L'evoluzione normativa tra privacy e Intelligenza Artificiale

Autore: Giancarlo Butti

Ritorniamo[1] dopo oltre un anno ad affrontare il tema di privacy ed IA (si veda in proposito il n. 2/2017 di Cybersecurity trends). L'occasione è la recente pubblicazione (25 gennaio 2019 a Strasburgo) da parte del **Comitato consultivo (cd. t-pd) della convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (convenzione 108) delle Linee-guida in materia di intelligenza artificiale[2] e protezione dei dati.**

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9096716

Si tratta di un passo importante che si colloca in un percorso che aveva visto a ottobre 2018 le Autorità Garanti privacy mondiali emettere un documento dal titolo molto significativo: **Declaration on ethics and data protection in artificial intelligence.**

Tale documento[3] è stato adeguatamente sintetizzato dall'Autorità Garante italiana[4] nei seguenti punti:

- sviluppare le applicazioni di IA secondo un principio di correttezza, garantendo che vengano utilizzate soltanto per facilitare lo sviluppo umano senza ostacolarlo o minarlo
- responsabilizzare tutti i soggetti coinvolti, attivando forme di vigilanza continua e definendo processi verificabili di governance dell'IA
- migliorare la trasparenza e l'intelligibilità dei sistemi di IA
- permettere un effettivo "controllo umano"
- sviluppare le applicazioni di IA secondo principi di privacy-by-design e di privacy-by-default.

Già in precedenza specifiche Autorità Garanti avevano emesso pubblicazioni su questo tema.

In particolare **ICO** (Autorità garante inglese) ha pubblicato: **Big data, artificial intelligence, machine learning and data** ed il **CNIL** (Autorità garante francese): **Comment permettre à l'homme de garder la man?**

Le pubblicazioni esprimono preoccupazioni in merito all'uso dell'IA, in particolare riguardo alla scarsa trasparenza degli algoritmi e alla loro possibile manipolazione, e propongono dei suggerimenti su come realizzare applicazioni che garantiscano una maggior trasparenza e un maggior coinvolgimento degli utenti.

Al riguardo le **Linee guida** recitano:

11.Gli interessati dovrebbero essere informati se interagiscono con un'applicazione IA e hanno il diritto di ottenere informazioni sulla logica alla base dei trattamenti di dati che li coinvolgono. Le informazioni da fornire dovrebbero comprendere le conseguenze derivanti dall'applicazione di tale logica.

Anche nel caso in cui siano fornite adeguate informazioni, si pone il problema di capire se le stesse siano veritiere, e quindi uno dei temi evidenziati dai documenti di cui sopra è la possibilità di poter effettivamente verificare il comportamento di tali applicazioni, tramite un'attività di audit.

Attività questa tutt'altro che semplice e che richiede la disponibilità di competenze molto specializzate.

Anche il governo delle soluzioni di IA pone diversi problemi.

Come già espresso nel precedente articolo, il GDPR, nel suo articolo 22 **"Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione",** cerca di porre un freno quantomeno all'uso di profilazioni completamente automatizzate che abbiano conseguenze significative sugli individui.

Anche in questo caso ci sono tuttavia delle limitazioni. Da un lato, tale pratica è comunque consentita con il consenso del soggetto interessato o nell'ambito di un contratto (entrambe situazione dove la reale libertà di scelta dell'interessato è dubbia), dall'altra tale tutela riguarda unicamente le persone fisiche. Il GDPR introduce comunque delle misure correttive al possibile uso distorto dell'IA allorquando si presentino i casi prima citati (consenso dell'interessato o adempimenti contrattuali, autorizzazione di legge):

il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Il limite della reale tutela di questo articolo sta nella sua interpretabile applicabilità, che si limita a considerare i casi in cui la profilazione: *produca effetti giuridici che lo riguardano o che incida in modo analogo* ***significativamente*** *sulla sua persona.*

Sicuramente in tale fattispecie non si sarebbe portati a considerare l'inoltro mirato di semplici messaggi pubblicitari ad esempio ad una futura mamma, salvo poi essere contraddetti dalla missiva che Gillian Brockell ha indirizzato alle aziende che le inondavano di messaggi mirati per prodotti per bambini: *"se siete abbastanza intelligenti da rendervi conto che sono incinta siete sicuramente abbastanza intelligenti da rendervi conto che il mio bambino è morto".*

Appare evidente come la futura mamma fosse stata profilata in funzione della consultazione di siti dedicati a prodotti per neonati e in conseguenza di questo ricevesse pubblicità mirata.

Purtroppo i sistemi che hanno raccolto ed elaborato tali informazioni non hanno saputo cogliere un'altra importante informazione: l'assenza improvvisa di quelle ricerche cha hanno portato alla sua profilazione.

Certamente dopo la perdita del figlio, quella che poteva essere considerata una innocua e anche utile comunicazione, è diventata talmente spiacevole da spingerla alla comunicazione sopra riportata.

BIO

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo diversi ruoli: security manager, project manager ed auditor presso gruppi bancari; consulente in ambito sicurezza e privacy presso aziende dei più diversi settori e dimensioni.
Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, whitepaper, manuali tecnici, corsi, seminari, convegni. Svolge regolarmente corsi in ambito privacy, audit ICT e conformità presso ABI Formazione, CETIF, ITER, INFORMA BANCA, CONVENIA, CLUSIT, IKN, Università degli studi di Milano.
Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate tradizionali ed una decina on line. Ha pubblicato 21 fra libri e whitepaper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 9 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT…
È socio e proboviro di AIEA, socio del CLUSIT e di BCI.
Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity, Rischio Informatico e GDPR di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, GDPR, eidas, sicurezza dei pagamenti, SOC, di UNINFO sui profili professionali privacy, di ASSOGESTIONI sul GDPR…
È membro della faculty di ABI Formazione, del Comitato degli esperti per l'innovazione di OMAT360 e fra i coordinatori di www.europrivacy.info. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMCBI.

Questo sposta notevolmente la valutazione di cosa possa essere considerato *significativo*, e come, in casi analoghi a quello considerato, tale valutazione possa variare nel tempo, o meglio come non ci si possa limitare all'uso di sistemi di profilazione automatizzata, ma debba esistere un sistema complessivo di governo degli stessi, capace di gestire rapidamente casi come quello citato.

Anche la limitazione alle persone fisiche della tutela offerta dalla normativa suscita qualche perplessità; concedere o meno un fido ad un'azienda in base a scelte totalmente automatizzate non trova una mitigazione nel GDPR, che non si applica a tali soggetti, ma presenta gli stessi limiti e rischi che si hanno con le persone fisiche.

Non va inoltre dimenticato che un'azienda è comunque composta da persone fisiche e quindi, una decisione che può influenzare il futuro di un'azienda, impatta sicuramente su tali soggetti.

Anche in questo caso l'uso di sistemi automatizzati rende sicuramente più oggettiva la valutazione, (ovviamente se non sono stati introdotti ad arte criteri

discriminatori) e questo è sicuramente un grosso vantaggio per tutti; il problema può risiedere nella incapacità del sistema di cogliere aspetti nuovi o diversi rispetto a quelli che rappresentano il suo patrimonio di conoscenze. È lì che l'uomo prevale sui sistemi automatizzati e suggerisce che l'ottimo per creare un sistema che possa essere oggettivo, ma anche flessibile, richieda necessariamente la combinazione di uomo e macchina.

Anche nel caso della concessionaria di auto, che si è vista rifiutare la pubblicità da parte di un social network, (perché il suo nome è stato considerato offensivo dall'algoritmo che controlla i testi da pubblicare), il problema non è certo dell'algoritmo utilizzato (che ha fatto il suo dovere), quanto sul governo del processo. Sarebbe sufficiente la presenza di un operatore che possa raccogliere le osservazioni di soggetti coinvolti per migliorare la capacità di analisi del sistema e offrire un servizio di qualità.

Ma c'è un altro articolo del GDPR che impone l'uso di misure tutelanti per gli interessati; l'art. *Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, richiede*, più comunemente noto come privacy by design e by default.

È interessante notare che le **Linee guida** citate all'inizio si spingono oltre tale formulazione, e introducono il concetto di *"human rights by design"*, riferendosi alle cautele che gli sviluppatori di applicazioni di IA devono mettere in atto onde *evitare qualsiasi potenziale pregiudizio (bias), anche involontario o occulto, il rischio di discriminazione o altri effetti negativi sui diritti umani e le libertà fondamentali degli interessati.*

Tali rischi possono derivare, fra gli altri, dalle vulnerabilità intrinseche di qualunque applicazione software, alle quali però si aggiunge un ulteriore strato di vulnerabilità, costituito dagli algoritmi che già in fase di addestramento o successivamente possono essere a loro volta manipolati e indotti nell'errore. Da ultimo un cenno al problema della qualità dei dati utilizzati (molto spesso provenienti da fonti aperte) ad esempio per elaborare profili o per concedere un prestito.

Al riguardo la pubblicazione **Big data and privacy – Making ends meet della FPF (Future of Privacy Forum)** riporta il caso della signora Judy Thomas e dalla signora Judith Upton i cui profili creditizi sono stati scambiati in conseguenza della quasi perfetta coincidenza dei loro SSN, con le relative conseguenze. La pubblicazione indica che ben il 26% dei credit report analizzati contenevano errori. ■

1 Coautore con il prof. Lorenzo Schiavina di "Intelligenza artificiale esoftcomputing", FrancoAngeli, 2017
2 Il Consiglio d'Europa definisce l'IA come „Un insieme di scienze, teorie e tecniche il cui scopo è quello di riprodurre, attraverso la macchina, le capacità cognitive di un essere umano. Gli sviluppi attuali mirano, ad esempio, ad affidare a una macchina compiti complessi precedentemente delegati a un essere umano."
3 https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf
4 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9059156#4