Etica e Governance dell’intelligenza Artificiale

Date : 5 febbraio 2018

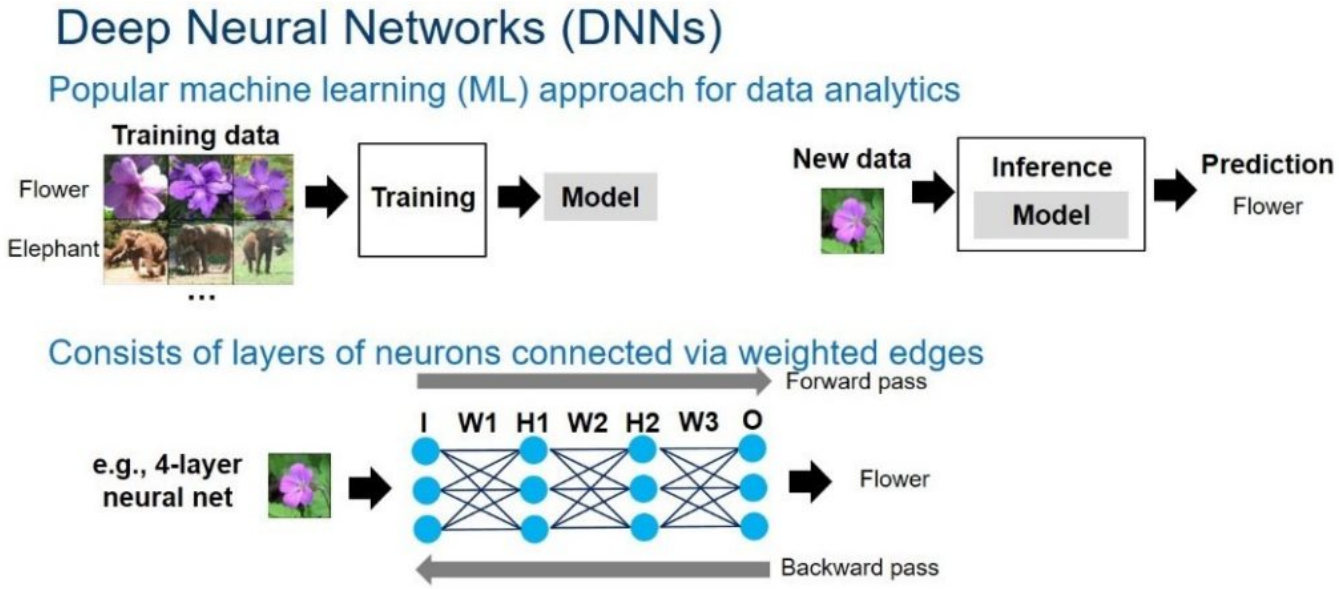
Uno dei mali della nostra epoca è la mancanza di lavoro e l’uso eccessivo, talvolta “abuso”, delle tecnologie informatiche. Nel primo decennio del nuovo millennio siamo passati dai sistemi gestionali e di automazione locali ai sistemi *web based* che hanno aperto la strada per lo sviluppo di applicazioni in molteplici campi: mobile, medicina, automazione, ricerca e servizi *Front End* di marketing e pubblica amministrazione. Tutti servizi che, per funzionare correttamente, avevano bisogno di dati: pertinenti e non eccessivi. Per tali motivi il legislatore era già corso ai ripari con la legge sulla privacy 196/2003 e poi con il regolamento europeo 679/2016. Tuttavia, nell’ultimo decennio la corsa all’accumulo dei *Big data*, necessari per l’erogazione di determinati servizi e per attività di marketing, ha messo in serio dubbio gli sforzi del legislatore nel normare un settore in continua evoluzione.

L’accumulo di “Big data”

Ho già scritto sulla pericolosità dell’accumulo indiscriminato di dati in grandi database (*Big data*), che da qualche tempo sono oggetto di commercio a cavallo di un confine tra lecito e illecito, cessione e raccolta consensuale secondo i dettami della legge in materia di *privacy* o carpiti in modo illegale. *Big data* è tuttavia il termine usato per descrivere una raccolta di dati in grandi database e l’analisi di tali dati (*data analytics)* richiede strumenti sempre più potenti, come l’intelligenza artificiale e metodi analitici specifici per l’estrazione di valore. La raccolta dei dati è fatta da aziende specializzate che rivendono alla propria clientela le banche dati corredate, il più delle volte, da specifiche analisi di mercato. I clienti, nella fattispecie, sono banche, aziende private e pubbliche, società di assicurazioni e istituti di ricerca. La raccolta dei dati non sempre è chiara e trasparente e le fonti sono spesso non evidenziate. Con l’avvento di internet e del fenomeno dei social la quantità di dati personali rilasciati dagli utenti è enorme: dati personali, immagini e video concorrono alla costruzione di grandi database, con o “senza” il consenso degli utenti. E’ recente, infatti, l’ultimatum della comunità europea nei confronti di WhatsApp e Facebook per la condivisione dei dati.

Data analytics e Intelligenza Artificiale

Come già accennato i *data analytics* sono piattaforme applicative che utilizzano tecniche d'intelligenza artificiale (IA), apprendimento automatico (*machine learning*) e analisi predittiva in molti settori, in particolare nel marketing, per individuare con maggior precisione le modalità più idonee ed efficaci del rapporto cliente/fornitore. In particolare la *machine learning* è quella branca dell'intelligenza artificiale che riguarda lo studio, la costruzione e l'implementazione di algoritmi che permettono ai sistemi di elaborazione, sui quali sono implementati, di imparare e fare previsioni in modo automatico, iniziando da un insieme di dati in ingresso e costruendo modelli previsionali che prevedono la riduzione degli errori alla fine di ogni processo di apprendimento. Branca affine e di grande interesse del *machine learning* è invece il *deep learning* (apprendimento profondo o apprendimento approfondito), in particolare di *feature learning*, supervisionato o meno, che caratterizza i processi di reti neurali artificiali su larga scala che possono contenere milioni di neuroni simulati, in genere dotate di due o più strati e capaci di processare informazioni in modo non-lineare. **Il *deep learning, in altri termini,* è quindi un insieme di algoritmi e tecniche statistiche che permettono di individuare pattern, modelli, schemi ricorrenti, in un insieme di dati non organizzati**. Di queste tipologie di reti le più comuni sono chiamate *convolutional neural networks* (CNNs) o *recurrent neural networks* (RNNs). Queste reti neurali imparano attraverso l'uso di dati di addestramento e algoritmi di backpropagation. I campi di applicazione riguardano molti settori come quelli della sicurezza, robotica, medicina, mobilità, eGov, ricerca e molto altro. Per esempio, utilizzando le tecniche di *Deep Learning* è possibile riconoscere un viso in una fotografia (strumento già utilizzato da Facebook per suggerire tag in un'immagine), un'immagine rilevata da una telecamera, oppure individuare degli ostacoli lungo un percorso stradale (come fanno molte *driverless car*, veicoli senza conducente attualmente in fase di sperimentazione).



IA e privacy

L'utilizzo nella raccolta dati dell'intelligenza artificiale consente il censimento e l'elaborazione dati di grandi volumi (*Big data*) per finalità molteplici che non hanno paragone con il passato. Oggi ogni interazione con i sistemi informativi che abbiamo nella quotidianità genera la raccolta di dati: scelte di navigazione su motori di ricerca, acquisti on line, like e post sui social, caricamento e condivisione di video e immagini sui social network. Tutte situazioni nelle quali i dati vengono in parte "forniti" dall'utente e, in parte, generati automaticamente dalle applicazioni dei fornitori di servizi che rilevano anche l'IP utente e talvolta l'utenza social.

Con l'impiego di strumenti dell'IA, in particolare della *machine e deep learning,* questi dati vengono processati già durante l'attività di acquisizione e raccolti con modalità diverse in database che non sempre rispecchiano le finalità per cui sono stati raccolti. Spesso le *form* di raccolta dei dati "eccedono" nella richiesta dei dati necessari all'espletamento del servizio, chiedendo talvolta l'attivazione di *flag,* non obbligatori*,* riguardanti i gusti, la politica, religione e lo stato di salute dell'utente. Certo, raramente richieste esplicite, ma velate di "opinione". Il tutto in quel sottile confine tra l'opinare e l'essere presocratico.

Tuttavia, dal punto di vista della privacy, la tutela dei dati personali viene dettata da norme nazionali (decreto legislativo n.196/2003) e da disposizioni comunitarie. Si tratta nella fattispecie di norme che trovano applicazione anche quando il trattamento dei dati personali viene realizzato attraverso l'acquisizione mediante sistemi di IA. La normativa comunitaria è stata recentemente aggiornata con il nuovo regolamento per la protezione dei dati personali (n.2016/679). Esso, che pure non contiene alcun evidente riferimento all'IA, enuncia alcuni principi e regole che appaiono concepite soprattutto per i sistemi informativi che di questa si avvalgono. E' chiaro tuttavia che la sola regolamentazione appare insufficiente senza la responsabilità ed una buona etica da parte di chi tratta i dati.

IA e Etica

In quasi tutte le professioni, ordinistiche e non, l'etica è il principio che tutela chi professa e il suo interlocutore. Certo la legge ci dice cosa possiamo fare, ma l'etica ci dice cosa dovremmo fare. Non abbiamo tuttavia la certezza che allo stesso modo l'etica appartenga anche alle categorie commerciali dove non ci sono molte adozioni esplicite di regolamenti etici nelle singole attività commerciali, ma piuttosto il semplice "istinto" di convenienza per sè e per il cliente. E ciò non può essere a tutela del cliente. Infatti, a frenare le frodi commerciali sono le leggi, non l'etica.

Nel campo dell'IA la capacità di autoapprendimento (machine e deep learning) delle macchine o robot è ad uno stato avanzato che porterà prima della fine del terzo decennio ad un'alta capacità di autoapprendimento di macchine, robot e sistemi.

Nel 1942 Isaac Asimov postulava le tre leggi della robotica:

1. Un robot non può recar danno a un essere umano né può permettere che, a causa del proprio mancato intervento, un essere umano riceva danno;
2. Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non contravvengano alla Prima Legge;
3. Un robot deve proteggere la propria esistenza, purché questa autodifesa non contrasti con la Prima e con la Seconda Legge.

E' di qualche anno fa, invece, l'allarme lanciato da oltre 400 scienziati firmatari del manifesto *Research Priorities for Robust and Beneficial Artificial Intelligence* ("Le priorità della ricerca per una robusta e benefica Intelligenza artificiale"). Voci che se da un lato invitano ad un uso benefico dell'intelligenza artificiale, dall'altro ammoniscono sui possibili effetti negativi dell'IA. Tra le voci critiche, ma anche invitanti ad un uso eticamente compatibile dell'IA, Stephen Hawking, Elon Musk, Nick Bostrom e James Harrat .

Oggi la grande scommessa dei ricercatori è sull'algoritmo etico che renderà in futuro l'uso della IA compatibile e benefica per l'uomo. Tuttavia l'algoritmo etico è solo il punto di arrivo di attività multidisciplinari per un'etica della scienza dei dati.

IA, sicurezza e amministrazione pubblica

I processi decisionali nella pubblica amministrazione avranno in futuro sempre più bisogno di utilizzare l'IA per migliorare la qualità dei processi decisionali che non dipendano solo dalla governance politica. L'IA potrà essere utilizzata nei servizi di *Front End* con i cittadini e per ottimizzare i flussi documentali di *Back End* nelle AOO degli enti locali. Allo stesso modo l'IA potrà occuparsi della sicurezza del sistema informativo. E' tuttavia inutile precisare che un buon utilizzo dell'IA dipende anche dalla riorganizzazione dei processi interni di un ente che potrà ottimizzare, con l'aiuto dell'IA, il numero dei procedimenti già in fase di Front End.

Processi decisionali eticamente complessi riguardano invece i settori della salute e della

giustizia in cui l’utilizzo dell’IA dovrà passare attraverso la certificazione di algoritmi etici, supportati da attività multidisciplinari riguardanti l’etica della scienza dei dati.

Bibliografia

- **Agrillo, A.,** (1994), La rete unitaria della pubblica amministrazione, Torino, Elea Press;
- **Melindo, F.**, (1991), Tecnologie di elaborazione e intelligenza artificiale nelle Telecomunicazioni, Edizioni CSELT;
- **Marsland, S**., (2015), Machine Learning: An Algorithmic Perspective, CRC Press
- **Duchesnay, E., Löfstedt, T**., (2017), Statistics and Machine Learning in Python;
- **Zinoviev D**., (2016), Data Science con Python, Apogeo
- **Cencetti C**., (2014), Cybersecurity: Unione europea e Italia: Prospettive a confronto, Roma, Ed. Nuova Cultura

A cura di: **Agostino Agrillo**