GDPR, machine learning per migliorare la privacy ma algoritmi poco trasparenti

Venerdì scorso, 25 maggio, è entrato ufficialmente in vigore il nuovo **regolamento generale sulla protezione dei dati** voluto dall'Unione europea. Detto anche **GDPR**, dall'acronimo dell'inglese di *General Data Protection Regulation*, il provvedimento è un atto unico nel suo genere e presto o tardi tutte le organizzazioni a livello globale, che avranno modo di trattare i dati personali di cittadini/consumatori europei, dovranno averci a che fare.

Il GDPR inizia così il suo lungo viaggio in giro per il mondo e non certo per raccogliere ovunque consensi, perché le imprese dovranno affrontare delle spese e non pochi cambiamenti nel loro modo di gestire la ***privacy*** degli utenti.

Sta di fatto che ora, i dati personali dei cittadini europei andranno trattati in un certo modo e molto probabilmente il GDPR potrebbe anche essere preso a standard per sviluppare modelli più omogenei in ogni parte del pianeta.

D'altronde, la diffusione inarrestabile degli oggetti intelligenti (*smart objects*) e connessi in rete (***internet of things***), calcolati in circa 8 miliardi già oggi, e la metà della popolazione mondiale che accede regolarmente a internet, pongono la questione della *privacy* al centro delle agende di tutti i Governi e anche delle imprese.

In questo scenario, le tecnologie di ***machine learning*** (ML),

cioè di apprendimento automatico, potrebbero tornare utili nel rafforzamento delle difese della *privacy*. Secondo la testata Telecompaper, tali soluzioni consentirebbero di proteggere i nostri dati senza esporre a possibili violazioni e sottrazioni le informazioni più sensibili e le *personally identifiable information* (PII), cioè tutti quei dati che possono sfruttati per identificare in maniera univoca un utente all'interno di un sito web o di una piattaforma (ad esempio dalla combinazione di nome e cognome assegnati ad un indirizzo IP in combinazione con l'indirizzo fisico del soggetto).

I modelli ML possono così esaminare una grande mole di dati in tempo praticamente reale. Grazie ad essi e agli algoritmi utilizzati è possibile rilevare modelli specifici di comportamento, anomalie e tendenze generali.

I processi necessitano di una minima supervisione umana, adeguandosi facilmente al GDPR, che premia quelle organizzazioni che riducono al minimo l'attenzione degli esseri umani ai dati.

Il problema è che il *machine learning* va alimentato con una grande quantità di dati (***big data***), che gli sono offerti dall'automazione crescente e dall'internet delle cose. *"I big data sono una cosa, la protezione dei dati un'altra*", ha affermato la professoressa **Lilian Edwards** della University of Strathclyde di Glasgow.

L'apprendimento automatico che poi sta alla base dell'intelligenza artificiale (*artificial intelligence*, **AI**), comporta l'impiego costante di algoritmi, che riescono a migliorare sé stessi "*abbuffandosi di dati*": "*più dati consumano ed elaborano, più facilmente indovinano i modelli*

giusti”.

Ad esempio, uno di quei modelli che permettono ad una macchina a guida autonoma di riconoscere gli oggetti, le persone, gli ostacoli sulla strada.

Si tratta per l’appunto di modelli/schemi di comportamento del veicolo frutto del lavoro dell’apprendimento automatico.

I big data possono essere una minaccia al GDPR nel momento in cui la conservazione dei dati è approssimativa e presenta troppe “*falle*”: “*si mettono in discussione le nozioni di trasparenza e fiducia. Diventa subito opaca la gestione dei dati e scarsa la trasparenza degli obiettivi. Per rendere un algoritmo trasparente si deve riuscire a capire come si raggiunge una determinata decisione, che tipo di strategie sono state adottate, ma questo non sembra sia semplice da ottenere dalle aziende proprietarie* ”.

The post GDPR, machine learning per migliorare la privacy ma algoritmi poco trasparenti appeared first on Key4biz.

https://www.key4biz.it/gdpr-machine-learning-per-migliorare-la-privacy-ma-algoritmi-poco-trasparenti/222516/