori-strategici-per-creare-valore-ict/322587/

War Stories: How Forza learned to love neural nets to train AI drivers

reader comments

3 with 3 posters participating

Share this story

[embedded content]
Produced by Justin Wolfson, edited by Shandor Garrison. Click here for transcript.
Once an upstart, the *Forza* franchise is now firmly established within the pantheon of great racing games. The first installment was created as the Xbox’s answer to *Gran Turismo*, but with a healthy helping of online multiplayer racing, too. Since then, it has grown with Microsoft’s Xbox consoles, with more realistic graphics and ever-more accurate physics in the track-focused *Forza Motorsport* series as well as evolving into open-world adventuring (and even a trip to the Lego dimension)

for the *Forza Horizon* games.

If you're one of the millions of people who've played a Forza racing game, you're probably aware of the games' AI opponents, called "Drivatars." When the first Drivatars debuted in *Forza Motorsport* in 2005, they were a substantial improvement over the NPCs we raced in other driving games, which often just followed the same preprogrammed route around the track. "It was a machine-learning system on a hard drive using a Bayesian Neural Network to record [racing] lines and characteristics of how somebody drove a car," explains Dan Greenawalt, creative director of the *Forza* franchise at Turn 10 Studios, in our latest War Stories video.

In fact, the technology originated at Microsoft Research's outpost in Cambridge, England, where computer scientists started using neural nets to see if it was possible to get a computer to identify a Formula 1 driver by the way they drove through corners.

In the years since, Drivatars have evolved considerably—and not always in ways that players appreciate. For the first few games, which were written for the Xbox and Xbox 360 consoles, Drivatars lived entirely on the console's local hard drive. As you lapped the various tracks in the game, the Drivatar system was quietly using that data in the background to train the AI you were racing against. But with the move to the Xbox One, Greenawalt's team decided to make use of the cloud.

"All of a sudden going to Thunderhead, we had millions of laps within what, a week?" Greenawalt says. "It was crazy."

More data, more problems

Very quickly, the team at Turn 10 began learning a lot about the way different players drove their cars. Tracks aren't uniform—they vary in elevation, width, corner profile, and more—and that complicates the way the neural net tries to

generalize a racing line. Things get even more complicated when you're racing against other cars; human players are much more aggressive with AI drivers than other humans, and by *Forza Motorsport 6*, the games started to include a way to toggle off some of the AI's aggression as a way to combat single-player games that became demolition derbies when the AI tried to wreck the humans at every opportunity.

In this video—recorded remotely due to COVID-19—Greenawalt goes into some degree of detail in recalling how his team has handled these challenges across the years and even discusses the dreaded problem of "rubber banding," where the AI cars slow down a little to allow a human player to catch up after a spin. Even if you're not a fan of racing games, we think you'll find this one pretty engrossing.

Listing image by Ars Technica

https://arstechnica.com/?p=1705877

AI ruined chess. Now it's making the game beautiful again

reader comments

58 with 44 posters participating

Share this story

Chess has a reputation for cold logic, but Vladimir Kramnik loves the game for its beauty.

“It’s a kind of creation,” he says. His passion for the artistry of minds clashing over the board, trading complex but elegant provocations and counters, helped him dethrone Garry Kasparov in 2000 and spend several years as world champion.

Yet Kramnik, who retired from competitive chess last year, also believes his beloved game has grown less creative. He partly blames computers, whose soulless calculations have produced a vast library of openings and defenses that top-flight players know by rote. “For quite a number of games on the highest level, half of the game—sometimes a full game—is played out of memory,” Kramnik says. “You don’t even play your own preparation; you play your computer’s preparation.”

Wednesday, Kramnik presented some ideas for how to restore some of the human art to chess, with help from a counterintuitive source—the world’s most powerful chess computer. He teamed up with Alphabet artificial intelligence lab DeepMind, whose researchers challenged their superhuman game-playing software AlphaZero to learn nine variants of chess chosen to jolt players into creative new patterns.

In 2017, AlphaZero showed it could teach itself to roundly beat the best computer players at either chess, Go, or the Japanese game shogi. Kramnik says its latest results reveal beguiling new vistas of chess to be explored, if people are willing to adopt some small changes to the established rules.

The project also showcased a more collaborative mode for the relationship between chess players and machines. “Chess engines were initially built to play against humans with the

goal of defeating them," says Nenad Tomašev, a DeepMind researcher who worked on the project. "Now we see a system like AlphaZero used for creative exploration in tandem with humans rather than opposed to them."

People have played chess for around 1,500 years, and tweaks to the rules aren't new. Neither are grumbles that computers have made the game boring.

New rules

Chess spread rapidly around 500 years ago after European players promoted a slow-moving piece into the powerful modern-day queen, giving the game more zip. In 1996, one year before IBM's Deep Blue defeated Kasparov, chess wunderkind-turned-fugitive Bobby Fischer called a press conference in Buenos Aires and complained that chess needed a redesign to demote computer-enhanced memorization and encourage creativity. He unveiled Fischer Random Chess, which preserves the usual rules of play but randomizes the starting positions of the powerful pieces on the back rank of the board each game. Fischer Random, also known as Chess960, slowly earned a niche in the chess world and now has its own tournaments.

DeepMind and Kramnik tapped AlphaZero's ability to learn a game from scratch to explore new variants more quickly than the decades or centuries of human play that would reveal their beauty and flaws. "You don't want to invest many months or years of your life trying to play something, only to realize that, 'Oh, this just isn't a beautiful game,'" says Tomašev.

AlphaZero is a more flexible and powerful successor to AlphaGo, which laid down a marker in AI history when it defeated a champion at Go in 2016. It starts learning a game equipped with only the rules, a way to keep score, and a preprogrammed urge to experiment and win. "When it starts playing it's so bad I want to hide under my table," says Ulrich Paquet, another DeepMind researcher on the project.

“But seeing it evolve from a void of nothingness is exciting and almost pure.”

In chess, AlphaZero initially doesn’t know it can take an opponent’s pieces. Over hours of high-speed play against successively more powerful incarnations of itself, it becomes more skilled and, to some eyes more natural than prior chess engines. In the process, it rediscovers ideas seen in centuries of human chess and adds flair of its own. English grandmaster Matthew Sadler described poring over AlphaZero’s games as like “discovering the secret notebooks of some great player from the past.”

Enlarge / Former chess world champion Vladimir Kramnik, left, worked with Alphabet’s DeepMind, founded by Demis Hassabis, right, to explore new forms of chess using artificial

intelligence.
The nine alternative visions of chess that AlphaZero tested included no-castling chess, which Kramnik and others had already been thinking about and which had its first dedicated tournament in January. It eliminates a move called castling that allows a player to tuck their king behind a protective screen of other pieces—powerful fortification that can also be stifling. Five of the variants altered the movement of pawns, including torpedo chess, in which pawns can move up to two squares at a time throughout the game, instead of only on their first move.

One way of reading AlphaZero's results is in cold numbers. Draws were less common under no-castling chess than under conventional rules. And learning different rules shifted the value AlphaZero placed on different pieces: under conventional rules, it valued a queen at 9.5 pawns; under torpedo rules, the queen was only worth 7.1 pawns.

But is it fun?

DeepMind's researchers were ultimately more interested in the analysis of the other great chess brain on the project, Kramnik. "This is not about numbers, but whether it is qualitatively, aesthetically pleasing for humans to sit down and play," says Tomašev. A technical paper released Wednesday includes more than 70 pages of commentary by Kramnik on AlphaZero's explorations.

Kramnik saw flashes of beauty in how AlphaZero adapted to the new rules. No-castling chess provoked rich new patterns for keeping the king safe, he says. A more extreme change, self-capture chess, in which a player can take their own pieces, proved even more alluring. The rule effectively gives a player more opportunities to sacrifice a piece to get ahead, Kramnik says, a tactic considered a hallmark of elegant play for centuries. "All in all it just makes the game more beautiful,"

he says.

Kramnik hopes AlphaZero's adventures in alien forms of chess will convince players of all levels to try them. "It is our gift to the world of chess," he says. Now could be an opportune moment.

Chess has been gaining popularity for years but experienced a pandemic boost as many people sought new intellectual stimulation, says Jennifer Shahade, a two-time women's US chess champion. Interest in Chess960 has grown too, suggesting an appetite for new types of play, including from some superstars. Later this week, Shahade will provide commentary for a Chess960 tournament including world No.1 Magnus Carlsen and Kasparov, the former champ.

"Mind-bending"

Like Kramnik, Shahade saw things to like in several variants AlphaZero tested, even if changes like allowing pawns to move sideways felt "mind-bending." If any gain traction, some players will still want to lean on computers and deep research to get ahead, but resetting the cycle could be fascinating to watch. "The discoveries would feel fresh—it could be very exciting and benefit a different type of player," says Shahade, who is also women's program director at the US Chess Federation.

DeepMind and Kramnik's project might also encourage computer chess to get more creative, now that machines are unbeatable. "Instead of making computer chess stronger and trashing humans, we can focus on chess as an art in the form of a game," says Eli David, a researcher at Bar-Ilan University in Israel who has built machine-learning-powered chess engines of his own. One grad student in his lab is working on chess software that learns to mimic the style of a particular player, which could make it possible to ask a machine what a favorite grandmaster past or present would do in a particular

situation.

Kramnik’s experience suggests that having humans work with, not against, machines can expand the emotional as well as technical experience of the game. AlphaZero took him to places outside even his vast understanding. “After three moves you simply don’t know what to do,” he says. “It’s a nice feeling, like you’re a child.”

This story originally appeared on wired.com.

https://arstechnica.com/?p=1705570

Google offers to help others with the tricky ethics of AI

Yuchiro Chino | Getty Images

reader comments

66 with 57 posters participating

Share this story

Companies pay cloud-computing providers like Amazon, Microsoft, and Google big money to avoid operating their own digital infrastructure. Google’s cloud division will soon invite customers to outsource something less tangible than CPUs and disk drives—the rights and wrongs of using artificial intelligence.

The company plans to launch new AI ethics services before the

end of the year. Initially, Google will offer others advice on tasks such as spotting racial bias in computer vision systems or developing ethical guidelines that govern AI projects. Longer term, the company may offer to audit customers' AI systems for ethical integrity and charge for ethics advice.

Google's new offerings will test whether a lucrative but increasingly distrusted industry can boost its business by offering ethical pointers. The company is a distant third in the cloud-computing market behind Amazon and Microsoft, and it positions its AI expertise as a competitive advantage. If successful, the new initiative could spawn a new buzzword: EaaS, for ethics as a service, modeled after cloud-industry coinages such as SaaS, for software as a service.

Google has learned some AI ethics lessons the hard way—through its own controversies. In 2015, Google apologized and blocked its Photos app from detecting gorillas after a user reported the service had applied that label to photos of him with a Black friend. In 2018, thousands of Google employees protested a Pentagon contract called Maven that used the company's technology to analyze surveillance imagery from drones.

Soon after, the company released a set of ethical principles for use of its AI technology and said it would no longer compete for similar projects, but it did not rule out all defense work. In the same year, Google acknowledged testing a version of its search engine designed to comply with China's authoritarian censorship and said it would not offer facial recognition technology, as rivals Microsoft and Amazon had for years, because of the risks of abuse.

Google's struggles are part of a broader reckoning among technologists that AI can harm as well as help the world. Facial recognition systems, for example, are often less

accurate for Black people and text software can reinforce stereotypes. At the same time, regulators, lawmakers, and citizens have grown more suspicious of technology's influence on society.

A deeper examination

In response, some companies have invested in research and review processes designed to prevent the technology going off the rails. Microsoft and Google say they now review both new AI products and potential deals for ethics concerns, and they have turned away business as a result.

Tracy Frey, who works on AI strategy at Google's cloud division, says the same trends have prompted customers who rely on Google for powerful AI to ask for ethical help, too. "The world of technology is shifting to saying not 'I'll build it just because I can' but 'Should I?'" she says.

Google has already been helping some customers, such as global banking giant HSBC, think about that. Now, it aims before the end of the year to launch formal AI ethics services. Frey says the first will likely include training courses on topics such as how to spot ethical issues in AI systems, similar to one offered to Google employees, and how to develop and implement AI ethics guidelines. Later, Google may offer consulting services to review or audit customer AI projects, for example to check if a lending algorithm is biased against people from certain demographic groups. Google hasn't yet decided whether it will charge for some of those services.

Google, Facebook, and Microsoft have all recently released technical tools, often free, that developers can use to check their own AI systems for reliability and fairness. IBM launched a tool last year with a "Check fairness" button that examines whether a system's output shows potentially troubling correlation with attributes such as ethnicity or ZIP code.

Going a step further to help customers define their ethical limits for AI could raise ethical questions of its own. “It is very important to us that we don’t sound like the moral police,” Frey says. Her team is working through how to offer customers ethical advice without dictating or taking on responsibility for their choices.

“Legally compelled to make money”

Another challenge is that a company seeking to make money from AI may not be the best moral mentor on curbing the technology, says Brian Green, director of technology ethics at the Markkula Center for Applied Ethics at Santa Clara University. “They’re legally compelled to make money and while ethics can be compatible with that, it might also cause some decisions not to go in the most ethical direction,” he says.

Frey says that Google and its customers are all incentivized to deploy AI ethically because to be broadly accepted the technology has to function well. “Successful AI is dependent on doing it carefully and thoughtfully,” she says. She points to how IBM recently withdrew its facial recognition service amid nationwide protests over police brutality against Black people; it was apparently prompted in part by work like the Gender Shades project, which showed facial analysis algorithms were less accurate on darker skin tones. Microsoft and Amazon quickly said they would pause their own sales to law enforcement until more regulation was in place.

In the end, signing up customers for AI ethics services may depend on convincing companies who turned to Google to move faster into the future that they should in fact move more slowly.

Late last year, Google launched a facial recognition service limited to celebrities that is aimed primarily at companies that need to search or index large collections of entertainment video. Celebrities can opt out, and Google vets

which customers can use the technology.

The ethical review and design process took 18 months, including consultations with civil rights leaders and fixing a problem with training data that caused reduced accuracy for some Black male actors. By the time Google launched the service, Amazon's celebrity recognition service, which also lets celebs opt out, had been open to all for more than two years.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1702049

What's this? A bipartisan plan for AI and national security

Enlarge / Closeup of a Predator MQ-9 uncrewed aerial vehicle.

reader comments

30 with 15 posters participating

Share this story

US Reps. Will Hurd and Robin Kelly are from opposite sides of the ever-widening aisle, but they share a concern that the United States may lose its grip on artificial intelligence, threatening the American economy and the balance of world

power.

On Thursday, Hurd (R-Tex.) and Kelly (D-Ill.) offered suggestions to prevent the US from falling behind China, especially, on applications of AI to defense and national security. They want to cut off China's access to AI-specific silicon chips and push Congress and federal agencies to devote more resources to advancing and safely deploying AI technology.

Although Capitol Hill is increasingly divided, the bipartisan duo claims to see an emerging consensus that China poses a serious threat and that supporting US tech development is a vital remedy.

"American leadership and advanced technology has been critical to our success since World War II, and we are in a race with the government of China," Hurd says. "It's time for Congress to play its role."

Kelly, a member of the Congressional Black Caucus, says that she has found many Republicans, not just Hurd, the only Black Republican in the House, open to working together on tech issues. "I think people in Congress now understand that we need to do more than we have been doing," she says.

The Pentagon's National Defense Strategy, updated in 2018, says AI will be key to staying ahead of rivals such as China and Russia. Thursday's report lays out recommendations on how Congress and the Pentagon should support and direct use of the technology in areas such as autonomous military vehicles. It was written in collaboration with the Bipartisan Policy Center and Georgetown's Center for Security and Emerging Technology, which consulted experts from government, industry, and academia.

The report says the US should work more closely with allies on AI development and standards, while restricting exports to China of technology such as new computer chips to power machine learning. Such hardware has enabled many recent advances by leading corporate labs, such as at Google. The report also urges federal agencies to hand out more money and computing power to support AI development across government, industry, and academia. The Pentagon is asked to think about how court martials will handle questions of liability when autonomous systems are used in war and to talk more about its commitment to ethical uses of AI.

Hurd and Kelly say military AI is so potentially powerful that America should engage in a kind of AI diplomacy to prevent dangerous misunderstandings. One of the report's 25 recommendations is that the US establish AI-specific communication procedures with China and Russia to allow human-to-human dialog to defuse any accidental escalation caused by algorithms. The suggestion has echoes of the Moscow-Washington hotline installed in 1963 during the Cold War. "Imagine in a high-stakes issue: What does a Cuban missile crisis look like with the use of AI?" asks Hurd, who is retiring from Congress at the end of the year.

Cut through the hype

Beyond such worst-case scenarios, the report includes more sober ideas that could help dismantle some hype around military AI and killer robots. It urges the Pentagon to do more to test the robustness of technologies such as machine learning, which can fail in unpredictable ways in fast-changing situations such as a battlefield. Intelligence agencies and the military should focus AI deployment on back-office and noncritical uses until reliability improves, the report says. That could presage fat new contracts to leading computing companies such as Amazon, Microsoft, and Google.

Helen Toner, director of strategy at the Georgetown center, says although the Pentagon and intelligence community are trying to build AI systems that are reliable and responsible, “there’s a question of whether they will have the ability or institutional support.” Congressional funding and oversight would help them get it right, she says.

The paper released Thursday is the second of four on AI strategy issued by Hurd and Kelly with the Bipartisan Policy Center. The first, released earlier this month, focused on the workplace. Its recommendations included reworking education from kindergarten through grad school to prepare more Americans to work with or on AI. The two papers to come are on AI research and development, and AI ethics.

Kelly and Hurd have shared an interest in AI since working on hearings on the subject by the House Oversight Committee’s Subcommittee on Information Technology in 2018. The pair later authored a report warning that the US could lose its leading position on AI. Kelly says she wants to ensure the United States remains a leader in AI, but also that “people in the diverse district I come from have a piece of that pie, and that there are not biases against them or concerns around privacy.”

Falling behind

At the tail end of the Obama administration, the White House produced lengthy documents on how to support US AI development and deployment and address potential downsides such as technological unemployment. The Trump administration chose not to build on those, but last year President Trump signed an executive order directing existing government programs to be tilted towards AI projects. It leaves the US with a less toothy AI strategy than many other nations, including China, which have stood up new programs and funding sources. Hurd and Kelly are trying to change that.

James Lewis, who leads work on technology policy at the Center for Strategic and International Studies, applauds the effort. The timing is good, he says, because more lawmakers are taking an interest in tech policy. “They now realize we’re in a contest with China and have woken up to the fact that technology like AI and semiconductors and cybersecurity are important,” he says. Last week, the Senate voted 96-4 to amend the annual Pentagon budget bill with $25 billion to support domestic research and manufacturing of new chip technology.

Lewis supports restricting chip exports to China—an idea that could gain traction in a Congress showing new interest in tech export controls. He’s skeptical that an AI hotline or inventing special forms of AI diplomacy to prevent autonomous accidents are worthwhile. Events during the Cold War and since, most recently in areas such as cybersecurity, suggest China and Russia don’t take such programs seriously, Lewis says.

Hurd and Kelly are now drafting a congressional resolution incorporating their ideas about AI, including in national security. After that, they’ll start work on AI legislation. “Some of that I hope we get done in this Congress, and others can be taken and run with in the next Congress,” Hurd says.

This story first appeared on wired.com.

https://arstechnica.com/?p=1695629