IX Commissione (Trasporti, poste e telecomunicazioni) e X Commissione (Attività produttive, commercio e turismo) della Camera dei deputati

ciclo di audizioni informali sulla "Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione"

1. DEFINIZIONE

Il primo punto che solleviamo è formale e si riferisce a cosa intendiamo con "intelligenza artificiale". Si tratta forse dell'aspetto più importante in assoluto su cui si stanno concentrando i negoziati europei, dato che l'intera applicabilità e portata del Regolamento ovviamente dipenderà da cosa verrà incluso o escluso in questa definizione. Il dibattito è molto attuale perché alcuni Stati membri stanno chiedendo una riduzione della portata dell'attuale definizione, indicata all'**articolo 3(1)** e specificata nell'**allegato 1**. Al momento la Commissione considera tra le tecniche l' apprendimento automatico (supervisionato e non supervisionato) ma anche i motori inferenziali e deduttivi, ed altri approcci statistici.

Il Consiglio europeo, in rappresentanza degli Stati membri, ha chiesto di ridurre la definizione alle sole applicazioni più avanzate di apprendimento automatico (quindi non supervisionato), o *machine learning.* La preoccupazione degli Stati deriva dall'idea che la definizione attuale considererebbe troppe tecniche come IA, includendole quindi potenzialmente nei sistemi considerati ad alto rischio. Ricordiamo, infatti, che l'approccio del presente Regolamento è *risk-based*, e che le disposizioni si riferiscono e applicano principalmente alle applicazioni di IA considerate "ad alto rischio". Per questo motivo, siamo convinti che né gli Stati né i settori produttivi debbano preoccuparsi nè della definizione nè del contenuto di questo Regolamento, che fornisce tutti i presupposti per poter innovare, ma in sicurezza e rispettando i diritti. È giusto che un sistema considerato ad alto rischio dall'Europa sia sottoposto a controlli più puntuali, dato l'enorme potenziale impatto che queste applicazioni hanno sulla vita delle persone.
Noi crediamo che una definizione ridotta rispetto a quella già proposta nel Regolamento limiterebbe drasticamente il suo campo di applicazione ed escluderebbe molti sistemi che già hanno conseguenze gravi per i diritti fondamentali delle persone.

Un esempio utile a comprendere sia questo punto che il successivo è quello dei **Paesi Bassi**, dove nel gennaio del 2021 il governo è stato coinvolto nel *Toeslagenaffaire*, lo scandalo dei sussidi per l'infanzia. Si tratta del primo episodio europeo di discriminazione di massa basata sui dati, di cui il governo è responsabile e che ha portato il premier a dimettersi poco dopo a causa della portata dello scandalo. Nell'arco di 10 anni, l'autorità fiscale e i ministeri avevano utilizzato un software automatizzato, il SyRI, per controllare a quali famiglie veniva concesso un sussidio per la crescita dei figli e verificare che non ci fossero casi di frode. Nel corso degli anni il software ha discriminato e accusato ingiustamente oltre 45.000 famiglie eseguendo una correlazione automatica tra il possesso della doppia cittadinanza e il rischio di frode. Dopo aver individuato che alcune famiglie con doppia cittadinanza erano a rischio di frode, il software ha applicato la correlazione a tutte le famiglie, le cui vite sono state rovinate (alle persone accusate di frode, negli anni, era stato richiesto di restituire i sussidi) senza neanche conoscerne il motivo: il governo olandese, infatti, non è stato in grado di motivare le decisioni del software, salvo poi essere condannato dalla Corte dell'Aja per violazione del GDPR e dei diritti fondamentali:
https://www.privacy-network.it/scandalo-welfare-olandese-colpa-di-un-algoritmo/

Non si trattava in questo caso di un software chissà quanto sofisticato: riducendo la definizione di IA così come chiesto da alcuni Stati, un algoritmo come quello usato nei Paesi Bassi rimarrebbe escluso dallo scopo del Regolamento, come molti altri importanti algoritmi "*rule-based*" che stanno causando danni in tutto il mondo. Pensiamo quindi sia il minimo, considerata la portata di questi strumenti, includerli e quindi mantenere la definizione attuale del testo. Anche tecniche relativamente semplici possono portare a cortocircuiti pericolosi, se mancano i doverosi controlli umani: i risultati delle decisioni automatizzate hanno a che fare con il modo in cui vengono gestite, più che con la tecnica utilizzata.

2. SORVEGLIANZA BIOMETRICA

La normativa europea (Reg. 2016/679 e Dir. 2016/680) già prevede alcuni limiti e tutele per le persone nel contesto della sorveglianza biometrica. **Per trattare dati biometrici (come quelli necessari al riconoscimento facciale) c'è oggi bisogno di una legge specifica** in grado di prevedere specifiche garanzie per la salvaguardia dei diritti e libertà delle persone. Il Regolamento sull'Intelligenza Artificiale prevederà ulteriori limiti sostanziali a questa attività, che viene ritenuta intrinsecamente ad alto rischio. Tra questi ricordiamo in particolare la necessità di rispettare limiti temporali e geografici della sorveglianza biometrica. In pratica, queste attività dovrebbero essere contenute sia nel tempo che nello spazio, data la loro estrema invasività nella vita privata delle persone. Purtroppo deve notarsi che in Italia in questi ultimi anni abbiamo assistito ad una esponenziale proliferazione di sistemi di videosorveglianza, spesso anche attraverso telecamere di ultima generazione già predisposte per la videosorveglianza biometrica. Queste telecamere vengono installate, accese e utilizzate in modo continuativo e senza alcun contingentamento temporale. Questo, unitamente all'accessibilità delle nuove tecnologie e alla maggiore certezza giuridica del Regolamento, potrebbe scatenare una vera e propria corsa alla videosorveglianza biometrica nei Comuni italiani, tale da creare in poco tempo una rete nazionale di sorveglianza inevitabile. Un tale scenario è a nostro avviso assolutamente da scongiurare. La natura di questi sistemi di sorveglianza trasforma e ribalta il rapporto di potere tra Stato e cittadini: ognuno di noi sarebbe soggetto a una sorveglianza sistematica e perenne; talmente invasiva e intensa da trasformare ogni cittadino in un potenziale sospetto; un codice a barre pedinabile virtualmente in tempo reale in ogni luogo e tempo.

Inoltre, va menzionata la sostanziale fallibilità di questi sistemi, che hanno elevati tassi di errore che variano in base all'angolazione del viso, alle condizioni di luce, all'altezza della telecamera, alla copertura parziale del viso della persona. A questo devono aggiungersi gli errori di riconoscimento di persone che esulano dall'archetipo di persona (uomo, bianco) con cui solitamente vengono allenati gli algoritmi di riconoscimento facciale. Il riconoscimento errato, a partire da un database di sospetti, potrebbe avere conseguenze giuridiche e impatti sia economici che psicologici molto gravi sulla vita di una persona.

Per tutti questi motivi chiediamo primariamente di prevedere un divieto assoluto, più stringente di quanto previsto dal Regolamento, di questi sistemi - al fine di tutelare i principi costituzionali dei cittadini italiani, che non dovrebbero essere sottoposti a sorveglianza diretta e pervasiva senza gravi indizi di reato.
In caso contrario, chiediamo comunque di prevedere specifici e stringenti limiti temporali, geografici e quantitativi sull'uso di questi strumenti in Italia, preferibilmente evitando strumentazione fissa e permanente, anche nel rispetto del Regolamento, che prevede la liceità dell'uso di questi sistemi soltanto per il perseguimento di determinati scopi, che quindi devono essere specifici e determinati di volta in volta, e non certo vaghe e generiche finalità di "sicurezza pubblica".

3. REGISTRI PUBBLICI E TRASPARENZA

A tutto questo è collegato un altro aspetto fondamentale: quello della trasparenza. L'esempio gravissimo dei Paesi Bassi è frutto di una totale assenza di trasparenza nei confronti dei cittadini. Il Regolamento, all'art. 52, richiederà obbligatoriamente a tutte le autorità nazionali di indicare in un *database* europeo i sistemi ad alto rischio impiegati in ogni Stato. Quello che noi suggeriamo è di cogliere l'occasione per predisporre un registro pubblico italiano di intelligenza artificiale, a cui Privacy Network sta già lavorando con un osservatorio sull'automazione nella PA: https://www.privacy-network.it/osservatorio/

4. BIAS E QUALITÀ DEI DATASET

L'**articolo 8** si riferisce alla qualità dei set di dati usati per allenare le applicazioni di IA, perché da questi dati dipendono molto i risultati degli output e delle decisioni automatizzate.
L'articolo richiede che i dati utilizzati per addestrare i modelli siano di alta **qualità**, **robusti**, **privi di bias** e che non producano effetti prevedibilmente indesiderati. Il Regolamento quindi sta identificando i dati come **unica fonte di potenziali problemi** che possono causare dei bias nei risultati, il che è fuorviante perché come dimostrato e sostenuto da molti esperti i bias possono emergere anche dalle scelte progettuali e di design. Pensiamo sia necessario estendere il controllo ad altri aspetti del sistema, e quindi considerare il cruciale ruolo umano tenendo conto che le scelte su quali dati utilizzare sono inevitabilmente sociali e politiche, perché riflettono particolari interessi che in un dato momento decidono di estrarre un certo modello da quei dati. A maggior ragione se il Regolamento richiede in molti casi solamente un'auto-valutazione di conformità, è necessario che le richieste di qualità siano più precise.

5. AUTORITÀ

Infine, ultimo punto e chiudo, sarebbe importante iniziare a chiederci a chi spetterà in Italia il compito di far rispettare disposizioni e divieti indicati dal Regolamento, e quindi quale sarà l'autorità che governerà l'intelligenza artificiale. È un nodo determinante, dal momento che deciderà quanto e come applicare le regole previste. Ogni Paese dovrà indicare «una o più autorità nazionali competenti».

Gli scenari quindi sono essenzialmente due: decidere di creare una nuova autorità a cui affidare la governance dell'IA o dotare un'autorità esistente delle risorse necessarie per potersene occupare. Entrambe le scelte hanno dei pro e dei contro, ma l'aspetto cruciale è che il testo attuale non specifica che le autorità competenti debbano essere indipendenti, come invece era specificato nel GDPR. Pensiamo sia necessario specificare l'indipendenza di questa autorità, così come hanno già fatto notare i garanti europei per la protezione dei dati.

Milano, 14.02.2022

Diletta Huyskes
Responsabile Advocacy e Consiglio direttivo

PRIVACY NETWORK