



Regione Toscana

Linee guida per l’adozione e per l’uso corretto e consapevole di soluzioni di intelligenza artificiale in Toscana

[LGAI_RT_#1]

Indice generale

1. Premesse: finalità e ambito soggettivo e oggettivo di applicazione.....	2
2. Contesto normativo di riferimento.....	4
2.1. Legge regionale n. 57/2024 (“ <i>Disciplina dell’innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla l.r. 54/2009</i> ”).....	5
3. Principi di base in materia di impiego dell’intelligenza artificiale.....	6
4. Aspetti Etici dell’Intelligenza Artificiale.....	7
5. Benefici dell’IA nella PA.....	7
6. Criteri per un uso responsabile dell’IA nella PA.....	8
7. AI ACT e Principi sulla Privacy e il Trattamento dei dati personali (GDPR).....	9
7.1. Trasparenza e sicurezza.....	11
8. Raccomandazioni e linee guida.....	11
8.1 Raccomandazioni generali.....	12
9. Conclusioni.....	14

1. Premesse: finalità e ambito soggettivo e oggettivo di applicazione

Il presente documento si propone di offrire un quadro di indirizzo generale, mediante una breve disamina introduttiva e organica relativa agli aspetti da attenzionare e alle tematiche focali per una corretta e progressiva introduzione di soluzioni di Intelligenza Artificiale (di seguito “IA”) a livello regionale.

Esso si inserisce in un contesto più ampio di documenti mirati a indirizzare gli utenti all’uso corretto e consapevole di soluzioni IA di prossima introduzione nel contesto regionale.

Nello specifico questo documento introduttivo vuole rappresentare un valido strumento di supporto e proporre indicazioni di carattere generale, in tanto mutuabili anche dagli Enti del territorio regionale, in quanto siano adattabili e perfettamente sovrapponibili al contesto di riferimento, riservando agli ulteriori documenti che lo affiancano, indicazioni e indirizzi più di dettaglio, in relazione agli specifici campi di applicazione, per un utilizzo responsabile delle soluzioni IA, garantendo una graduale introduzione delle stesse nel rispetto del principio di trasparenza e di tutela dei diritti fondamentali. Più in generale le linee guida si propongono di orientare al corretto utilizzo delle soluzioni IA, in prima battuta il personale dipendente di Regione Toscana, nonché, più in generale, gli enti e le PA presenti sul territorio toscano che vogliano prenderle a modello e adeguarvisi, con l’intento di fornire un livello adeguato di alfabetizzazione in materia di IA e di rafforzare le loro competenze e assicurarne un utilizzo trasparente, efficace ed eticamente corretto per lo svolgimento dell’attività amministrativa e della produzione normativa¹.

Con tale documento Regione Toscana intende adeguarsi progressivamente alla normativa europea e nazionale e fornire - sulla base del contesto di norme e linee guida attuali in materia² - indicazioni pratiche su come accompagnare l’adeguamento all’AI Act, che diventerà pienamente operativo nel corso dei prossimi anni. Questo documento inoltre implementa quanto previsto all’art. 8 comma 2 della Legge Regionale Toscana 57 – 2024 “*Disciplina dell’innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla l.r. 54/2009*”.

I lavori di redazione delle Linee guida sul consapevole e corretto utilizzo delle soluzioni di IA, in continuo aggiornamento ed ampliamento, seguono un’architettura che, sebbene improntata alla redazione di più documenti distinti tra loro, sotto il profilo del perimetro di applicazione (ambito oggettivo) e dei destinatari degli stessi (ambito soggettivo), segue una lettura interconnessa e armonizzata dei vari documenti che la compongono. Nello specifico esse si articolano, al momento, nei seguenti documenti che, seppur distinti, risultano complementari tra loro:

- 1) Il presente documento (LGAI_RT_#1), “**Linee guida per l’adozione e l’uso corretto e consapevole di strumenti di intelligenza artificiale in Toscana**” di portata generale, introduce e prende in disamina gli aspetti legati all’adozione (principi e temi) e all’utilizzo di soluzioni IA in Toscana. Tale documento offre una cornice generale di orientamento sul tema dell’IA prendendo in disamina i principi cardine che ne sovrintendono il corretto utilizzo (trasparenza, controllo e supervisione umana, non discriminazione algoritmica, *accountability*, illustrati in dettaglio nei paragrafi successivi) e i relativi profili critici da attenzionare. Esso, nello specifico, è destinato, in prima battuta, al personale dipendente di

¹ Pertanto, secondo il disegno sopra rappresentato, le presenti LG risultano astrattamente applicabili a tutti gli enti e organismi dell’amministrazione regionale, alle società partecipate regionali che erogano i servizi pubblici, nonché ai soggetti privati che, in base a convenzioni o contratti, utilizzino sistemi AI per conto della Regione.

² Bozze di Linee guida per l’adozione di IA nella Pubblica Amministrazione – AGID, febbraio 2025 (in fase di pubblicazione).

Regione Toscana ma si presta ad essere preso a riferimento, adattandolo al contesto specifico e apportando le necessarie modifiche, anche dagli altri Enti e PA presenti sul territorio toscano. Ad esso si affiancano i documenti più specifici che si richiamano di seguito;

- 2) Il secondo documento denominato “**Indicazioni operative per l’adozione di soluzioni di Intelligenza Artificiale in riferimento all’AI Act in Toscana**” (LGAI_RT_#2) ha carattere più specialistico rispetto al presente documento di carattere generale e si propone di offrire utili indicazioni sugli aspetti legati alla preventiva analisi d’impatto dei sistemi da adottare e alla verifica *ex post* di *compliance* degli stessi. Esso fornisce una serie di *checklist* e di allegati³ finalizzati a guidare gli “*adopters*” (utilizzatori e personale tecnico addetto al monitoraggio e all’implementazione dei sistemi di IA) nella redazione della documentazione fornita. Esso contiene, inoltre, due casi d’uso esemplificativi per guidare alla corretta compilazione dei documenti allegati.

Questo documento è indirizzato, in particolare, al personale tecnico e a tutti gli altri portatori di interesse chiamati a introdurre, monitorare, sviluppare e implementare gli applicativi e le soluzioni di IA.

- 3) 3) “**Prime indicazioni sull’utilizzo degli strumenti di Intelligenza Artificiale (IA) a supporto dell’attività lavorativa**” (LGAI_RT_#3), anch’esso si affianca agli altri documenti ed è indirizzato, *generaliter*, a tutto il personale dipendente dell’ente regionale ed è volto a fornire una serie di suggerimenti e prime indicazioni per un approccio adeguato all’utilizzo delle soluzioni di IA nello svolgimento del proprio lavoro. Questo documento è, dunque, orientato a supportare coloro che nello svolgimento dell’attività lavorativa si trovino a dover utilizzare applicativi o soluzioni di IA e a guidarli al corretto impiego degli stessi. Il documento rinvia inoltre, al catalogo generale degli applicativi IT già in uso in Regione Toscana, ai quali si affiancherà un’apposita sezione dedicata agli applicativi IA di prossima diffusione.

Si viene dunque a costituire un “*Kit di Adozione*” che Regione Toscana mette a disposizione per supportare il processo di adozione dell’IA che sta investendo i vari Enti e realtà regionali, indirizzato in primis all’Ente Regione Toscana. Beneficiari possono essere anche altri soggetti del territorio toscano, interessati a determinate componenti del *Kit*, di carattere più generale e flessibile, tali che potranno essere traslate ed applicate anche a realtà diverse.

Il *Kit* contiene:

- Linee Guida generali (LGAI_RT_#1), le indicazioni operative (LGAI_RT_#2), le prime indicazioni sul corretto utilizzo delle soluzioni di IA (LGAI_RT_#3) oltre ad ulteriori documenti di carattere settoriale e dedicati ai contesti specifici di adozione delle soluzioni IA, che si affiancheranno a quelli già esistenti all’interno della cornice tracciata dalle presenti Linee Guida (che sono pubblicate in forma di bozza per la condivisione con il territorio su partecipa.toscana.it e successivamente, una volta approvate, sui siti di Regione Toscana relativi alla Toscana);

³ Tra i quali si attenziona l’allegato denominato “**Considerazioni tecniche ed architetture su possibili implementazioni di IA**” volto ad inquadrare l’adozione dell’Intelligenza Artificiale in un Ente/Organizzazione dal punto di vista tecnico-architetture, partendo da esigenze concrete e fornendo possibili indicazioni di scenari di soluzione.

- Strumenti operativi come checklist di rischio, modelli di impact assessment e template per la stesura della documentazione (inseriti nei documenti di Linee Guida più tecnici o comunque ad essi allegati).

Il Kit verrà via via esteso con ulteriori documenti a supporto, venendo così a comporre un corpus documentale che recepisce e declina sul territorio regionale lo AI Act europeo, le norme italiane in materia di IA e le linee guida nazionali da parte di AGID.

2. Contesto normativo di riferimento

Le presenti linee guida si inseriscono in un contesto di interventi, a livello nazionale ed europeo, in tema di digitalizzazione, utilizzo dell’IA e garanzia della sicurezza cibernetica.

In particolare il Regolamento (UE) 2024/1689, *AI Act*, ossia l’*“Artificial Intelligence Act”*, è il primo regolamento organico sulla IA, approvato il 21 maggio 2024 dal Consiglio dell’UE e mira a garantire sistemi di IA sicuri e rispettosi dei diritti fondamentali nel mercato europeo, favorendo un’innovazione sicura in tale ambito attraverso regole armonizzate tra gli Stati membri dell’Unione europea.

L’*AI Act* è fondato su un approccio *“risk-based”* al pari del GDPR: all’aumentare del rischio insito nell’utilizzo di un determinato sistema di IA, aumenteranno anche le regole che si dovranno seguire per la loro commercializzazione, implementazione e fruizione, con la previsione anche di divieti di utilizzo per quei sistemi che manifestano un rischio inaccettabile.

Il Regolamento, infatti, individua quattro diverse categorie in cui poter incasellare i sistemi di AI:

-Sistemi vietati (art. 5 *AI Act*): essi hanno un livello di rischio inaccettabile (alcuni esempi sono quei sistemi di AI che utilizzano tecniche subliminali e volutamente manipolative o ingannevoli che distorcono il comportamento di una persona, o che sfruttano le vulnerabilità di una persona dovute all’età, alla disabilità o a una specifica situazione sociale o economica, o per quei sistemi di riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione etc...)⁴.

-Sistemi ad alto rischio (art. 6 dell’*AI Act* e dell’allegato III): quei sistemi di AI che possono porre rischi significativi per la salute e la sicurezza, o per i diritti fondamentali delle persone. Secondo il Regolamento rientrano in questa categoria i sistemi di AI destinati a essere utilizzati come componenti di sicurezza di prodotti, o che rientrano in uno o più settori critici. Detti sistemi a norma dell’*AI Act* sono soggetti a prescrizioni stringenti in considerazione dell’elevato rischio che li caratterizza.

-Determinati sistemi di IA (art. 50 *AI Act*): sistemi destinati a interagire direttamente con le persone fisiche per i quali sono previsti specifici obblighi di trasparenza.

-Modelli di IA per finalità generali (art. 53 *AI Act*): sono modelli caratterizzati da una generalità significativa e possono svolgere un’ampia gamma di compiti distinti. I fornitori di questi sistemi hanno specifici obblighi attinenti alla redazione della documentazione tecnica e ad obblighi di trasparenza. Tali obblighi diventano più stringenti per i modelli di IA con rischio sistemico (art. 55 *AI Act*), cioè quei sistemi che presentano capacità di impatto elevato valutate sulla base di strumenti tecnici adeguati.

A livello nazionale è necessario sottolineare che il 17 settembre 2025 è stata approvata la Legge italiana in materia di IA n. 132/2025 del 25.09.2025. Il documento è tra i primi a regolare la materia dell’IA a livello interno e si colloca all’interno del quadro sovranazionale sul tema, in armonia con

⁴ Prescrizione già operativa da febbraio 2025.

quanto già previsto a livello comunitario. Obiettivo di tale atto, come si evince dal suo primo articolo, è quello di dettare dei principi sul tema, in un panorama antropocentrico, promuovendo un utilizzo corretto, trasparente e responsabile dei sistemi di IA, ma cercando, al contempo, di tutelare ulteriori interessi, primi fra tutti i diritti fondamentali della persona. Si richiamano, infatti, una serie di principi, già presenti anche nell’*AI ACT*, nel rispetto dei quali si dovranno sperimentare, adottare e utilizzare tali sistemi con finalità generali: nello specifico si fa riferimento ai principi di proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità; per quanto attiene ai dati impiegati se ne deve garantire la correttezza, l’attendibilità, la sicurezza, la qualità e la trasparenza.

Si disciplina, poi, l’applicazione dell’IA in ambiti specifici (a titolo esemplificativo: sistema sanitario, pubblica amministrazione, attività giudiziaria ecc..) e individuando AGID e dell’ACN quali autorità nazionali per l’IA (art. 20), in linea con quanto richiesto nell’*AI ACT*. Infine, il Governo è delegato a definire una disciplina organica sull’utilizzo di dati, algoritmi e metodi matematici per l’addestramento dei sistemi di IA, per l’adeguamento della normativa nazionale all’*AI Act*, nonché per specificare la disciplina in materia di progettazione e uso illecito di sistemi di IA.

Sempre a livello interno, la legge n. 241/1990 (art. 3-*bis*) prevedeva già che le PA favorissero l’utilizzo di strumenti digitali per migliorare i rapporti interni tra le diverse Amministrazioni e tra queste e i privati.

Del pari, il Codice dell’Amministrazione Digitale (D.Lgs. n. 82/2005) all’art. 2 prevede l’obbligo in capo alle pubbliche amministrazioni di assicurare la disponibilità, la gestione, l’accesso, la trasmissione, la conservazione e la fruibilità dell’informazione in modalità digitale e dedica la Sezione III del Capo I alla organizzazione delle PA, nella quale si dispone espressamente l’utilizzo delle tecnologie ICT.

Infine, il Codice dei Contratti Pubblici (D.Lgs. n. 36/2023, art. 30): incentiva, “ove possibile”, l’utilizzo di tecnologie innovative, tra cui l’IA, per l’automazione dei procedimenti amministrativi, assicurando trasparenza e accessibilità del codice sorgente e delle logiche decisionali e introducendo negli atti di indizione delle gare clausole volte ad assicurare le prestazioni di assistenza e manutenzione necessarie alla correzione degli errori derivanti dall’automazione.

Di seguito giova dedicare uno specifico paragrafo alla legge regionale di riferimento in materia di innovazione digitale e tutela dei diritti di cittadinanza digitale, che riserva un’apposita sezione alla progressiva introduzione e all’utilizzo di soluzioni IA nella Pubblica Amministrazione.

2.1. Legge regionale n. 57/2024 (“Disciplina dell’innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla l.r. 54/2009”)⁵.

In un’ottica di razionalizzazione e semplificazione la legge regionale n. 57/2024 mira a unificare in un unico atto normativo la l.r. 1/2004 e le parti ad essa collegate della l.r. 54/2009, anche al fine di garantire un adeguamento al contesto normativo in continua evoluzione nell’ambito della digitalizzazione, dell’IA e della *cybersecurity*, per favorire una pubblica amministrazione più accessibile ed efficiente.

Nell’art. 6 della legge n. 57/2024 tra i principi ispiratori dell’intervento legislativo alla lettera i) viene individuata la promozione di regole di “*progettazione e utilizzo consapevole dei sistemi IA affidabili*”

⁵ Viene qui proposta una sintesi dei punti centrali affrontati dalla normativa in oggetto in tema di IA, per maggiori approfondimenti si rimanda alla lettura integrale del testo di legge.

e sicuri soprattutto nell’esercizio delle funzioni amministrative, tenendo conto in particolar modo dei principi di trasparenza, umanità e responsabilità, in accordo con la normativa statale e dell’Unione europea, ed in collaborazione con le autorità nazionali di riferimento”. L’IA è individuata nella legge regionale come ambito strategico per la Regione Toscana (cfr. art. 7, comma 1, lettera f), pertanto, la Regione promuove lo sviluppo delle tecnologie basate sull’IA, in linea con i principi definiti dalla normativa, europea e nazionale (art. 7, comma 2, lettera g).

A norma dell’art. 8 della suddetta legge la Regione Toscana, nel rispetto dei “principi di trasparenza, etica, non discriminazione, equità, responsabilità, accessibilità, inclusività, coinvolgimento delle persone e protezione dei dati personali”: a) promuove la formazione e lo sviluppo delle competenze necessarie per gestire e applicare l’IA in modo efficace nell’ambito dei servizi erogati e del supporto ai processi decisionali e operativi dell’amministrazione; b) recepisce le indicazioni dalla normativa, europea e nazionale, circa i rischi associati all’impiego di sistemi di IA a garanzia dei diritti fondamentali della persona, rendendo conto delle decisioni adottate e dei servizi erogati con il supporto dell’IA; c) disciplina contesti strutturati e controllati di sperimentazione al fine di testare nuovi approcci e nuove tecnologie tramite l’adozione di opportune misure di salvaguardia dei dati e di valutazione dei rischi e dei risultati connessi con l’adozione a regime delle soluzioni sperimentate; d) tiene conto degli impatti, ambientali ed energetici, legati all’adozione di tecnologie di IA, nonché del rischio di “lock-in tecnologico”.

Nell’ottica di favorire la sperimentazione delle tecnologie di IA, in ottemperanza all’art. 57 *AI Act*, l’art. 25 della legge regionale prevede l’implementazione negli ambiti di propria competenza ed in raccordo con le autorità nazionali delle cd. “regulatory sandboxes”⁶.

3. Principi di base in materia di impiego dell’intelligenza artificiale

Questo documento nasce principalmente con l’intento di fornire delle indicazioni e proporre buone pratiche per un uso consapevole degli strumenti di IA, accompagnare l’adozione delle tecnologie di IA nei settori chiave, garantire trasparenza, accessibilità e partecipazione, oltre ad aiutare la Pubblica Amministrazione toscana a introdurre e implementare soluzioni di IA a supporto dell’attività lavorativa in modo consapevole e il più sicuro possibile e in linea con la normativa vigente.

In accordo con il percorso intrapreso dall’Unione Europea⁷ in materia di adozione dell’IA, Regione Toscana intende promuovere un utilizzo consapevole delle tecnologie dell’IA, allo scopo di innovare e migliorare la qualità e l’efficacia delle attività quotidiane e nel contempo massimizzare i benefici per la diversità e l’inclusività, compresa la diversità culturale, salvaguardando la non discriminazione, promuovendo la libertà di espressione e la parità di genere, l’equità e i principi generali sanciti dalla L. 241/1990 e successive modifiche.

Nello specifico, in aderenza con quanto stabilito dalla Raccomandazione dell’Unesco in materia di IA l’impiego di questa tecnologia deve conformarsi ai seguenti principi:

⁶ Per approfondimenti sul tema si rinvia alla lettura delle fonti normative citate.

⁷ V.di Ethics Guidelines for Trustworthy AI (2019), The Assessment List for Trustworthy Artificial Intelligence (2020), White Paper on Artificial Intelligence (2020), The Ethics of Artificial Intelligence: Issues and Initiatives (2020), Robustness and Explainability of Artificial Intelligence (2020), Review of the Coordinated Plan on Artificial Intelligence (2021) il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull’IA e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regolamento sull’intelligenza artificiale).

trasparenza, equità, responsabilità, intervento e sorveglianza umana, riservatezza e governance dei dati, non discriminazione, benessere sociale e ambientale.

Inoltre, l’Ente Regionale si fa garante del rispetto della *privacy* e dell’uso dei dati relativi ai propri utenti nell’ambito dei sistemi di IA in una logica di *accountability*, adottando le misure necessarie per trattare correttamente i dati personali in maniera adeguata da ridurre e minimizzare i rischi correlati all’utilizzo di tali sistemi, attraverso il rispetto di quanto previsto dalla normativa vigente in materia di protezione dei dati personali e dei dati sensibili.

4. Aspetti Etici dell’Intelligenza Artificiale

L’adozione dell’IA nell’ambito delle istituzioni pubbliche e private impone una riflessione sugli aspetti etici e sulle implicazioni sociali derivanti dall’adozione di questa tecnologia. In linea con l’*AI Act* e con le principali raccomandazioni internazionali in materia, le presenti linee guida della Regione Toscana si propongono di recepire i principi etici fondamentali che devono orientare lo sviluppo e l’implementazione dell’IA, con particolare riferimento ai valori dell’Unione Europea.

Uno dei principi chiave per garantire un uso responsabile dell’IA è la sua affidabilità (*Trustworthy AI*), basata su tre pilastri: legalità (i.e. rispetto della normativa vigente), eticità (i.e. rispetto di principi e valori etici) e solidità tecnica.

Un altro aspetto fondamentale riguarda la robustezza e l’esplicabilità dell’IA. Il rapporto “*Robustness and Explainability of Artificial Intelligence*” evidenzia, in particolare, come un sistema AI debba essere resiliente a errori e attacchi, oltre a garantire una chiara comprensione delle sue decisioni. L’esplicabilità è un principio essenziale per favorire la fiducia degli utenti e per consentire un adeguato controllo umano sulle operazioni dell’IA, specialmente nei contesti in cui le decisioni algoritmiche possono avere un impatto significativo sulla vita delle persone.

Infine, il rapporto “*The Ethics of Artificial Intelligence: Issues and Initiatives*” evidenzia l’importanza di un approccio inclusivo e interdisciplinare nell’elaborazione di politiche sull’IA. Solo attraverso un dialogo aperto e costruttivo sarà possibile garantire che l’IA sia progettata e utilizzata nel rispetto dei valori fondamentali di equità, giustizia e dignità umana.

Alla luce di questi riferimenti, la Regione Toscana si impegna a integrare questi principi etici nelle proprie politiche e strategie per il recepimento dell’*AI Act*, promuovendo un utilizzo trasparente, responsabile e sostenibile dell’IA nel territorio.

5. Benefici dell’IA nella PA

L’IA consente di migliorare l’efficienza operativa della PA, automatizzando attività ripetitive e burocratiche, riducendo errori umani e ottimizzando le risorse. Le tecnologie di *Machine Learning* (ML)⁸ e *Robotic Process Automation* (RPA) permettono di snellire processi quali:

- la gestione delle domande amministrative;
- l’analisi automatizzata di documenti;

⁸ Sistemi di AI che apprendono per migliorare le proprie prestazioni.

- il monitoraggio delle scadenze e l’ottimizzazione dei flussi di lavoro;
- la personalizzazione dei servizi ai cittadini.

Sfruttando l’IA, qualsiasi PA può, dunque, implementare i propri livelli di efficienza, beneficiando simultaneamente di una riduzione significativa dei costi operativi.

6. Criteri per un uso responsabile dell’IA nella PA

Le PA nell’implementare strumenti innovativi che si dotano di soluzioni di IA, deve essere consapevole delle criticità insite in queste tecnologie. In tal senso l’impiego dell’IA deve garantire:

- **Supporto e non sostituzione del decisore umano:** l’IA deve essere uno strumento di ausilio all’attività amministrativa senza esautorare il coinvolgimento umano.
- **Trasparenza e conoscibilità:** il meccanismo tramite il quale si concretizza la decisione automatizzata dovrebbe essere quanto più spiegabile in tutti i suoi aspetti, dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo dell’indicazione dei dati selezionati come rilevanti. Ciò allo scopo di poter verificare che il procedimento automatizzato sia in linea con le prescrizioni e le finalità stabilite dalla legge e dalla singola Amministrazione⁹.
- **Supervisione umana:** è indispensabile assicurare che ogni sistema di intelligenza artificiale impiegato nei processi amministrativi sia soggetto a un’effettiva supervisione umana, al fine di garantire trasparenza, correttezza e comprensibilità delle decisioni. Occorre individuare procedure volte a massimizzare la comprensione delle logiche di funzionamento dell’algoritmo, interpretarne gli esiti e intervenire in caso di anomalie o effetti indesiderati. Al fine di garantire adeguata accountability di tale processo di supervisione, è opportuno documentare le modalità e le fasi operative dei processi utilizzati, così da consentire la verifica e la ricostruzione delle catene decisionali.
- **Non discriminazione algoritmica:** è opportuno che il titolare del trattamento inserisca nei processi di analisi preliminare e nei documenti di valutazione del rischio considerazioni volte a monitorare potenziali fenomeni di discriminazione algoritmica, prendendo in considerazione ed affrontando anche formalmente il continuo monitoraggio e presidio della qualità dei dati trattati dalla IA.
- **Cybersecurity:** nell’ambito delle misure di sicurezza sui sistemi informativi contenenti IA, è opportuno inserire misure dedicate a tale ambito, volte a ridurre il rischio di alterazioni di

⁹ Sul punto si veda la sentenza del Consiglio di Stato n. 2270 del 2019 che affronta specificamente il tema delle decisioni interamente automatizzate per mezzo di un algoritmo, di cui però non è possibile conoscere la formula e i criteri posti alla base della decisione. In particolare con tale sentenza si precisa che, in ossequio al principio di trasparenza, l’utilizzo delle procedure automatizzate non può comportare l’elusione dei principi che regolano l’attività amministrativa: ne consegue, in primo luogo che, l’algoritmo debba essere conoscibile: pertanto tutti gli aspetti della formula tecnica devono essere tradotti nella regola giuridica ad essa sottesa, in modo da renderla leggibile e comprensibile sia ai cittadini che al giudice. La conoscibilità, infatti, consente di verificare che la procedura automatizzata sia conforme a quanto stabilito dalla legge o dalla stessa amministrazione, in questo modo possono essere verificate le modalità e le regole poste alla base della decisione. Inoltre, in base all’articolo 13, par. 2, lett. f) e all’art. 15, par. 1, lett. h) del GDPR è riconosciuto il diritto dell’interessato a conoscere l’esistenza del processo decisionale automatizzato e, in particolare, di ottenere informazioni significative sulla logica utilizzata (i criteri assunti per raggiungere la decisione, senza che con ciò si debba necessariamente fornire una spiegazione complessa degli algoritmi utilizzati) e sulle conseguenze previste di tale trattamento.

comportamento del modello, delle risposte, o accessi illeciti ai dati del sistema di IA (a tale scopo si può fare riferimento anche al progetto OWAP AI Testing Guide reperibile in Rete).

- Parallelamente alla formazione continua del personale dell’Ente, al fine di renderlo sempre più qualificato in materia IA, risulta strategico incentivare forme di *partnership* pubblico-privato e collaborazioni con le Università al fine di creare sinergie di *know-how* fra interni, fornitori di mercato e centri di competenza universitari (come anche richiamato all’art. 24 della LR57/24 relativamente al valore e rilevanza dei Centri di competenza).
- *Accountability*: occorre definire in prima battuta le azioni da intraprendere per una corretta ed efficace azione di minimizzazione e di *privacy by design & by default* che devono trovare applicazione dalla fase di pianificazione e progettazione dei sistemi di AI fino a quella di dismissione, finalizzata anche a definire in modo trasparente la catena decisionale e delle azioni prese in relazione allo strumento di IA nell’ambito del procedimento amministrativo.

L’obiettivo è far sì che i cittadini possano comprendere il funzionamento dei sistemi di IA, i loro limiti e vantaggi. Ciò aiuterebbe sia a promuovere la trasparenza degli stessi (*Explainable AI*) sia nel fidarsi dei loro risultati. Una indicazione che risulta estremamente di successo in questo ambito è la previsione per l’utente di lasciare un *feedback* sulle risposte ricevute dalla IA in modo da permettere la tempestiva segnalazione di allucinazioni, dati da bonificare o comportamenti errati¹⁰.

7. AI ACT e Principi sulla Privacy e il Trattamento dei dati personali (GDPR)

Dall’utilizzo di sistemi IA possono derivare rischi rilevanti per i diritti fondamentali, in particolare per la protezione dei dati personali.

Il quadro normativo di riferimento vede il GDPR come norma cardine, affiancata dall’*AI Act*, che disciplina l’intero ciclo di vita delle tecnologie IA. Il GDPR mantiene infatti il proprio ruolo di normativa di riferimento soprattutto grazie alla sua “*neutralità tecnologica*”¹¹, tanto che lo stesso *AI Act* rimanda alla disciplina dettata dallo stesso¹².

L’*AI Act* stabilisce che il diritto alla protezione dei dati personali debba essere garantito durante l’intero ciclo di vita dei sistemi di IA e, per far sì che ciò avvenga, richiama sia alcuni principi sanciti dal GDPR che alcune sue norme specifiche.

In particolare, vengono richiamati i principi di minimizzazione¹³ e di *privacy by design e by default*¹⁴.

¹⁰ Tali indicazioni, utili anche ai fini di un efficace adozione di soluzioni AI da parte di RT, Comuni ed altri Enti del territorio toscano, sono reperibili nel documento “*AI and GenAI adoption by local and regional administrations*” del *Committee of the Regions* europeo sul livello di adozione della *AI in Local and Regional Authorities* del 07.01.2025.

¹¹ Le regole previste dal GDPR, infatti, devono essere attuate a prescindere dagli strumenti e dalle modalità mediante cui viene svolto il trattamento di dati personali.

¹² Si raccomanda sempre di prendere a riferimento quanto previsto nel Regolamento già citato. In riferimento agli aspetti più in dettaglio legati alla preventiva analisi d’impatto dei sistemi da adottare e alla verifica *ex post* di *compliance* degli stessi, invece, si rinvia al documento specifico di riferimento (“*Indicazioni operative per l’adozione di soluzioni di Intelligenza Artificiale in riferimento all’AI Act in Toscana*”).

¹³ Il principio di minimizzazione dei dati prevede che i dati personali debbano essere adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali vengono raccolte e trattate (v.di in particolare l’art.5 del GDPR).

¹⁴ In base a tale principio le pubbliche amministrazioni e le imprese sono tenute a integrare la protezione dei dati personali già nelle fasi di progettazione di prodotti e servizi (*Design*) e a garantire che vengano trattati solo i dati strettamente necessari (*Default*). Pertanto tale principio impone di valutare e curare, nel rispetto dei principi di trasparenza e di sicurezza, fin dalle fasi iniziali di

In generale, tutti i principi applicabili al trattamento dei dati personali, enunciati nell’art. 5 GDPR, trovano applicazione nelle attività di trattamento mediante un sistema di IA. Ciò significa che quando il sistema di AI implica il trattamento di dati personali, occorre effettuare un’analisi di tale sistema sotto lo specifico profilo della protezione dei dati personali¹⁵.

L’*AI Act* richiama poi le disposizioni del GDPR in materia di processo decisionale esclusivamente automatizzato, inclusa la profilazione, che stabiliscono il 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.

Le pubbliche amministrazioni devono porre la massima attenzione al rispetto dei tre principi cardine che devono necessariamente governare l’utilizzo di algoritmi e sistemi di IA nell’esecuzione di compiti di rilevante interesse pubblico¹⁶:

-il principio di conoscibilità, (l’interessato ha il diritto di conoscere l’esistenza di processi decisionali basati su trattamenti automatizzati e di ricevere informazioni significative sulla logica utilizzata);

-il principio di non esclusività della decisione algoritmica (deve comunque esistere nel processo decisionale un intervento umano capace di controllare, validare ovvero smentire la decisione automatica c.d. “*human in the loop*”);

- il principio di non discriminazione algoritmica (il titolare del trattamento utilizzi sistemi di IA affidabili che riducano le opacità, gli errori dovuti a cause tecnologiche e/o umane, verificandone periodicamente l’efficacia, al fine di garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori¹⁷).

È, infine, importante ricordare che l’art. 35 del GDPR prescrive che i trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche devono essere sottoposti a una previa valutazione di impatto sulla protezione dei dati personali (DPIA). Tra i trattamenti soggetti alla DPIA rientrano anche quelli svolti mediante sistemi di IA¹⁸. Nel caso di sistemi di IA ad alto rischio,

progettazione e sviluppo del prodotto gli aspetti legati alla privacy (v.di in particolare l’articolo 25 del GDPR).

¹⁵ Occorre garantire che il trattamento dei dati personali avvenga in modo lecito, corretto e trasparente, che i dati personali siano raccolti per finalità determinate, esplicite e legittime e siano trattati compatibilmente con tali finalità, che tali dati siano esatti e conservati in una forma che consenta l’identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per cui sono trattati, che si attuino misure tecniche (Nell’*AI Act* sono inoltre indicate alcune misure che i fornitori di sistemi di AI possono utilizzare per garantire la compliance a tali principi, tra cui l’anonimizzazione, la cifratura e l’uso di tecnologie che consentano di inserire algoritmi nei dati e di addestrare i sistemi di AI senza trasmissione o copia dei dati.) e organizzative adeguate a proteggere i dati da violazioni di sicurezza che possano comportare la perdita, la modifica, la divulgazione non autorizzata, l’accesso ai dati personali trasmessi, conservati o comunque trattati. Nel documento “*Indicazioni operative per l’adozione di soluzioni di Intelligenza Artificiale in riferimento all’AI Act in Toscana*” sono reperibili gli appositi modelli standard per guidare alla corretta analisi d’impatto.

¹⁶ Su specifici aspetti di protezione dei dati personali trattati nel contesto dei modelli di IA, si è recentemente espresso altresì lo *European Data Protection Board* con il parere n. 28 del 17 dicembre 2024, utile strumento di indirizzo per la PA in merito alla natura dei modelli di IA in relazione alla definizione di dato personale, alle circostanze in cui i modelli di IA potrebbero essere considerati anonimi e alla relativa dimostrazione, all’adeguatezza dell’interesse legittimo come base giuridica per il trattamento dei dati personali nel contesto dello sviluppo e dell’implementazione dei modelli di IA e al possibile impatto di un trattamento illecito di dati personali nello sviluppo di un modello di IA sulla liceità del successivo trattamento o funzionamento del modello di IA.

¹⁷ cfr. considerando n. 71 del Regolamento.

¹⁸ Il Garante per la protezione dei dati personali li ha inclusi nell’elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a DPIA (Allegato 1 al provvedimento n. 467 dell’11 ottobre 2018).

è il GDPR ad imporre agli utilizzatori (*deployer*) di svolgere una DPIA sulla base delle istruzioni comunicate dal fornitore all’utente, per informarlo sulle finalità previste e sull’uso corretto del sistema di IA.

L’*AI Act*, inoltre, introduce un’ulteriore valutazione d’impatto, centrata sui diritti fondamentali (FRIA), finalizzata alla valutazione degli effetti che un sistema di IA ad alto rischio può avere sui diritti fondamentali delle persone e all’individuazione delle misure da adottare al concretizzarsi di tali rischi. L’*AI Act* stabilisce una connessione tra la DPIA e la FRIA, prevedendo che possano essere svolte congiuntamente¹⁹.

7.1. Trasparenza e sicurezza

Uno dei principi che orientano l’interpretazione dell’*AI Act* e del GDPR è quello di trasparenza, a cui gli operatori di sistemi di IA devono dare concreta attuazione, soprattutto con riferimento ai sistemi di IA ad alto rischio e ai modelli di IA per finalità generali.

Di conseguenza, i sistemi di IA devono essere sviluppati e utilizzati in modo da consentire un’adeguata tracciabilità e spiegabilità, prevedendo anche una adeguata informazione agli utilizzatori riguardo le capacità e i limiti dei sistemi. A tal fine, è opportuno prevedere richieste ai fornitori di documentazione chiara sulle logiche di funzionamento, sulle fonti dei dati e sui criteri di addestramento, assicurando la disponibilità di registri di log o tracciamento delle decisioni. Si deve inoltre mirare ad adottare procedure che consentano di ricostruire come l’algoritmo ha inciso sull’output finale e predispongono indicazioni operative per gli utilizzatori sui limiti e le capacità del sistema, garantendo trasparenza anche nei confronti dei cittadini coinvolti.

E’ previsto inoltre che ogni cittadino abbia diritto a conoscere l’esistenza e il funzionamento del sistema di IA che incidono sulla propria sfera giuridica (principio di conoscibilità). Pertanto, l’informativa sul trattamento dei dati personali, ai sensi del GDPR, deve essere integrata anche con i contenuti previsti dall’*AI Act*.

8. Raccomandazioni e linee guida

Con l’obiettivo di sviluppare la capacità interna rispetto al tema dell’IA, l’Ente regionale sostiene l’adozione responsabile di questa tecnologia mediante un processo di alfabetizzazione critica e consapevole, attraverso la conoscenza fondamentale dell’IA e dei suoi impieghi, le sue implicazioni etiche e il suo impatto sul mondo del lavoro. Si tratta di un processo continuo per promuovere la conoscenza sulla crescente presenza dell’IA nella società contemporanea, capirne le potenzialità e coglierne i limiti (ad es. “*bias*” di genere, di etnia, etc., nonché le così dette “*allucinazioni*”²⁰ nelle quali può incorrere erroneamente il sistema).

¹⁹ Per una trattazione più specifica del tema si rimanda al documento “*Indicazioni operative per l’adozione di soluzioni di Intelligenza Artificiale in riferimento all’AI Act in Toscana*”.

²⁰ Lo stato di “*allucinazione dell’intelligenza artificiale*” (*AI Hallucination State*) è un fenomeno che si manifesta quando l’output generato è falso, non è basato sul *set* di dati su cui è stato addestrato né è previsto dal modello con cui è stato realizzato (Treccani). Nello stato di allucinazione viene fornita una risposta esaustiva, efficace, chiara, logica, ma inventata, completamente infondata. (Chiara Cilardo, Agendadigitale.eu, 28 giugno 2023, Società digitale).

Tra le iniziative avviate a livello regionale si segnalano i c.d. “*Centri di facilitazione digitale*” (Punti Digitale Facile) attivi in maniera capillare sul territorio toscano (deliberazione di Giunta n. 295 del 20 marzo 2023 “*Approvazione criteri dell’avviso per gli enti locali del territorio per l’attivazione di centri di facilitazione digitale previsti dalla misura 1.7.2 Missione 1 Componente 1 PNRR e assegnazione dei relativi finanziamenti a Sviluppo Toscana come organismo intermedio*”), ovvero forme di coordinamento stabili e strutturate, mirate a supportare lo sviluppo di competenze di base della cittadinanza, e a contribuire all’inclusione digitale della popolazione non adeguatamente formata all’utilizzo dei servizi online e in particolare della Pubblica Amministrazione, individuando le esigenze dei singoli cittadini e fornendo loro aiuto e orientamento e a fruire efficacemente dei servizi pubblici offerti in modalità telematica dalla Pubblica Amministrazione e dagli enti eroganti servizi pubblici²¹.

Ulteriore aspetto meritevole di menzione è il percorso di coinvolgimento intrapreso di recente, esteso anche alle imprese presenti nel territorio toscano, mirato a proporre iniziative congiunte per la promozione dell’IA, in particolare mediante la programmazione di eventi di divulgazione e formazione sull’uso dell’IA e lo sviluppo di competenze digitali, indirizzato anche ad un target giovanile, al fine di coinvolgerli attivamente nel processo in corso di trasformazione digitale²².

Inoltre, l’Ente pone particolare attenzione al tema sempre più attuale dell’attività di sperimentazione normativa (c.d. “*regulatory sandbox*”), centrale e necessaria per l’adozione e l’implementazione sicura dei sistemi di IA, ciò anche in accordo con quanto previsto dalla normativa nazionale e sovranazionale in materia. In questo ambito l’Ente è attualmente impegnato nel portare avanti una serie di progetti ad essa dedicati, anche mediante il supporto scientifico delle Università e degli organismi di ricerca toscani.

8.1 Raccomandazioni generali

A seguire alcune raccomandazioni alle quali attenersi per condividere una posizione appropriata e univoca nei confronti dell’utilizzo dell’IA. Le raccomandazioni e le presenti Linee Guida saranno comunque oggetto di aggiornamento in base agli sviluppi tecnologici e della normativa vigente in materia che è in costante evoluzione.

1. Si raccomanda di far precedere l’avvio in produzione di sistemi di IA da una preliminare fase di sperimentazione per le nuove soluzioni IA che si intende introdurre, al fine di consentire una propedeutica e necessaria valutazione degli impatti e una eventuale progressiva estensione dei campi di applicazione delle stesse, nonché un graduale avvicinamento dell’utenza a queste soluzioni, sia essa esterna o interna.

2. Nell’adozione o nell’utilizzo di sistemi di intelligenza artificiale è necessario fornire informazioni chiare ed esplicite sia agli operatori interni che ne fanno uso, sia ai cittadini eventualmente coinvolti dai processi decisionali. Le informazioni devono riguardare le finalità del sistema, le modalità con cui supporta l’attività amministrativa, il grado di autonomia decisionale, i

²¹ V.di in proposito le informazioni di riferimento reperibili sul sito: <https://competenzedigitali.toscana.it/>

²² V.di. Decreto dirigenziale n. 12577 del 11/06/2025 che ha approvato l’Avviso pubblico “*Per la ricerca di soggetti interessati ad attivare iniziative congiunte per la promozione dell’intelligenza artificiale in Toscana*”.

limiti e le cautele d’uso, nonché la possibilità di intervento umano o di revisione delle decisioni automatizzate.

3. Nell’ambito dell’analisi di impatto, è necessario includere una valutazione specifica sull’utilizzo di strumenti di intelligenza artificiale, descrivendo finalità, logiche di funzionamento, tipologie di dati trattati e possibili effetti sui diritti e sugli interessi delle persone coinvolte. E’ inoltre necessario valutare i rischi connessi a errori, *bias* o mancanza di trasparenza e individuare le misure tecniche e organizzative più idonee a garantire tracciabilità, spiegabilità e possibilità di intervento umano.

4. Nell’introduzione dell’IA, è consigliato indicare - nella valutazione di impatto - chiaramente gli ambiti di applicazione appropriati, le finalità e le eventuali limitazioni motivandole rispetto alla coerenza/incoerenza con le finalità per il raggiungimento degli obiettivi prefissati. In ogni caso si consiglia di incentivarne la riflessione critica.

5. Nell’utilizzo dell’IA nell’attività lavorativa quotidiana non si può prescindere da un adeguato e accurato controllo umano.

6. Sono fatte salve le prescrizioni normative del diritto UE e nazionale in materia di diritto d’autore e di diritti ad esso collegati e in particolare ad individuare e rispettare una riserva di diritti espressa a norma dell’articolo 4 paragrafo 3 della direttiva UE 2019/790 (Diritto d’autore e diritti connessi nel mercato unico digitale).

7. Chiunque utilizzi gli strumenti di IA deve considerare che essi potrebbero fornire informazioni false, inaccurate o incomplete per cui le informazioni raccolte dovrebbero essere utilizzate come punto di partenza ma essere verificate attraverso fonti dirette e sottoposte a una attenta valutazione critica.

8. La produzione di testi, immagini o altri contenuti mediante l’utilizzo di sistemi di intelligenza artificiale deve essere dichiarata in modo chiaro e trasparente. A tal fine, nei documenti, nelle pubblicazioni o nei materiali divulgativi deve essere inserita un’indicazione esplicita, ad esempio attraverso una dicitura come “*contenuto generato con il supporto di strumenti di intelligenza artificiale*” o equivalente. Nei casi di utilizzo interno, tale informazione deve essere riportata nella documentazione di progetto o nelle note di accompagnamento, così da garantire tracciabilità e corretta attribuzione della fonte.

Di seguito vengono riportate alcune indicazioni di carattere più prettamente tecnico destinate alla Pubblica Amministrazione.

Nell’adottare soluzioni di IA, è opportuno che l’Ente introduca – secondo modalità organizzative coerenti con le proprie specificità – misure tecniche e organizzative finalizzate a:

- Favorire la conoscibilità e disponibilità della documentazione relativa al funzionamento degli strumenti di IA, tramite la predisposizione di una documentazione tecnica e descrittiva aggiornata accessibile al personale autorizzato e ai soggetti competenti, anche mediante una piattaforma o archivio digitale interno dedicato;
- Prevedere verifiche periodiche per valutare l’affidabilità e l’adeguato temperamento degli interessi e nell’impiego di strumenti di IA e relativo corretto funzionamento, mediante previsione di

un calendario annuale di *audit* o revisioni interne sull’uso dei sistemi di IA, con *report* sintetici sugli esiti e sugli eventuali interventi correttivi, assicurando il coinvolgimento delle strutture competenti in materia giuridica, informatica e organizzativa;

- Monitorare e verificare periodicamente la qualità dei dati inseriti e i livelli di robustezza e resilienza dei sistemi che adottino soluzioni IA, con test di accuratezza e *stress test* periodici, documentando gli esiti e programmando eventuali interventi di aggiornamento o sostituzione dei componenti tecnologici, in modo da improntare le eventuali misure rimediali o *upgrade* di sistema da porre in essere per garantire il raggiungimento di più elevati standard di sicurezza.
- Assicurare percorsi di formazione continua per il personale coinvolto nell’utilizzo di sistemi di IA, attraverso la pianificazione di attività formative differenziate per ruoli e competenze - moduli introduttivi per gli utilizzatori, corsi specialistici per tecnici e responsabili - integrando sessioni pratiche, linee guida etiche e aggiornamenti normativi sul tema dell’IA.
- Implementare sistemi di monitoraggio per rilevare eventuali anomalie o discriminazioni insite nel funzionamento di strumenti di IA²³, tramite l’attivazione di strumenti di controllo automatico (*log*, *alert*, ecc...) per identificare comportamenti anomali o risultati distorsivi, prevedendo un canale interno di segnalazione e una procedura standardizzata per l’analisi e la correzione degli errori.

Nel corpus di documentazione a supporto configurato nel suddetto Kit di adozione della IA, Regione Toscana produrrà ulteriori documenti a supporto degli Enti per indicare possibili modalità organizzative ed attuative anche con riferimento alle raccomandazioni operative suddette.

9. Conclusioni

Regione Toscana, in linea con quanto espresso nella LR57/24, si impegna a promuovere una transizione digitale equilibrata, che sfrutti le potenzialità dell’IA garantendo al contempo trasparenza, equità e tutela dei diritti fondamentali. È, infatti, evidente come le nuove tecnologie, che si dotano di IA, offrano alla PA la possibilità di perseguire in modo più efficiente ed economico (*ex art. 1, l. n. 241/1990*) i principi costituzionali di buon andamento e imparzialità (*ex Art. 97 Cost.*). L’implementazione tecnologica in seno alla PA dovrà, in definitiva, basarsi sui principi di trasparenza e conoscibilità, di non esclusività e di non discriminazione algoritmica e di obbligo di motivazione al fine di garantire che l’*output* automatizzato sia comprensibile, equo e, dunque, legittimo.

²³ “Bozze di Linee guida per l’adozione di IA nella Pubblica amministrazione” vedi par. 3.4 e ss., AGID, feb.2025.

Approfondimenti multimediali

Guidance for generative AI in education and research:

Artificial intelligence. A reading list:

<https://commonslibrary.parliament.uk/research-briefings/cbp-10003/>

Archivio multimediale UNESCO:

<http://www.unesco.org/archives/multimedia/tags/artificial+intelligence>

Strategia italiana per l’intelligenza artificiale 2024/2026:

https://www.agid.gov.it/sites/agid/files/2024-07/Strategia_italiana_per_l_Intelligenza_artificiale_2024-2026.pdf

Indicazioni operative per l’adozione di soluzioni di IA in riferimento all’AI Act in Toscana – Regione Toscana, Giunta Regionale

FAQ²⁴

1. Qual è il ruolo di Regione Toscana nel processo di adozione della IA nella Pubblica Amministrazione presente sul territorio?

Regione Toscana si pone come punto di riferimento, guida e normatore per tutti gli enti del territorio toscano, promuovendo l’adozione della IA consapevole, etica, trasparente, equa, responsabile, accessibile e conforme alle normative vigenti, anche ai sensi dell’art.8 comma 2 della LR57/2024.

2. Quali strumenti fornisce Regione Toscana agli enti del territorio?

Per supportare il processo di adozione alla IA, viene fornito un “Kit di Adozione”, composto da:

-Linee guida generali, indicazioni operative, L.R. 57/2024;

-Strumenti pratici come *checklist* di rischio, modelli di *impact assessment* (DPIA e FRIA) e *template* per la stesura della documentazione; Governance e Supporto formati da RTD regionale, il Gruppo di Lavoro (GdL) interno multidisciplinare, il GdL interdirezionale e il Catalogo software;

-Formazione e collaborazione attraverso le collaborazioni con Università e centri di ricerca, Centri di Competenza Regionali, l’erogazione di corsi formativi per l’alfabetizzazione della IA, e i centri di facilitazione digitale.

3. Quali sono i passi per l’adozione della IA suggeriti da Regione Toscana ad un Ente del territorio?

Il processo di adozione prevede tre fasi operative principali.

Identificare il proprio ruolo nel ciclo di vita del sistema IA secondo le categorie dell’AI Act (Fornitore, Utilizzatore, Importatore, Distributore); Valutare il livello di Rischio del sistema IA secondo le categorie dell’AI Act (Proibito, Altro Rischio, Rischio Limitato e Rischio Minimo); Produzione della documentazione specifica per garantire la trasparenza, la sicurezza e la conformità (*Impact Assessment* e la documentazione tecnica del sistema di IA).

4. Quali sono i benefici di un sistema o strumento di IA nella Pubblica Amministrazione?

L’IA consente di migliorare l’efficienza operativa della PA, automatizzando attività ripetitive e burocratiche, riducendo errori umani e ottimizzando le risorse. Riduce i tempi di conclusione dei procedimenti amministrativi. Consente di erogare un numero maggiore di servizi a cittadini e imprese, migliorandone la qualità e la personalizzazione. Rappresenta uno strumento di supporto per i dipendenti, aiutandoli nell’analisi di documenti, nel monitoraggio delle scadenze e nell’ottimizzazione dei flussi di lavoro.

5. Cosa significa adottare un comportamento “consapevole” di un sistema IA?

²⁴ Tra le varie fonti di riferimento si ricorda e si rinvia per ulteriori approfondimenti a:

https://ec.europa.eu/commission/presscorner/detail/it/qanda_21_1683;

<https://www.eqs.com/it/polo-di-conoscenza-compliance/white-papers/eu-ai-act-mini-guida/#form>.

L’utilizzo consapevole di un sistema di IA implica una serie di attitudini e conoscenze pratiche come: Conoscerne i Limiti e i Rischi ponendo attenzione alle cosiddette "allucinazioni" e i pregiudizi (*bias*). Avere un Approccio Critico utilizzando l’output come un punto di partenza, una bozza da verificare, correggere e validare con le proprie competenze. Riconoscere che la responsabilità di qualsiasi documento, decisione o azione presa con l’aiuto dell’IA è sempre e solo umana. Proteggere le informazioni ed essere coscienti del tipo di dati che si inseriscono nel sistema, con la massima cautela nelle fasi che prevedono e tutelano l’immissione di -dati personali, di tipo particolare -o riservati.

6. Quali sono le misure da adottare per la protezione dei dati personali quando si utilizzano sistemi di IA?

Le misure da adottare per la protezione dei dati personali promosse si possono raggruppare in tre aspetti.

Normativo: applicando i principi indicati dal GDPR e AI Act. Utilizzare fin dall’inizio della progettazione del sistema di IA l’approccio *Privacy by Design* e *by Default*. Questo serve per tutelare la *privacy*, limitare l’utilizzo e il trattamento dei dati personali raccolti solo per scopi specifici, espliciti e legittimi.

Tecnico e Organizzativo : ove possibile, i dati devono essere elaborati in modo da non poter identificare la persona a cui si riferiscono, utilizzando tecniche anonimizzazione, pseudonimizzazione, crittografia e con controlli rigorosi sugli accessi, o tecniche di gestione nei prompt delle informazioni che riconducono al riconoscimento della persona (Personally Identifiable Information). Inoltre è necessario che i set di dati utilizzati per l’addestramento siano pertinenti, rappresentativi e il più possibile privi di errori e pregiudizi (*bias*), prevedendo e proceduralizzando misure di audit periodico a verifica del buon funzionamento del sistema di IA nel rispetto del guardrail o per rilevare *bias* di vario genere. Monitoraggio: adottare strumenti di valutazione d’impatto sulla Protezione dei Dati (DPIA) per analizzare e mitigare tali rischi.

7. Cosa può essere concretamente realizzato in materia di alfabetizzazione e educazione in materia di IA?

Sicuramente l’organizzazione di corsi di formazione risulta particolarmente utile per incrementare le proprie conoscenze, nonché per sensibilizzare sul corretto utilizzo di tali tecnologie e promuoverne un uso responsabile.

L’individuazione presso l’ente di figure di riferimento con competenze specialistiche sia di natura giuridica che informatica (*AI specialist*) da dislocare presso le direzioni regionali e da affiancare a tutto il personale può rappresentare un valido ausilio per uno svolgimento più efficiente e consapevole dell’attività lavorativa nel solco delle prescrizioni normative.

8. Come valuto il livello di rischio del sistema AI?

Si può fare riferimento al documento “*Indicazioni operative per l’adozione di soluzioni di Intelligenza Artificiale in riferimento all’AI Act in Toscana*” (LGAI_RT_#2), che contiene, tra i suoi Allegati, specifiche indicazioni e checklist che risultano particolarmente utili. Gli stessi casi pratici allegati a tale documento possono essere un esempio tangibile da seguire.

Inoltre, L’Unione Europea fornisce uno strumento di supporto e autovalutazione del livello di rischio denominato “EU AI Act Compliance Checker”²⁵.

9. Quali obblighi ho nell’utilizzo di sistemi ad alto rischio?

- Rispettare quanto previsto dall’AI Act per l’implementazione di tali tecnologie;
- Garantire un monitoraggio costante di tali sistemi;
- Assicurarci che tutti i dati di *input* utilizzati siano corretti, privi di *bias*, nonché sufficientemente rappresentativi;
- In caso di incidente interrompere l’utilizzo del sistema e informare tutti i soggetti coinvolti nonché l’autorità di sorveglianza competente.

10. Quali obblighi ho come fornitore o sviluppatore di un sistema ad alto rischio?

- Implementare un sistema di gestione del rischio;
- Fornire una documentazione tecnica dettagliata;
- Stabilire misure di *governance* e garantire il rispetto del principio della necessaria supervisione umana;

²⁵ <https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/>

- Eseguire valutazioni di *compliance*;
- Assicurare la conformità del sistema rispetto alle norme vigenti europee e nazionali.

11. Come valuto l’affidabilità del sistema IA secondo i principi etici dell’AI Act?

L’Unione Europea fornisce uno strumento pratico, denominato “*The Assessment List for Trustworthy Artificial Intelligence*” (ALTAI)²⁶, di supporto a sviluppatori, aziende ed enti per valutare se un sistema di IA è affidabile secondo i 4 principi etici e 7 requisiti fondamentali stabiliti dalla Carta dei diritti fondamentali dell’Unione europea²⁷.

12. Quali sono i soggetti che partecipano alle varie fasi che compongono l’intero ciclo di vita del sistema di IA?

L’accesso a un sistema di IA varia a seconda della fase del suo ciclo di vita e del ruolo degli operatori coinvolti. Non c’è un unico soggetto che ha accesso a tutto il sistema e sempre.

-Sviluppo e Addestramento: il Fornitore (Provider), i suoi sviluppatori, i data scientist e tecnici che lavorano sul codice sorgente, sugli algoritmi e sui dati di addestramento.

-Valutazione della Conformità (per sistemi ad Alto Rischio), gli enti terzi hanno accesso alla documentazione tecnica, ai risultati dei test e ai sistemi di gestione della qualità del Fornitore per poter certificare la conformità del sistema.

-Distribuzione e inserimento sul mercato: gli importatori e i distributori avranno accesso al prodotto finale e alla documentazione di accompagnamento (come le istruzioni per l’uso), ma non al codice sorgente o ai dati di addestramento. Mentre il rappresentante autorizzato: (Per fornitori extra-UE) custodisce una copia della documentazione tecnica da fornire alle autorità su richiesta.

-Utilizzo: l’Utilizzatore (Deployer) che ha accesso alle sue funzionalità operative del sistema di IA attraverso l’interfaccia utente e all’accesso ai “log” generati dal sistema per monitorarne il funzionamento.

-Durante tutto il ciclo di vita: le Autorità di Vigilanza del Mercato, le Autorità Nazionali Competenti, e le Autorità che tutelano i diritti fondamentali, hanno il potere di richiedere l’accesso alla documentazione tecnica, ai log e, in casi motivati, anche al codice sorgente - laddove applicabile - per verificare la conformità alla legge e per accertare eventuali violazioni ai diritti dei cittadini.

²⁶ <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>

²⁷ <https://www.europarl.europa.eu/charter/>