Se il database di Clearview AI mette a rischio la privacy...

Più di 20 miliardi di immagini e volti, sono queste le dimensioni del database di Clearview AI, azienda statunitense che è stata coinvolta in inchieste sull'abuso e l'appropriazione indebita di file per addestrare il proprio software di riconoscimento facciale. La grande mole di dati è stata accumulata tramite un processo di web scraping, letteralmente «raschiatura del web», e proviene da diverse fonti, da social network, siti di broadcasting, blog e qualsiasi sito che possa contenere immagini. Durante il mese di maggio l'azienda ha fatto parlare di sé a seguito di due condanne, una in Italia ed una nel Regno Unito, volte alla cancellazione dai database dell'azienda di un enorme quantitativo di dati relativi ai cittadini dei due stati, con una conseguente multa di quasi 30 milioni di euro. L'azienda, già nota per diversi articoli di denuncia pubblicati dal New York Times, è stata citata anche per l'utilizzo del software di riconoscimento facciale in collaborazione con le forze dell'ordine, azione illecita perpetrata negli ultimi anni in molteplici stati.
Il caso Clearview sembra però essere solo la punta dell'iceberg: se tramite un processo di web scraping è semplice entrare in possesso di enormi quantità di immagini e dati sensibili, non è altrettanto facile identificare e localizzare chi opera simili raccolte e non sempre è possibile risalire ad un'azienda. Alla minaccia sempre maggiore di appropriazione indebita dei dati e delle immagini personali si aggiunge una progressiva diffusione di software di manipolazione di immagini e creazione di deepfake, che potrebbe rendere ancora più complesso il rapporto tra i dati e il loro proprietario.
Risulta dunque sempre più importante avere una legislazione che regoli e protegga la privacy e i dati personali, come il Gdpr europeo a cui ha fatto riferimento l'Italia contro Clearview IA. A questa è necessario aggiungere, da parte dell'utenza di internet, una presa di coscienza dei rischi di una diffusione incontrollata di dati ed immagini e lo sviluppo di una maggiore consapevolezza riguardo le concessioni che si rilasciano quotidianamente online.

Jasmine MILONE

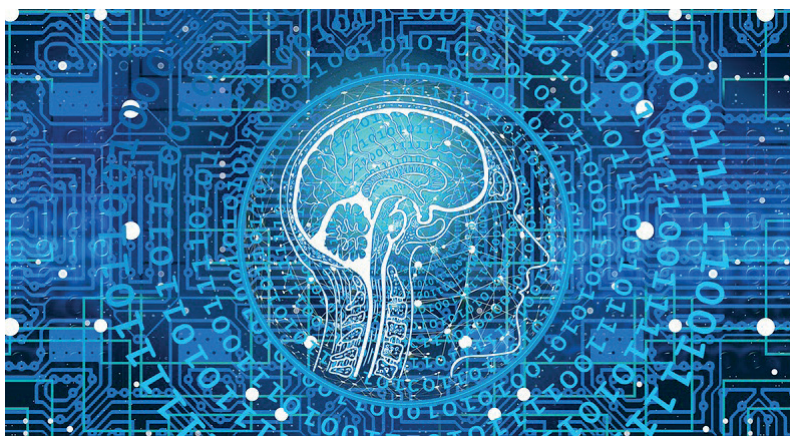
APOSTOLATO DIGITALE

condividere codici di salvezza

ARTIFICIAL INTELLIGENCE ACT – IL REGOLAMENTO EUROPEO SU CRITERI E DIRITTI

Intelligenza artificiale in Europa: 4 problemi, ma anche 4 soluzioni

L'obiettivo di questo documento è contribuire a creare una «IA affidabile» che bilanci proporzionalmente l'interesse sociale per l'innovazione e una migliore fornitura da parte dell'IA di servizi pubblici, con gli impatti negativi sui diritti fondamentali e sui valori sociali».



Fondamentale è l'incipit di questo recente studio, effettuato dall'Ada Lovelace Institute: «Non ci concentriamo sui tipi di tecnologie che vogliamo costruire, ma sui tipi di società che vogliamo costruire».
Questo breve studio, dal titolo «Regolamentazione dell'IA in Europa: quattro problemi e quattro soluzioni», vuole partire dal presupposto di «considerare come costruire, sviluppare - o forse rifiutare - questo modello, prima che diventi radicato». Si evidenzia come, l'Artificial Intelligence Act sia di per sé un ottimo punto di partenza per un approccio olistico alla regolamentazione dell'IA, pur tuttavia senza rappresentare un solido traino per il resto del mondo!
Ci sono diverse questioni aperte che questo documento analizza.
Primo punto: l'Intelligenza Artificiale non è un prodotto né un servizio «una tantum», ma un sistema erogato dinamicamente attraverso più mani («il ciclo di vita dell'IA») in contesti diversi con impatti diversi su vari individui e gruppi. La legge trae ispirazione dalla legislazione esistente sulla sicurezza dei prodotti e concepisce in gran parte i «fornitori» di Intelligenza Artificiale come l'equivalente dei produttori di prodotti del mondo reale come per esempio i giocattoli. Ma qui parliamo invece di un qualcosa di dinamico, in continua evoluzione che proprio per questa ragione richiede un monitoraggio ed una valutazione continua. Valutare in modo olistico il rischio di un tale sistema in astratto è impossibile. Tradurre questa complessa rete di attori, dati, modelli e servizi in un regime giuridico che attribuisca doveri e diritti a determinati attori identificabili è estremamente difficile. Nell'AI Act, la responsabilità primaria è, per analogia con i fabbricanti di beni fisici, posta su una duplice figura di «deployer»: la legge non si assume il lavoro, che è certamente difficile, di determinare quale dovrebbe essere la distribuzione della responsabilità esclusiva e congiunta contestualmente lungo tutto il ciclo di vita dell'IA, per proteggere i diritti fondamentali degli utenti finali nel modo più pratico e completo.
Inoltre i cosiddetti Training data, quasi sempre, sono appannaggio delle Big Tech, esonerando, in tal guisa, fornitori di tecnologia come Amazon, Google e Microsoft, il cui coinvolgimento nella certificazione dell'IA come sicura, è vitale, poiché hanno un controllo effettivo sull'infrastruttura tecnica, sui dati e sui modelli di formazione, nonché sulle risorse e potere di modificarli e testarli.
Secondo punto: quelli interessati dai sistemi di Intelligenza Artificiale, siano essi utenti finali, interessati o consumatori, non hanno diritti e quasi nessun ruolo nell'AI Act. Ciò è incompatibile con uno strumento la cui funzione è quella di salvaguardare i diritti fondamentali.
Derivando il disegno dell'AI Act principalmente dalla sicurezza dei prodotti e non da altri strumenti, il ruolo degli utenti finali dei sistemi di IA come soggetti di diritti, non solo come oggetti impattati, è stato oscurato e la loro dignità umana è stata trascurata.
Si auspica qui la creazione di una figura super partes, una sorta di difensore civico che potrebbe non solo ricevere e far avanzare i reclami degli utenti ma, su base europea, raggrupparli, individuare i modelli di reclamo e eventualmente istruire o aiutare le autorità di regolamentazione o la società civile a intraprendere azioni rappresentative!
Terzo punto. La presunta natura «basata sul rischio» della legge AI ACT, è illusoria e arbitraria. È necessaria un'autentica valutazione del rischio basata su criteri verificabili. Le tassonomie su sistemi ad alto o basso rischio sono talmente generiche e poco approfondite da non rappresentare, secondo questo studio, una garanzia di difesa dei diritti fondamentali delle persone. Quarto punto: la legge manca di una valutazione generale del rischio dei diritti fondamentali. E qui si pongono due domande fondamentali:
La prima: «Quali criteri dovremmo utilizzare per certificare la sicurezza dei sistemi di IA nella società?» È sufficiente certificare la conformità ai diritti fondamentali del tipo tutelato dalla Carta dell'Ue e dalla Convenzione europea dei diritti dell'uomo?
La seconda: «Se possiamo essere d'accordo su questi criteri, dovrebbero essere certificati prima che il sistema sia immesso sul mercato o nella società (valutazione 'ex ante') o dopo che sono stati spenti e hanno avuto un impatto (valutazione 'post factum' o audit); o una combinazione di entrambi?».
Stante una certa arbitrarietà del controllo ex ante e un aggravio notevole di costi per uno ex post, si suggerisce qui di prendere in considerazione seriamente di incentivare una valutazione d'impatto algoritmica (Aia - Algorithmic impact assessment).
Le soluzioni proposte sono pertanto: La legge sull'IA dovrebbe essere riformulata per fornire un'adeguata sorveglianza dei sistemi IA di uso generale da parte di fornitori e deployers; La partecipazione di coloro che sono colpiti dai sistemi automatizzati nella loro progettazione e salvaguardia deve essere consentita, con la dovuta considerazione delle loro opinioni. Certamente diventa indispensabile una terzietà, ovvero un organismo terzo in grado di fare da ponte tra segnalazioni o reclami degli utenti e responsabilizzazione dei produttori e sviluppatori.

Raffaella AGHEMO
avvocato

Metaverso e Blockchain cosa significano?
Un breve viaggio tra le parole più difficili del digitale a cura del progetto «Parole ostili».

«REPAIR» – PARTE DA FRAMMENTI

L'algoritmo salva anche i reperti

Ogni scavo archeologico può produrre anche diverse decine di migliaia di frammenti di opere che devono essere analizzati e, per quanto possibile riuniti per ricomporre l'oggetto originale. Il processo è da sempre molto difficoltoso, se non impossibile, a causa dell'ampia superficie delle opere, del numero e delle dimensioni spesso minuscole dei frammenti che dovranno essere riuniti, molte volte mancanti, non coincidenti o confusi tra altri frammenti di opere diverse, e della complessità del processo di ricostruzione. «Repair», sigla di Reconstructing the past: Artificial Intelligence and Robotics meet Cultural Heritage, sfrutta l'intelligenza artificiale per scannerizzare tridimensionalmente tramite fotogrammetria, analizzare, catalogare e ricollocare digitalmente nella posizione originale le migliaia di frammenti di diversi

affreschi antichi provenienti da differenti siti di scavo, per poi, tramite un sistema robotico guidato dalla stessa IA, andare ad operare sui frammenti stessi, ricomponendo l'affresco originale e riducendo al minimo il rischio di danneggiare ulteriormente i reperti. Il progetto, che fa parte del programma europeo Horizon 2020 e che coinvolge a capo del progetto l'Università Ca' Foscari Venezia ed il professor Marcello Pelillo, esperto di intelligenza artificiale, oltre ad un consorzio internazionale di università tra Italia, Israele, Germania e Portogallo, è attualmente attivo nel Parco Archeologico di Pompei, in cui sono conservati l'affresco della Casa dei Pittori al lavoro e l'affresco della Schola Armatorarum.
Il primo, distrutto durante l'eruzione del Vesuvio nel 79 d.C. ed ulteriormente danneggiato dai bombardamenti della Seconda Guerra Mondiale è situato nell'insula dei Casti Amanti e risulta la sfida più complessa per il progetto, in quanto manca un'immagine di riferimento antecedente alla sua distruzione, per quanto riguarda il secondo invece, si tratta di un progetto di più facile attuazione, infatti l'opera crollata nel 2010 e già parzialmente ricostruita.

Emanuele DENTIS