Breve commento alla proposta di Regolamento UE sull'AI

La proposta di Regolamento da parte della UE sull'Intelligenza Artificiale del 21 aprile 2021, introduce in maniera molto forte i concetti di sistema e di governance.

Già dalle prime righe del documento si evince come l'argomento AI debba essere trattato in maniera trasversale e multi disciplinare.

Il sistema AI è quindi considerato attraverso un approccio olistico ed integrato.

Un approccio generale alla governance ed al suo controllo della AI ed ai rischi che questa comporta è già stato affrontato negli articoli: https://www.ictsecuritymagazine.com/articoli/modello-di-autovalutazione-relativo-a-un-sistema-di-intelligenza-artificiale/; https://www.ictsecuritymagazine.com/articoli/un-approccio-alla-governance-della-ai/; https://www.ictsecuritymagazine.com/articoli/ancora-sulla-governance-della-ai/ ai quali rimandiamo per completezza e correttezza.

In particolare si vuole evidenziare come i legislatori abbiano inteso la bozza di regolamento, ispirandosi probabilmente anche al GDPR, come documento relativo proprio ad un sistema di gestione.

In effetti, riportando solo alcuni degli 85 articoli presenti, l'art. 9 e l'art 17, che vengono anche richiamati negli allegati precisamente negli allegati VI e VII si introduce in maniera chiara il concetto di sistema e del suo controllo.

L'art. 9 pone il focus su un sistema di gestione dei rischi, in particolare riportando l'attenzione sugli incidenti (art-

62). Tale sistema di gestione richiama sia modelli che metodologie note, che contemplano il concetto di sistema, e che possono in qualche modo essere d'aiuto integrandosi con altri framework sono ad esempio: la ISO 31000, il CSF NIST e il NIST 800-53, la ISO 27005.

La gestione dei rischi diventa quindi una forzante per guidare il sistema AI, attraverso metodologie e prassi consolidate.

L'art. 12 richiama alcuni concetti fondamentali della ISO 27001 e del CSF NIST cioè la registrazione e la gestione degli eventi (log) che permettono il monitoraggio, la gestione del loro ciclo di vita dei rischi e la gestione della tracciabilità.

L'art. 15 tratta gli argomenti tipici della cybersecurity, della security by design comprese ad esempio: le metriche, la resilienza, la gestione dei back up.

L'art 17, invece richiama proprio il concetto di Sistema di Gestione della Qualità. In quest'ottica la norma ISO 9001 integrata con la norma ISO 27001, che rispettano entrambe la struttura HLS (Hight Level Structure) cioè la suddivisione nei capitoli: 4 Contesto, 5 Leadership, 6 Pianificazione, 7 supporto, 8 Attività Operative, 9 Monitoraggio e 10 Miglioramento (attraverso il concetto di Azioni Correttive dell'art. 21) , permettono il soddisfacimento dei requisiti elencati nell'art. 17, quali ad esempio: la redazione e diffusione delle Policy, delle procedure la realizzazione di test e di assessment, la gestione degli incidenti, la gestione delle risorse, la gestione della comunicazione, il ciclo di vita dei dati.

Non solo proprio collegandosi agli allegati, è fondamentale introdurre il concetto di controllo e misura (assessment) richiamato dalla norma ISO 19011 e dal controllo di conformità della ISO 37301 (artt. 19 e 43).

Un breve riassunto è riportato nella figura sottostante.

L’implementazione di standard internazionali riferiti a sistemi di gestione ed al loro monitoraggio e controllo integrati con una corretta analisi dei rischi ed altri requisiti (GDPR) permettono di gestire i progetti AI e la governance dei dati in maniera conforme e trasparente ed adeguata rispettando le regole e garantendone l’accountability.

Dunque i sistemi di AI ci hanno abituato alla possibilità di utilizzo nei più disparati ambiti e settori, evidenziando tanto le potenzialità, quanto le ricadute in termini di discriminazione, opacità, rischio, danno e responsabilità. In tal senso, la strategia europea (ma per molti versi estesa anche a livello mondiale) sta tentando di approcciare all’intricata materia tenendo in debito conto gli innumerevoli profili di esposizione, richiedendo – in primis – che tali sistemi presentino necessariamente sette requisiti fondamentali, quali: supervisione umana; robustezza tecnica e sicurezza; privacy, controllo e gestione dei dati; trasparenza; diversità, correttezza, assenza di discriminazione; benessere sociale e ambientale; responsabilità.

A ciò si somma la proposta di Regolamento che, prendendo le mosse dal GDPR, sembra presentarsi come un *upgrade* della normativa in tema di protezione dei dati personali, andando a richiamare alcuni concetti ormai consolidatisi (come le definizioni, il dovere di informativa, l’approccio risk based che fonda le radici nel principio di accountability, la documentazione dettagliata, i principi di sicurezza e accuratezza, il risk assessment, la DPIA, la notifica delle violazioni), ma introducendo anche profili di innovazione. Questi ultimi parrebbero maggiormente concentrati sulla tracciabilità dei risultati, sulla supervisione umana, sui concetti di fiducia ed eccellenza, sull’eliminazione dei bias

(i dataset non potranno incorporare alcun pregiudizio intenzionale o non intenzionale), sull'individuazione dei sistemi cd. "ad alto rischio" (quelli ritenuti a rischio inaccettabile saranno vietati[1]) e sul concetto di robustezza.

Quest'ultimo profilo, a dirla tutta, desta non poche preoccupazioni poiché sembrerebbe non essere declinato a seconda della tipologia di AI e dell'ambito di applicazione, ma identificato come requisito imprescindibile di alto livello da rispettarsi tout court.

Anche in punto di sanzioni la Proposta si discosta leggermente dal GDPR, introducendo sanzioni maggiori con un tetto massimo di 30 milioni di € o del 6% del fatturato globale annuo.

Per la dimostrazione della *compliance* al Regolamento si è pensato, inoltre, ad una dichiarazione di conformità mediante marchio europeo di qualità dell'AI, rilasciato dall'Autorità competente designata dal singolo Stato membro.

Sul punto, vi è da specificare che le AI verranno classificate – in base alla "pericolosità" – in 4 gruppi: 1) a rischio inaccettabile; 2) ad alto rischio; 3) a rischio limitato; 4) a rischio minimo.

Per determinare l'appartenenza al 2° gruppo, sarà necessario che il sistema sia un prodotto, o sia destinato a essere utilizzato come componente di sicurezza di un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione (Allegato II); e che il prodotto in questione sia sottoposto a una valutazione di conformità da parte di terzi.

Le AI ad alto rischio potranno comunque essere immesse sul mercato, ma solo ove presentino determinati requisiti, quali:

- Istituzione di un sistema di gestione del rischio
- data governance (formazione, validazione e test di dataset)

- Documentazione tecnica
- Registrazione degli eventi,
- Trasparenza
- Supervisione umana
- Robustezza, precisione e sicurezza.

Appare, comunque, evidente come l'uso dell'intelligenza artificiale venga letto come foriero di vantaggi competitivi per le aziende, in ottica di raggiungimento di risultati sociali e ambientali vantaggiosi (Considerando 1), e pertanto la Proposta punta a definire standard di sicurezza, affidabilità, accuratezza e qualità condivisi in grado di gettare le basi per un "mercato" europeo di fiducia ed eccellenza dei sistemi di AI.

Note

[1] Ad esempio: AI che utilizzino tecniche subliminali che vanno oltre la coscienza di una persona, al fine di distorcerne materialmente il comportamento in un modo tale da causare o da rendere probabile causare a tale persona o ad un'altra persona un danno fisico o psicologico, oppure sistemi che sfruttino una qualsiasi delle vulnerabilità di un gruppo specifico di persone a causa della loro età, disabilità fisica o mentale.

Articolo a cura di **Stefano Gorla e Anna Capoluongo**

Stefano Gorla è nato a Milano, si è laureato in fisica nucleare presso l'Università di Padova. Ha insegnato per qualche anno Matematica e Fisica presso alcuni licei.

Da anni si occupa di privacy e sicurezza dei dati attraverso un approccio sistemico e olistico.
Consulente e formatore in ambito sicurezza e tutela dei dati e delle informazioni e relatore in numerosi convegni.

Auditor ISO 27001, DPO Certificato FAC Certifica, NIST

Specialist Certificato Fac Certifica, Certificato COBIT5 ISACA, Master EQFM.
Ha maturato notevoli esperienze come Referente Privacy (DPO) e consulente in tali ambiti.
È autore di varie pubblicazioni sul tema.

Avvocato, esperta in Diritto delle Nuove Tecnologie, Privacy&Data Protection, Contrattualistica e Diritto civile. Partner presso lo Studio Capoluongo, DPO per Aziende in ambito sanitario, universitario e tecnologie dell'informatica, Docente a contratto Sigmund Freud University – campus di Milano e 24Ore Business School, Vicepresidente "Istituto di Ricerca per gli Studi Giuridici, Economici e Sociali", si occupa prevalentemente di consulenza societaria sia nazionale che internazionale ed è specializzata in new tech law, privacy&data protection, videosorveglianza, contrattualistica e responsabilità medica.

https://www.ictsecuritymagazine.com/articoli/breve-commento-alla-proposta-di-regolamento-ue-sullai/