

APPROFONDIMENTI

AI ACT e GDPR, tra opacità algoritmica e principio di trasparenza

Ottobre 2024

Luca Tufarelli, Partner & Founder, Ristuccia Tufarelli & Partners
Maria Lilia La Porta, Senior Associate, Ristuccia Tufarelli & Partners
Gaia Leoncini, Ristuccia Tufarelli & Partners



Luca Tufarelli, Partner & Founder,
Ristuccia Tufarelli & Partners

Maria Lilia La Porta, Senior Associate,
Ristuccia Tufarelli & Partners

Gaia Leoncini, Ristuccia Tufarelli &
Partners

➤ **Luca Tufarelli**

L'avvocato Luca Tufarelli, Partner e socio fondatore dello studio, ha conoscenze specifiche nei campi del diritto civile, commerciale, amministrativo e del diritto dell'informatica dove assiste sia soggetti privati che pubblici. Ha contribuito alla realizzazione di progetti speciali nei settori delle tecnologie innovative, delle telecomunicazioni, della informatizzazione della PA e del commercio elettronico occupandosi anche degli aspetti consumeristici e di compliance regolamentare (privacy, tutela del mercato e vigilanza delle comunicazioni).

Studio associato

Ristuccia Tufarelli & Partners



1. Il problema della opacità algoritmica

Negli ultimi anni si è assistito a un rapido sviluppo e a una crescente implementazione dell'intelligenza artificiale in diversi processi e settori produttivi. L' *Artificial Intelligence Index Report 2023*¹ redatto dalla Stanford University ha rivelato come l'intelligenza artificiale sia oramai il nuovo trend di sviluppo tecnologico tanto che negli ultimi due anni sono state rilasciate dai grandi player del mercato IT varie "piattaforme" di intelligenza artificiale generaliste basate per lo più su Large Language Model. Sono quindi sorte le prime controversie in materia di modalità di utilizzo degli strumenti di AI causate anche da alcuni incidenti legati all'utilizzo di questi strumenti.

L'intelligenza artificiale comporta il potenziale verificarsi di diversi rischi significativi, tra cui spicca il problema dell'opacità algoritmica, che si riferisce alla difficoltà di comprendere come vengano prese le decisioni all'interno di algoritmi complessi, rendendo poco trasparenti i processi decisionali.

Una delle maggiori difficoltà che si riscontra trattando di sistemi AI è infatti quella di conoscere tutte le informazioni rilevanti e relative al funzionamento del sistema: non è sempre possibile spiegare perché un modello abbia generato un particolare risultato o decisione e quale combinazione di fattori di input vi abbia contribuito.

Gli algoritmi, in particolare quelli sviluppati attraverso tecniche di machine learning, operano spesso come "scatole nere" (black box), il che significa che, mentre il modello può fornire previsioni o risultati, il processo attraverso cui giunge a tali conclusioni è spesso poco trasparente. Questo avviene perché tali algoritmi, analizzando grandi quantità di dati, imparano a fare previsioni o a prendere decisioni senza essere esplicitamente programmati per ogni singolo compito. Anche se i dati in ingresso e le decisioni in uscita sono visibili, i passaggi intermedi e le logiche decisionali rimangono oscuri, persino per gli stessi sviluppatori.

L'opacità algoritmica ha implicazioni etiche e legali significative. Il problema è che anche la macchina

¹ https://aiindex.stanford.edu/wp-content/uploads/2023/04/HALAI-Index-Report_2023.pdf

è fallibile e quando le decisioni automatizzate hanno un impatto sulle vite delle persone - ad esempio, nelle assunzioni, nei prestiti bancari o nelle sentenze giudiziarie - la mancanza di trasparenza può dare luogo a decisioni discriminatorie a causa di *bias* decisionali. Accade non di rado che i c.d. dati di addestramento (ossia i dati a cui ricorrono gli algoritmi di intelligenza artificiale per assumere decisioni) siano essi stessi discriminatori. Senza una comprensione chiara di come vengono prese le decisioni, diventa difficile contestarle, il che mina la fiducia degli utenti nei sistemi automatizzati, nonché nelle istituzioni che li utilizzano, specialmente in settori critici come la sanità, la finanza o il diritto.

In questo scenario, si sente - sia a livello europeo che nazionale - la necessità dell'intervento della trasparenza quale soluzione al nodo dell'opacità tecnologica dell'algoritmo dell'AI. La trasparenza è vista come l'unico elemento che possa consentire la realizzazione di soluzioni tecnologiche in grado di creare fiducia e benessere sociale.

L'obiettivo di una piena trasparenza algoritmica - intesa come totale ripercorribilità e intelligibilità dei processi digitali - si compie nel momento in cui l'algoritmo che conduce l'AI alla decisione automatizzata sia conoscibile al cittadino e realizzi la conoscibilità algoritmica. E ancora, si esprime nel diritto del cittadino a conoscere la cd logica algoritmica, ossia l'iter logico sulla base del quale è stata presa quella decisione.

Tale obiettivo è raggiungibile mediante la creazione di regole preventive che rendano l'AI affidabile e, quindi, una tecnologia al servizio della intelligenza umana senza che si sostituisca a questa. Si è quindi resa necessaria una regolamentazione che prevedesse nel dettaglio come progettare e sviluppare in modo trasparente, etico e responsabile i sistemi di IA.

Prima del Regolamento sull'Intelligenza artificiale, sebbene il GDPR fornisse alcuni strumenti sotto il profilo della protezione dei dati personali (cfr. par. 3), non esisteva una norma che affrontava direttamente le sfide specifiche legate all'interpretabilità degli algoritmi.

Nell'ambito dell'azione della Pubblica Amministrazione, la giurisprudenza amministrativa ha iniziato a trattare il problema della mancanza di trasparenza del procedimento amministrativo, sollevando inter-

rogativi cruciali su come le decisioni automatizzate influenzino i diritti dei cittadini e incentivando una maggiore responsabilità e trasparenza.

2. L'opacità algoritmica nel diritto amministrativo

Il Giudice amministrativo ha iniziato a trattare il problema di garantire la conoscibilità delle decisioni alla base degli algoritmi e il Consiglio di Stato, in particolare, si è espresso sul tema in numerose sentenze.

Il Consiglio di Stato si è dapprima pronunciato affermando che la decisione algoritmica debba essere conoscibile in ogni aspetto e pienamente sindacabile da parte del giudice amministrativo, sia con riferimento al profilo "procedimentale" della correttezza del processo di costruzione e gestione dell'algoritmo (come viene costruito, come vengono inseriti i dati, chi sceglie i dati), sia con riferimento a quello "intrinseco" sulla logicità e sulla ragionevolezza della decisione (sentenza Cons. Stato, sez. VI, 8 aprile 2019, n. 2270). Ciò al fine di poter verificare che gli esiti del procedimento automatizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare - e conseguentemente sindacabili - le modalità e le regole in base alle quali esso è stato impostato.

Il Consiglio di Stato ha successivamente affermato che la legittimità dell'azione amministrativa è assicurata dalla piena conoscibilità del codice sorgente utilizzato e dei criteri applicati e ha riconosciuto l'imputabilità della decisione all'organo titolare del potere, il quale deve poter verificare la logicità e legittimità della scelta e degli esiti (sentenza Cons. Stato del 13 dicembre 2019 n. 8472).

Infine, il Consiglio di Stato si è pronunciato affermando il principio secondo il quale, per contrastare l'opacità dell'algoritmo, occorre garantire la piena trasparenza algoritmica - intesa come totale ripercorribilità e intelligibilità dei processi digitali - rendendo l'algoritmo che conduce alla decisione automatizzata conoscibile al soggetto interessato. In particolare, la trasparenza intesa quale "conoscibilità dell'algoritmo" "deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutati-

va e decisionale e dei dati selezionati come rilevanti” (Cons. Stato, sez. V, 4 febbraio 2020 n. 881).

I principi giurisprudenziali sin qui riportati hanno di recente trovato collocazione nel nuovo codice dei contratti pubblici (Cfr. art. 30, d.lgs. 36/2023), in cui il legislatore delegato ha introdotto le leggi della legalità algoritmica, così come elaborate dalla giurisprudenza amministrativa, incentivando il ricorso da parte delle Amministrazioni all'utilizzo di procedure automatizzate (con specifico riguardo all'intero "ciclo di vita" dell'appalto) in una prospettiva di efficienza e semplificazione dell'attività amministrativa.

Sul punto, si è espresso anche il TAR Lazio, ammettendo *“la piena accessibilità ai sensi della legge n. 241 del 1990”* al funzionamento dell'algoritmo, in quanto *“la descrizione delle modalità di funzionamento dell'algoritmo assicura una conoscenza assolutamente non paragonabile a quella che deriverebbe dalla acquisizione del richiesto linguaggio sorgente”* (sentenza TAR Lazio n. 3769 del 22 marzo 2017). Il Tar ha affermato, in altri termini, che deve essere consentito direttamente l'accesso all'espressione algoritmica per assicurare una piena tutela. In una successiva pronuncia, il TAR Lazio ha ammesso l'accesso all'intero codice sorgente del software utilizzato per la selezione, affermando che solo esso permette di conoscere l'effettivo funzionamento del sistema informatico utilizzato (Sentenza TAR Lazio n. 7370/2020).

In conclusione, nell'ambito dell'azione della Pubblica Amministrazione, al fine di garantire trasparenza nel caso dell'utilizzo di algoritmi e sistemi automatizzati, nel rispetto altresì degli obblighi previsti dal Codice Trasparenza, la giurisprudenza ha esplicitato l'esigenza di permettere ai soggetti interessati di conoscere la c.d. logica algoritmica, ossia l'iter logico sulla base del quale è stata presa la decisione.

3. Il diritto alla spiegazione nel GDPR

Il suddetto principio di conoscibilità della logica algoritmica è, per altro, presente anche nel GDPR e si desume in diverse norme.

L'art. 22 del GDPR stabilisce un divieto generale di sottoporre l'interessato a decisioni totalmente automatizzate che producano effetti giuridici che lo riguardano o che incidano in modo analogo signifi-

cativamente sulla sua persona (es. il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani).

Le decisioni “basate unicamente” sul trattamento automatizzato a cui si riferisce l'art. 22 del GDPR, sono quelle in cui non vi è alcun coinvolgimento umano nel processo decisionale, o comunque quelle in cui l'intervento umano costituisce un semplice gesto simbolico. Quindi nel caso in cui vi sia un intervento umano, seppur nella fase finale del trattamento, che abbia un'influenza reale sull'esito della decisione, allora il trattamento è considerato ammissibile.

Le decisioni totalmente automatizzate, tuttavia, non sono vietate *tout court*. Tale divieto incontra delle eccezioni nei casi in cui la decisione sia: a) necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato o c) si basi sul consenso esplicito dell'interessato. Laddove si applichi una di queste eccezioni, il titolare del trattamento deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, tra cui almeno il diritto di ottenere l'intervento umano (art. 22 par. 3).

Sul tema, tra le misure che il titolare deve adottare nel caso in cui ponga in essere un trattamento di dati personali che dia luogo a una decisione totalmente automatizzata, il considerando 71 aggiunge il diritto dell'interessato di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la stessa.

Il diritto alla spiegazione nel GDPR si può ricavare da una lettura sistematica dell'art. 22 e del considerando 71, assieme agli artt. 13, par. 2, lett. f), art. 14, par. 2, lett. g) e art. 15, par. 1 lett. h).

Tali articoli infatti sanciscono il diritto dell'interessato di ottenere “informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato”.

Per “informazioni significative” si deve intendere quelle informazioni che sono utili per garantire traspa-

renza e leggibilità del processo decisionale automatizzato, mentre per “logica utilizzata” si intende la descrizione delle funzionalità del processo decisionale, l’architettura e la modalità di implementazione.

Tali informazioni dovrebbero essere fornite sia ex ante come obbligo di informazione preliminare dei titolari del trattamento (artt. 13 e 14), sia ex post su specifica richiesta dell’interessato (art. 15).

Sebbene il GDPR stabilisca questi principi, tale disciplina non è sufficiente ad affrontare il problema dell’opacità algoritmica. L’art. 22 infatti ha un ambito applicativo limitato: le decisioni basate unicamente sul trattamento automatizzato si riferiscono a un numero ridotto di casi, dato che basta anche un minimo di intervento umano per escluderne l’applicazione. Inoltre, è necessario il verificarsi di effetti giuridici significativi su un individuo, il che implica l’esclusione di tutti quei casi in cui questi effetti non siano rilevanti.

Occorre tenere conto altresì che il combinato disposto degli articoli sopra menzionati non è sufficiente ad affermare un vero e proprio diritto alla spiegazione sancito nel GDPR.

Tali considerazioni confermano la necessità di regole più dettagliate per la progettazione, lo sviluppo e l’utilizzo dei sistemi di IA che prevedano anche processi decisionali automatizzati in modo da garantire la comprensibilità e la trasparenza nei confronti dei soggetti interessati.

4. La trasparenza nell’AI Act

Il Regolamento (UE) 2024/1689 del 13 giugno 2024 che stabilisce regole armonizzate sull’Intelligenza Artificiale (“AI Act”) si propone di colmare le lacune normative esistenti, introducendo requisiti specifici per la trasparenza nell’uso dell’IA, al fine di costruire fiducia e responsabilità.

Nel fornire una definizione del principio di trasparenza, il regolamento richiama gli orientamenti etici per un’IA affidabile elaborati nel 2019 dall’AI HLEG indipendente nominato dalla Commissione Europea. La trasparenza è ricompresa nei sette principi etici tesi a garantire affidabilità ed eticità dei sistemi di IA ed è definita nel senso che i sistemi di IA devono essere sviluppati e utilizzati in modo da consentire

un’adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA nonché informando debitamente i deployer delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti (considerando 27).

Per affrontare le preoccupazioni legate all’opacità e alla complessità di alcuni sistemi di intelligenza artificiale e garantire la trasparenza, l’AI Act fornisce delle indicazioni e prescrive degli obblighi, che mettono in evidenza i seguenti aspetti fondamentali relativi alla trasparenza:

a) Trasparenza by design

L’AI Act prevede che la trasparenza sia garantita fin dalla fase di progettazione. I sistemi di IA, in particolare quelli ad alto rischio, devono infatti essere progettati in modo trasparente prima che siano immessi sul mercato o messi in servizio. Ciò consente al deployer di comprendere il funzionamento del sistema di IA, valutarne le funzionalità ed effettuare fin da subito la scelta corretta del sistema che intenda utilizzare (considerando 72).

Il fornitore del sistema dovrebbe altresì individuare le misure di sorveglianza umana adeguate prima dell’immissione del sistema sul mercato o della sua messa in servizio.

b) Comprensibilità/Spiegabilità

L’AI Act prevede che i sistemi di IA siano progettati e sviluppati in modo che il loro funzionamento sia sufficientemente trasparente per consentire ai deployer di interpretare l’output del sistema e utilizzarlo adeguatamente.

Al fine di affrontare il problema della comprensibilità algoritmica, i fornitori di un sistema di IA devono fornire spiegazioni tali da rendere ragionevolmente comprensibile ai soggetti interessati il funzionamento e i limiti del modello, sistema o servizio di IA fornito, nonché le modalità con cui è giunto ad una determinata decisione o risultato e il modo in cui tali decisioni o risultati debbano essere interpretati e possano essere correttamente utilizzati, descrivendo in maniera dettagliata tali informazioni in appo-

sita documentazione.

c) Accessibilità delle informazioni

I fornitori di sistemi di IA devono poter mettere a disposizione di tutti i soggetti interessati che ne facciano richiesta le informazioni necessarie per comprendere il funzionamento del modello, servizio o sistema di IA, con riguardo agli aspetti sia tecnici (ad es., funzionamento del modello algoritmico, parametri o variabili utilizzati nella progettazione del sistema di IA, le logiche utilizzate nel processo decisionale), sia agli aspetti di interazione uomo – macchina (ad es., il controllo e la validazione del soggetto fisico sul processo e i risultati del modello, servizio o sistema di IA), sia agli aspetti di conformità al quadro normativo applicabile.

A tal fine devono garantire che tutte le informazioni relative al modello, sistema o servizio di IA siano rese facilmente accessibili a tutti i soggetti interessati che ne facciano richiesta, o per ispezioni e audit, contribuendo a garantire responsabilità e conformità.

d) Sorveglianza umana

In linea con quanto previsto dal GDPR in merito al diritto a non essere sottoposti a decisioni basate unicamente su trattamenti automatizzati che producono effetti giuridici o che incidono significativamente sulle persone e il diritto di ottenere l'intervento umano (Considerando 71, art. 22), l'AI Act prevede altresì meccanismi di supervisione umana sui sistemi di AI. Infatti, i sistemi di IA ad alto rischio dovrebbero essere progettati e sviluppati in modo da consentire alle persone fisiche di sorvegliarne il funzionamento (considerando 73 e art. 14).

Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA.

La sorveglianza umana consente alle persone fisiche alle quali è affidata, tra le altre cose, di:

- comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese;
- interpretare correttamente l'output del sistema di IA, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili;
- comprendere se sia necessario non usare il sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga.

e) Esattezza dei dati

Al fine di garantire la comprensibilità delle decisioni prese dai sistemi di IA e assicurare la fiducia degli utenti, i set di dati utilizzati per l'addestramento, la convalida e la prova dei sistemi nonché per le finalità previste, devono essere di elevata qualità, pertinenti, sufficientemente rappresentativi, e possibilmente esenti da errori e completi (Considerando 67, 69, art. 10).

L'uso di dati esatti e pertinenti è cruciale per garantire la trasparenza nei sistemi di intelligenza artificiale.

Per disporre di set di dati di questo tipo e ottenere i migliori risultati dai sistemi di IA, è quindi essenziale attuare adeguate pratiche di governance e gestione dei dati, tenendo conto altresì della normativa sulla protezione dei dati personali. A tal riguardo, l'AI Act prevede che le pratiche di governance e gestione dei dati debbano includere la trasparenza anche in merito alla finalità originaria di raccolta dei dati.

f) Documentazione

L'AI Act prevede che siano documentate per iscritto tutte le politiche, procedure e istruzioni riguardanti ogni aspetto del ciclo di vita di un sistema di IA (Art. 17) e che tale documentazione contenga informa-

zioni significative, complete, accessibili e comprensibili (considerando 72).

I fornitori devono descrivere in apposita documentazione in maniera dettagliata, chiara e comprensibile l'architettura del modello, sistema o servizio di IA e le logiche del suo funzionamento, incluse, a titolo esemplificativo, le scelte di progettazione (quali parametri e variabili) e di sviluppo che hanno inciso o incidono sui processi decisionali, le modalità di analisi dei set di dati utilizzati per l'addestramento del modello di IA e dei set di dati utilizzati come input, i fattori chiave che hanno generato un determinato risultato e le modifiche che possono essere apportate ai dati di input per generare un risultato diverso, nonché ogni altra informazione tecnica o di altro tipo necessaria a spiegare in maniera quanto più esaustiva possibile il funzionamento del modello, sistema o servizio di IA. Il fornitore si impegna inoltre a motivare, tramite adeguata documentazione, le eventuali difficoltà tecniche che possono impedire o limitare la comprensibilità del funzionamento del modello, sistema o servizio di IA.

Tra questa documentazione sono ricomprese per esempio le istruzioni per l'uso, che devono essere fornite per ogni sistema di IA, in particolare per quelli ad alto rischio, e devono contenere informazioni pratiche, comprensibili e utili (considerando 72). Queste istruzioni devono:

- illustrare il funzionamento del sistema, dando spiegazioni su come il sistema esegue determinate operazioni e quali dati influenzano i risultati;
- definire usi previsti e vietati, chiarendo in quali contesti il sistema può essere utilizzato in modo appropriato e quali applicazioni sono sconsigliate o vietate;
- evidenziare le limitazioni, informando i deployer sui limiti del sistema e sui contesti in cui potrebbe non funzionare come previsto.

Inoltre l'art. 26, paragrafo 1 stabilisce che è necessario adottare misure tecniche e organizzative adeguate a garantire che l'uso di un sistema di IA sia conforme alle istruzioni per l'uso che accompagnano il sistema, anche per quanto riguarda la supervisione umana.

g) Mitigazione del rischio di bias e discriminazioni

La trasparenza è vista come uno strumento per identificare e mitigare i rischi, in particolare quelli legati a bias e discriminazioni. A riguardo, l'AI Act richiede che i sistemi siano progettati e testati per evitare bias e garantire decisioni giuste e imparziali. Pertanto, è previsto il divieto di utilizzo di sistemi di IA che comportano risultati discriminatori (Cfr. considerando 21, 27 e 31).

L'AI Act introduce poi obblighi di trasparenza specifici per determinati sistemi che possono comportare rischi di manipolazione, con particolare riferimento ai sistemi che: (i) interagiscono direttamente con gli esseri umani; (ii) sono utilizzati per riconoscere emozioni o stabilire una categorizzazione sulla base di dati biometrici; oppure (iii) generano o manipolano contenuti (art. 50).

Per prima cosa viene prescritto di sviluppare i sistemi che interagiscono direttamente con le persone fisiche in modo tale che queste siano informate della circostanza che stanno interagendo con un sistema di intelligenza artificiale (salvo che ciò sia già evidente) e di rendere noto se i contenuti mostrati sono stati artificialmente creati o manipolati.

Queste informazioni devono essere fornite in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione delle persone fisiche al sistema.

L'unica eccezione è rappresentata nei confronti di quei sistemi di IA autorizzati dalla legge per accertare, prevenire, indagare o perseguire reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato.

Accanto agli obblighi sin qui previsti, occorre considerare anche gli specifici e ulteriori obblighi di trasparenza già previsti nel GDPR verso gli interessati. L'AI Act sancisce infatti il rispetto delle normative sulla protezione dei dati personali (considerando 10 e 69).

Gli artt. 12-15 del GDPR prevedono l'obbligo del titolare del trattamento di fornire agli interessati tutte le informazioni relative ai trattamenti dei loro dati, specificando le finalità, i destinatari e i diritti degli

interessati. Questo processo di informazione deve essere chiaro e comprensibile, facilitando l'accesso e la comprensione da parte degli utenti. L'art. 12 prescrive infatti che l'informativa sia fornita in "forma concisa, trasparente, intelligibile e facilmente accessibile". Le informazioni devono essere altresì presentate in un linguaggio semplice, evitando termini tecnici che potrebbero confondere gli utenti.

Questa enfasi sulla chiarezza e sull'accessibilità è cruciale per garantire che gli individui possano fare scelte informate riguardo all'uso dei loro dati e alle tecnologie con cui interagiscono.

5. Conclusioni

In un contesto in cui l'intelligenza artificiale permea sempre più le nostre vite, affrontare il problema dell'opacità algoritmica diventa imprescindibile. La crescente diffusione di sistemi automatizzati, sebbene porti con sé vantaggi notevoli, solleva interrogativi critici riguardo alla trasparenza e alla responsabilità delle decisioni che prendono questi sistemi. È fondamentale che i cittadini possano accedere a informazioni chiare e comprensibili sui processi decisionali degli algoritmi, per poter esercitare i propri diritti e contestare eventuali decisioni che possano influenzare, anche significativamente, la loro vita quotidiana.

L'AI Act rappresenta un passo avanti importante per garantire che la progettazione e l'implementazione dei sistemi di intelligenza artificiale siano intrinsecamente trasparenti. Obblighi come la documentazione rigorosa, la spiegabilità delle decisioni e l'accesso ai dati utilizzati, sono misure chiave per mitigare i rischi di *bias* e discriminazione, oltre a costruire un clima di fiducia tra la tecnologia e la società.

La sinergia tra l'AI Act e il GDPR sottolinea l'importanza di un approccio normativo integrato e trasversale, volto a proteggere i diritti degli individui e a promuovere un utilizzo responsabile, etico e trasparente dell'intelligenza artificiale. Mentre il GDPR prevede misure per garantire la trasparenza dei dati personali, l'AI Act dispone che i sistemi di IA siano progettati e implementati in modo da essere comprensibili e giustificabili.

Affrontare l'opacità degli algoritmi e promuovere la trasparenza non è solo una questione di conformità

Studio associato

Ristuccia Tufarelli & Partners



normativa, ma è fondamentale per costruire fiducia e garantire che l'IA rimanga un alleato dell'intelligenza umana, rispettando i diritti e le aspettative degli interessati.

Solo così potremo evitare il rischio di una "tirannia algoritmica" e assicurarci che i sistemi di intelligenza artificiale contribuiscano al benessere collettivo, rispettando i diritti e le libertà fondamentali di tutti gli individui.



DB non solo
diritto
bancario

A NEW DIGITAL EXPERIENCE

 **dirittobancario.it**
