AI Act, punti certi e nodi ancora da sciogliere

Nella tarda serata di venerdì 8 dicembre è stato finalmente raggiunto un accordo sull'attesissimo Artificial Intelligence ACT (AI Act), un momento epocale in ambito giuridico (e non solo) in quanto parliamo della prima normativa al mondo nata con l'obiettivo di disciplinare l'intelligenza artificiale. In poche ore, Internet è stata invasa da informazioni ed opinioni più o meno fondate sull'AI Act, motivo per cui è opportuno cercare di fare sintesi e ordine con un taglio pragmatico, distinguendo informazioni certe, da quelle non certe.

CERTO: AI Act è un regolamento

Sembra banale, ma sotto il punto di vista giuridico è fondamentale inquadrare l'AI Act nel modo corretto. La scelta di utilizzare un regolamento, in luogo di una direttiva è frutto di una strategia ben precisa che affonda le sue radici nel GDPR che potremmo considerare quasi un pilastro fondante di questa normativa sull'intelligenza artificiale. Scegliere un regolamento significa decidere di sottoporre l'intera UE ad una medesima normativa, senza possibilità per gli stati di intervenire (e di interferire) in questo processo di regolamentazione. Se l'UE avesse scelto una direttiva, avrebbe difatti obbligato gli stati membri a emanare un atto (legge) di recepimento, aprendo le porte a variabili incalcolabili. Ogni stato avrebbe avuto la sua normativa e questo non era certo l'obiettivo del legislatore europeo. Certo, come accadde per il GDPR, anche per l'AI Act gli stati potranno/dovranno intervenire con norme di "assestamento" (ricordate il Decreto 101 del 2018?), ma il faro da seguire in modo pedissequo sarà

il regolamento, non potendosi gli stati discostare in alcun modo da esso.

NON CERTO: il testo

Allo stato attuale, benché in molti siano corsi a commentare la norma, NESSUNO ha avuto modo di leggere il suo testo. Probabilmente, nemmeno Brando Benifei, relatore dell'AI Act. Questo significa che le informazioni che circolano debbono essere prese con le pinze. Sappiamo del resto tutti che la lettura e l'interpretazione di una norma, spesso dipende da una parola e da una virgola scritta in un certo modo piuttosto che un altro. Dobbiamo tutti porre una certa cautela nella lettura di articoli o nell'ascolto di commenti da qui sino alla pubblicazione del testo definitivo.

CERTO: l'iter non è finito

Trapattoni, noto allenatore di calcio, avrebbe invitato a "non dire quattro se non ce l'hai nel sacco" (la sua variante è più spinta, ma ci siamo capiti). Il punto è che l'iter dell'AI Act non è finito. Certo, i passaggi che mancano sono una pura formalità, ma ad oggi, come dicevamo sopra, non esiste un testo definitivo. Il Consiglio d'Europa definisce l'accordo dell'8 dicembre come un "accordo provvisorio", fornendoci una chiara idea di come qualcosa potrebbe andare ancora storto. È una possibilità molto remota, ma esiste. Dopo l'accordo provvisorio, nelle prossime settimane si continuerà a lavorare a livello tecnico per finalizzare i dettagli del nuovo regolamento. Una volta conclusi i lavori, la presidenza sottoporrà il testo di compromesso all'approvazione dei rappresentanti degli Stati membri (Coreper). L'intero testo dovrà infine essere confermato da entrambe le istituzioni e sottoposto a revisione giuridico-linguistica prima dell'adozione formale da parte dei colegislatori.

CERTO: applicabilità AI Act in 2 anni

L’applicazione dell’AI Act sarà soggetta ad un meccanismo simile a quello del GDPR: pubblicazione a breve ed effettiva applicazione dopo 24 mesi. Questo principio generale conoscerà però una deroga: i divieti assoluti, difatti, entreranno pienamente in vigore già tra 6 mesi. Non solo, le società, con molta probabilità, da qui ai prossimi 2 anni potranno godere di una sorta di “bollino di pre assesment”, potendo dichiararsi conformi all’AI Act anche prima del termine dei due anni. A parere di chi scrive, qualora confermati questi termini, e nonostante l’idea del “bollino di pre assessment”, il rischio è che la scelta di attendere due anni possa trasformare l’AI Act in una norma vecchia ancora prima di entrare in vigore. Si tratta di un grosso errore che non può che dare ragione a chi ha fino all’ultimo spinto per far naufragare l’AI Act. In un mondo che nel giro

di un anno è stato invaso da Chat GPT rendendolo uno strumento indispensabile, è impossibile calcolare cosa accadrà in questi 2 anni, rischiando seriamente di arrivare troppo tardi, troppo scomposti. Era meglio una scelta più coraggiosa, fornendo 6 mesi o al massimo un anno per adeguarsi.

CERTO: i limiti del riconoscimento biometrico

Numerose fonti attendibili (anche gli stessi politici) hanno dato una certezza: il riconoscimento biometrico è stato vietato… più o meno. Già perché sono previsti tre casi in cui il riconoscimento biometrico in real time potrà essere utilizzato: evidente pericolo terrorismo; ricerca di vittime; persecuzione di seri crimini. Sarà interessante leggere il testo definitivo per capire se queste condizioni sono state meglio circostanziate in quanto, da questo semplice elenco, si

apre un varco così ampio che ci potrebbe entrare di tutto. La stessa nozione di “seri crimini” è così generica e soggettiva da frenare anche il migliore degli ottimisti. Cos’è un crimine serio? Cos’è un pericolo di terrorismo? Un giornalista/divulgatore che usa i social per raccontare le barbarie della guerra a Gaza è qualcuno che incita al terrorismo? Un giudice che manifesta contro il governo è un serio crimine? Il figlio di un politico che stupra una ragazza? Il figlio di un politico di altra fazione che fa

la stessa cosa? Chi decide cosa è un serio crimine? Dove c’è soggettività c’è pericolo e, parlando di sistemi di questo tipo, il pericolo di controllo (o di abusi) è molto alto, senza considerare che, in ogni caso, volendo pensar male, nessuno sa se davvero i sistemi in real time saranno accesi o spenti, anche al netto dell’obbligo di notifica alla Autorità di Controllo che pare essere obbligatorio. Vedremo.

CERTO: altri sistemi di controllo

Si è letto che Brando Benifei, relatore del testo, ha confermato il divieto di sistemi atti a riconoscere le emozioni. Anche qui sarà importante capire in quale misura. Vale per PA e privati o solo per uno di essi? Altri divieti poi sono confermati da Benifei, come la polizia predittiva, il social scoring e il riconoscimento biometrico. Tuttavia, come immaginabile anche questi divieti conoscono eccezioni potendo essere usati per analisi di dati anonimi e non finalizzati ad indagare su un determinato individuo. A tal riguardo, considerata la potenza di calcolo dei sistemi in questione, dovrebbe essere spontaneo chiedersi: esiste davvero la possibilità di considerare anonimo un dato agli occhi di queste AI?

NON CERTO: utilizzo di sistemi non sicuri

In alcuni siti specializzati1 si legge: “In exceptional circumstances related to public security, law enforcement authorities might employ a high-risk system that has not passed the conformity assessment procedure requesting judicialauthorisation”. Ove confermata, si tratterebbe di una scelta molto pericolosa in quanto darebbe alle nazioni la possibilità di giocare un jolly utilizzando sistemi non collaudati e/o non conformi, magari anche viziati da bias. Una disparità o “double standard” come va di moda dire ora, tra stato e cittadini che, francamente, non si può ritenere accettabile dal punto di vista giuridico e di tutela dei diritti umani.

CERTO: Esclusione per usi militari

Uno dei punti che, sin dalla prima lettura della prima bozza dell’AI Act, ci ha lasciati perplessi è stato quello che prevede l’esclusione dell’applicabilità dell’AI Act ai sistemi utilizzati esclusivamente per scopi militari o di difesa. Ad avviso di chi scrive, una simile esclusione può trovare senso in un sistema giuridico solo laddove si preveda di escludere tale area dall’AI Act per riservarvi una normativa ad hoc, come avvenuto nel caso del GDPR con i trattamenti effettuati dalle forze di polizia a cui è stata dedicata una norma a parte, ma contestuale. Il timore, però, è che non avendo alcuna notizia a riguardo, si corra il rischio di una semplice esclusione tout court, lasciando l’ambito militare totalmente scoperto. Si consideri a riguardo che già oggi l’AI è utilizzata nelle due guerre che più attirano l’attenzione mediatica (Ucraina e Gaza), esponendo migliaia di persone a decisioni di sistemi automatizzati, con tutta probabilità colmi di bias. Del resto, come spesso accade è proprio il settore militare a sperimentare maggiormente e senza

particolari cautele, mettendo in questo caso ancora più in pericolo (se possibile) le vite di esseri umani. Cedere all'assunto che "in amore e in guerra tutto è lecito" risulta quantomeno da sprovveduti. Le vite umane sono vite umane; tanto in momento di pace quanto in momento di guerra e come tali vanno tutelate.

Alla luce di tutto quanto sopra evidenziato, è chiaro che i punti da chiarire sono ancora molti. Avremo quindi cura di seguire gli sviluppi.

Fonte:
https://www.euractiv.com/section/artificial-intelligence/news/european-union-squares-the-circle-on-the-worlds-first-ai-rulebook/

https://www.key4biz.it/ai-act-punti-certi-e-nodi-ancora-da-sciogliere/471479/