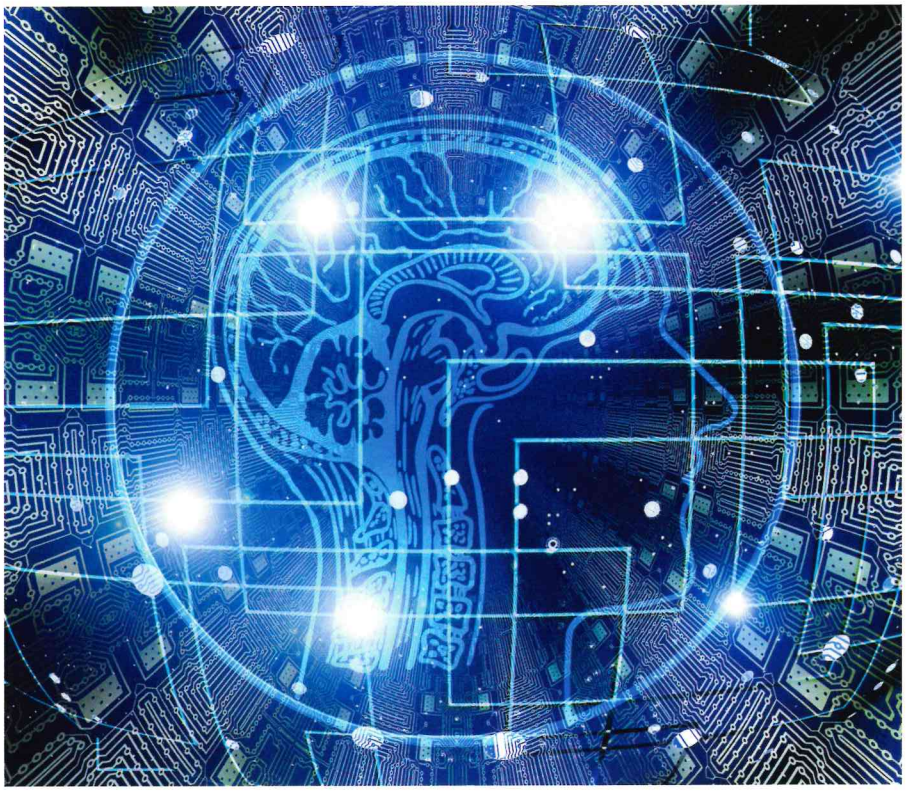
L'intelligenza Artificiale alla prova del GDPR



Intelligenza Artificiale?

L'intelligenza Artificiale, anche se ha una storia lunga di quasi settant'anni alle spalle, solo in tempi recenti ha lasciato il territorio della ricerca accademica per trasferirsi nel mondo reale. Sistemi per la raccomandazione dei prodotti in vendita, assistenti automatici che comprendono la lingua naturale, traduttori automatici, *software* per il riconoscimento facciale sono ormai incorporati nei prodotti di largo consumo e quasi dati per scontati. Le automobili a guida autonoma sembrano ormai dietro l'angolo. Sistemi che hanno la capacità di imparare sono ormai maturi in settori come quello finanziario (per la valutazione relativa alla concessione di prestiti e mutui, ad esempio), del *marketing* (per la profilazione individuale delle abitudini di consumo), della sicurezza (studio delle anomalie comportamentali, modelli predittivi della probabilità di reati in specifiche localizzazioni).

Anche se tutte le applicazioni descritte sono efficaci, esse sono ben lontane dall'IA che la fantascienza ci ha raccontato in moltissime opere: quello che hanno in comune è la limitatezza del loro perimetro. La singolarità (la comparsa delle IA sovrumane) e anche la rivolta delle macchine senzienti può certamente attendere. La realtà per il momento è molto più prosaica e più che di Intelligenza Artificiale si dovrebbe parlare di algoritmi per l'apprendimento automatico *(machine learning)*. Questi algoritmi sono sì in grado di "imparare", ma per farlo hanno bisogno di dati, in grandi quantità.

I dati sono stati definiti, a ragione, la moneta dell'economia digitale e spesso sono appunto usati come mezzo di scambio per ottenere servizi *online* che non richiedono pagamenti in denaro, come Google Maps, Facebook e innumerevoli altri esempi.

La norma europea

Dato che in molti casi i dati in questione sono dati personali, l'uso di queste tecniche ricade in pieno nel perimetro della protezione dei dati, ora regolata in Europa dal (famigerato?) Regolamento Generale per la Protezione dei Dati (RGPD in italiano GDPR in inglese).

L'Unione affronta la regolamentazione sulla protezione dei dati personali definendola come un diritto fondamentale degli individui (assieme alla *"privacy"* o riservatezza, che costituisce un diritto fondamentale a sé stante e distinto). Il Regolamento poggia sul principio che i dati personali che ci riguardano sono sempre e comunque sotto il nostro controllo, anche se ceduti a vari soggetti per svariati motivi (in contrasto va detto con l'approccio degli Stati Uniti, dove i dati, anche personali, una volta ceduti, appartengono in toto al titolare del trattamento).

Il GDPR impone limiti in particolare alle attività di profilazione degli individui, che viene definita come una *"forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona"*.

I paletti (e le sanzioni) previsti però prevedono una ben mirata eccezione, per gli stati e le pubbliche autorità. I soggetti privati, nello sviluppo e nello sfruttamento degli algoritmi di apprendimento automatico hanno l'obbligo di conformarsi a principi e limitazioni ben precise, tenendo conto nel caso del *marketing* diretto che gli interessati possono in qualsiasi momento opporsi.

La sfida della privacy

Dato che gli algoritmi di apprendimento automatico hanno la possibilità se ben usati di generare valore non solo per le aziende, ma anche per i clienti, costruirne di conformi alla regolamentazione diventa fondamentale per intercettarne il potenziale innovativo. Fare questo richiede un cambiamento di prospettiva, anche culturale. Occorre comprendere che operare ignorando i principi della protezione dati diventa ora estremamente rischioso e che i dati personali hanno valore economico solo se acquisiti e trattati in conformità. In particolare con il consenso esplicito dell'interessato, quando necessario (principio della liceità dei trattamenti) e per finalità esplicite e chiaramente comunicate agli interessati (limitazione della finalità). Culturalmente, è necessario combattere la "astinenza da *big data*", malattia che affligge chi era abituato a conservare grandi insiemi di dati personali per finalità non ben specificate e a tempo indeterminato.

Forse la sfida più grande per gli utilizzatori degli algoritmi, soprattutto quelli predittivi che realizzano la profilazione e le decisioni automatizzate, è costituita dal "problema della scatola nera". Data la loro particolare natura, questi algoritmi imparano dai dati e operano le loro decisioni senza la possibilità per gli utenti (e per gli stessi sviluppatori) di ricostruire i singoli passaggi che hanno portato al risultato finale. Il principio di trasparenza e responsabilità *(accountability)* della disciplina sulla protezione sono difficilmente soddisfatti da modelli simili. Ripensarli in modo da essere in grado di giustificare e ricostruire le decisioni prese è al momento un ambito attivo di ricerca, e in ogni caso modificare i modelli esistenti è quasi impossibile. La sfida è quella di creare algoritmi trasparenti sin dalla progettazione, per rispettare un altro limite fondamentale posto dal GDPR, il principio della *"privacy by design"* che obbliga a rendere conformi prodotti e processi sin dalla fase di progettazione.

L'altra faccia della medaglia è ovviamente il rischio di soffocare un settore innovativo e di rendere l'Europa meno competitiva. L'approccio UE alla regolamentazione potrebbe soffocare l'innovazione, spostando gli incentivi verso la non-adozione di tecnologie innovative o l'adozione di versioni "auto-limitate" delle stesse, con effetti pesanti anche sulla competitività dell'Europa rispetto alle altre aree del mondo. L'asticella posta dal GDPR all'uso dell'IA "pratica" è veramente molto alta, a volte più alta di quella degli stessi decisori umani, che non sono tenuti a giustificare sempre il loro processo cognitivo. Se riusciremo a conciliare i due aspetti però gli Europei potrebbero sviluppare un enorme vantaggio tecnologico.

Alessandro Guarino
CEO, StAG S.r.l. e convenor del CEN/CENELEC JTC13/WG5 "Privacy and data protection"