Policy sull'utilizzo dell'Intelligenza Artificiale negli ambienti di lavoro dell'Ente

delibera di Giunta comunale n. 37 dd. 24.03.2026

Sommario

1. DEFINIZIONI E AMBITO DELLA POLICY

1.1. Scopo e ambito di applicazione della Policy

La presente policy intende disciplinare l'utilizzo dei sistemi di Intelligenza Artificiale (di seguito IA o AI) nell'ambito dell'attività lavorativa o istituzionale svolta in favore dell'Ente, recando le linee guida per l'utilizzo di tali sistemi all'interno della organizzazione, promuovendo al contempo l'innovazione e aumentando l'efficienza e l'efficacia operativa delle Pubbliche Amministrazioni.

Le pubbliche amministrazioni utilizzano l'intelligenza artificiale allo scopo di incrementare l'efficienza della propria attività, di ridurre i tempi di definizione dei procedimenti e di aumentare la qualità e la quantità dei servizi erogati ai cittadini e alle imprese, assicurando agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo (art. 14 L. 132/2025).

Con questa policy l'Ente riflette il proprio impegno nell'adottare un uso responsabile ed etico dell'AI promuovendo, tra gli altri, i principi di trasparenza, equità, uguaglianza e rispetto della protezione dei dati personali.

Le disposizioni si applicano a tutto il personale dell'Ente (a tempo indeterminato e determinato), al personale di altri Enti coinvolti nell'ambito di gestioni associate, agli amministratori dell'Ente, e anche agli stagisti, ai tirocinanti, ai collaboratori esterni e, in generale, a tutti gli utenti che a diverso titolo abbiano accesso ai sistemi informativi dell'Ente (d'ora in avanti utenti utilizzatori).

Sono soggetti alle presenti Linee guida tutti i software, i servizi, le piattaforme web e le applicazioni che integrano funzionalità di Intelligenza Artificiale, sia acquisite e attivate direttamente dall'Ente, sia usate dagli utenti dell'Ente nell'ambito di servizi fruiti su piattaforme istituzionali nazionali o provinciali o nell'ambito di relazioni/interazioni con soggetti esterni (per esempio, sistemi di AI terzi in videoconferenze, in sistemi di messaggistica, ecc.).

In apposita sezione Intranet viene implementato e costantemente aggiornato – a cura del Responsabile della Transizione Digitale - l'elenco degli strumenti di AI autorizzati e messi a disposizione dall'Ente e le istruzioni sull'utilizzo, compresa l'indicazione del processo in cui il loro uso è consentito, la procedura per il suo aggiornamento e le modalità di comunicazione degli aggiornamenti agli Utenti.

È vietato l'utilizzo di strumenti di AI diversi da quelli espressamente autorizzati dall'Ente, né è consentito utilizzare per finalità lavorative strumenti di AI per il tramite di account personali.

1.2. Ambito normativo e riferimenti internazionali

La presente policy applica le prescrizioni contenute nel Regolamento (UE) 2024/1689 (di seguito "AI Act"), Regolamento (UE) 2016/679 (di seguito "GDPR"), Legge n. 132 dd. 23 settembre 2025 Disposizioni e deleghe al Governo in materia di intelligenza artificiale e relative normative collegate. Inoltre, integra i principi etici promossi dalle linee guida OCSE e UNESCO.

Come dichiarato nella Relazione di accompagnamento del "AI Act" con questa disciplina la Commissione Europea ha presentato una normativa orientata a sviluppare "*un approccio europeo coordinato alle implicazioni umane ed etiche dell'intelligenza artificiale*".

Come si evince dalla seconda Relazione della Commissione sull'applicazione del regolamento generale sulla protezione dei dati (COM (2024) 357 final): "*Il GDPR è uno dei fondamenti dell'approccio dell'UE alla trasformazione digitale. I suoi principi fondamentali (trattamento equo, sicuro e trasparente dei dati personali, volto a garantire che le persone mantengano il controllo su di essi) sono alla base di tutte le politiche dell'UE che comportano il trattamento di dati personali*".

Le Linee Guida OCSE del 3 maggio 2024 auspicano lo sviluppo di una AI affidabile, in grado di rispettare i principi di libertà, dignità, tutela dell'autonomia umana, della protezione dei dati personali e di accountability nel senso che tutti gli operatori che, a vario titolo, utilizzano questa tecnologia sono responsabili dei principi suindicati.

Allo stesso modo la Raccomandazione UNESCO sull'etica dell'intelligenza artificiale richiama il dovere di agire in modo etico e in linea con i diritti umani.

1.3. Definizioni

- **Intelligenza artificiale (AI):** L'Intelligenza Artificiale (AI) è una tecnologia che permette di realizzare sistemi informatici capaci di eseguire compiti complessi tipici dell'intelligenza umana, come il ragionamento logico e l'apprendimento dai dati. L'AI tradizionale agisce principalmente come un elaboratore di dati: classifica informazioni, riconosce oggetti o prevede tendenze partendo da schemi, regole e dataset predefiniti. L'AI generativa è un sotto-insieme di AI che, grazie a modelli linguistici avanzati (LLM), non si limita a classificare dati esistenti, ma ne crea di nuovi (testi, immagini, codici sorgenti) che appaiono coerenti e naturali. Mentre l'AI tradizionale segue schemi più rigidi, quella generativa "predice" la parola o l'elemento successivo statisticamente più probabile in un contesto, diventando uno strumento creativo di redazione e di confronto.
- **Fornitore servizi AI**: persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che sviluppa il sistema di AI fornito all'Ente;

- **Utente**: qualsiasi persona fisica - dipendente o amministratore - dell'Ente che utilizza un sistema di AI per scopi istituzionali o lavorativi;
- **Dati personali**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato), direttamente o indirettamente, con particolare riferimento a un identificativo come nome, numero di identificazione, dati relativi all'ubicazione, identificativo online o riferibile ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Dati non personali**: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva, che non rientri nella definizione di dati personali, quali, ad esempio, dati relativi ad una persona giuridica, know-how, dati sottoposti a privativa intellettuale;
- **Informazioni anonime**: informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato[1].
- **Parte coinvolta**: qualsiasi persona fisica o giuridica con cui l'Ente interagisce nell'ambito delle sue attività, decisioni, politiche e obiettivi, includendo cittadini, partner e dipendenti, amministratori, fornitori, altre pubbliche amministrazioni.

1.4.Significato dei principali termini e acronimi

Per facilitare la comprensione delle presenti Linee guida, si riporta una legenda dei principali termini tecnici e acronimi utilizzati:

- ACN: Agenzia per la Cybersicurezza Nazionale è l'Agenzia italiana che si occupa di cybersicurezza e di qualificazione dei servizi cloud per le Pubbliche Amministrazioni;
- AI Act: Regolamento europeo nr. 1689/2024 in materia di Intelligenza Artificiale;
- GDPR: Regolamento europeo nr. 679/2016 in materia di protezione dei dati personali;
- RTD: la figura dirigenziale o la persona titolare di posizione organizzativa che all'interno dell'Ente è nominata Responsabile per la Transizione al Digitale;
- LLM: Large Language Model, sono i modelli linguistici di grandi dimensioni progettati per comprendere e generare linguaggio naturale (principale esempio di AI generativa);
- Anonimizzazione: processo che elimina tutti i dati che potrebbero permettere di identificare un interessato, anche mediante tecniche di incrocio con altre informazioni;
- Pseudonimizzazione: rielaborazione dei dati personali che non permette di ricondurli ad uno specifico individuo interessato senza l'utilizzo di informazioni aggiuntive;

[1] Considerando 16 Regolamento (UE) 2018/1725 del Parlamento Europeo e del Consiglio del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

- Bias: pregiudizio o distorsione nei dati di addestramento di un modello di AI, che può portare a risultati non accurati, imprecisi o discriminatori;
- Prompt: input di testo o di altre tipologie di dato (per esempio, un file) inseriti in un modello di AI generativa per chiedere la generazione di un risultato (output) specifico;
- Output: previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;
- Sistemi di AI ad alto rischio: sistemi di AI le cui decisioni possono impattare in modo determinante sulla vita, sui diritti fondamentali e sulla sicurezza delle persone (per esempio, nella selezione del personale, nelle decisioni sull'accesso a servizi, ecc.);
- Sistemi di AI a rischio limitato o nullo: sistemi di AI che non hanno un impatto diretto sui diritti o sulla sicurezza delle persone (per esempio, AI generativa, chatbot, assistenti virtuali, classificazione di informazioni, sintesi di documenti, ecc.). Per tali sistemi la normativa prevede un regime di conformità semplificato che privilegia obblighi di informazione e trasparenza rispetto a specifiche valutazioni tecniche e di sicurezza.

2. PRINCIPI

2.1. Principi etici e morali

Nell'impiego dei sistemi di AI l'Ente si propone di abbracciare i seguenti principi etici e morali:

- **Equità e correttezza**: consapevoli che i risultati derivanti dall'impiego di sistemi di AI possono essere influenzati da pregiudizi o bias sistemici, computazionali e/o statistici, è essenziale utilizzare tali strumenti con attenzione per prevenire qualsiasi forma di discriminazione. Ogni output deve essere attentamente monitorato e analizzato per assicurare la correttezza del contenuto e l'assenza di qualsiasi tipo di discriminazione.
- **Etica e sostenibilità**: ogni pratica o processo funzionale all'utilizzo del sistema di AI dev'essere valutato per il suo impatto etico al fine di garantirne - a sua volta - l'aderenza ai principi adottati dall'Ente. In ogni caso l'AI non sarà utilizzata per arrecare danno alle persone o all'ambiente. La tecnologia sarà impiegata per promuovere il benessere e la sostenibilità, nel tentativo di sviluppare soluzioni innovative che possano migliorare la qualità della vita, ridurre l'impatto ambientale e creare opportunità equitative per tutti.
- **Trasparenza**: ogni Utente deve essere informato e formato dall'Ente prima di intraprendere l'interazione con il sistema di AI. Altresì ogni parte coinvolta dev'essere informata in modo chiaro e trasparente quando una decisione presa dall'Ente è stata influenzata o assunta con l'ausilio di un sistema di AI. Questo approccio non solo mantiene l'integrità e la fiducia nel processo decisionale, ma promuove anche una cultura di responsabilità e consapevolezza tecnologica. In questo contesto, per ogni decisione

assunta per mezzo di un sistema di AI dovrà essere assicurata la trasparenza, spiegabilità, verificabilità, accessibilità e coerenza.

- **Affidabilità**: i sistemi di AI dovranno essere affidabili e sicuri, e dovranno essere adottate misure tecniche ed organizzative idonee a prevenire errori e ridurre potenziali rischi per le parti coinvolte.
- **Riservatezza**: informazioni o dati personali e dati non personali riservati o sottoposti a privativa intellettuale non dovranno essere divulgati. In particolare, l'Ente si assicurerà che i predetti dati non siano utilizzati per addestrare i sistemi di AI.
- **Protezione dei dati personali**: i processi nei quali saranno implementati sistemi di AI dovranno essere improntati ai principi della data protection, ivi compresi quello di privacy by design & by default, al fine di assicurare il rispetto dei diritti e libertà di ogni interessato. In ogni caso tutti i dati utilizzati e generati dai sistemi di AI devono essere trattati in conformità alle normative vigenti, interne e sovranazionali, sulla protezione dei dati personali.
- **Valutazione dei rischi**: è fondamentale che gli Utenti comprendano le limitazioni della tecnologia - e quindi i pericoli insiti nell'utilizzo dei sistemi di AI -, siano quindi in grado di valutare i rischi agli stessi associati (in termini di probabilità e gravità del danno), riuscendo ad intervenire in caso di risultati imprevisti o inappropriati, pianificando e attuandole misure di prevenzione e protezione adeguate.
- **Formazione**: è fondamentale che tutti gli Utenti comprendano come funzionano gli strumenti di AI, come vengono utilizzati e quali impatti potrebbero avere sulle decisioni prese. La formazione continua deve garantire che il personale acquisisca le competenze tecniche necessarie per gestire tale strumento. L'ente deve essere in grado di garantire che sia aggiornato alle ultime innovazioni e sviluppi nel campo dell'AI, permettendo così un uso etico, efficace e consapevole delle tecnologie avanzate da parte dell'Utente.
- **Responsabilità e cultura dell'etica**: gli Utenti dei sistemi AI devono assicurarsi che venga utilizzata conformemente ai presenti principi etici e alla normativa vigente, evitando qualsiasi forma di abuso o discriminazione. A tal fine, i sistemi AI sono soggetti a meccanismi di supervisione adeguati a consentire l'uso appropriato di tale strumento, al fine di attenuare ogni rischio. Ogni Utente è personalmente responsabile dell'uso appropriato e conforme alla presente policy di tale strumento.

3. GOVERNANCE DEL SISTEMA DI AI

La Governance attiene a tutte quelle attività (processi, procedure, misure di sicurezza) finalizzate a garantire che gli strumenti di AI siano sicuri ed etici e soddisfino i principi summenzionati.

Una Governance efficace dell'AI deve includere meccanismi di supervisione che trattano rischi quali allucinazioni (output contenente dati falsi o fuorvianti), bias, violazioni della privacy e uso improprio, promuovendo al contempo l'innovazione e aumentando la fiducia.

4. FINALITÀ E REGOLE DI UTILIZZO

4.1. Supporto al lavoro umano: ambito di applicazione

I sistemi di AI devono essere utilizzati esclusivamente quali mezzi di efficientamento delle attività e processi istruttori dell'Ente, rappresentando un mero ausilio di dette attività senza sostituirsi al lavoro del dipendente o all'attività propria e connessa alla funzione di amministratore.

Nessun atto amministrativo, provvedimento, documento, avviso, risposta o comunicazione ufficiale dell'Ente può essere generato, pubblicato o inviato senza una preventiva, completa e critica verifica del contenuto prodotto con sistemi di AI, da parte di un operatore umano che se ne assume la piena paternità e responsabilità (imputabilità giuridica) e che dovrà mantenere la piena discrezionalità sulle eventuali scelte fatte.

I sistemi di AI sono, quindi, finalizzati al miglior esercizio e all'agevolazione dello svolgimento delle attività lavorative o istituzionali: la presente policy si applica sia in caso di utilizzo degli account e strumenti digitali forniti dall'Ente sia ai dati, documenti e informazioni acquisiti nell'ambito dell'attività lavorativa, anche se trattati tramite dispositivo elettronico privato.[2]

Attività accettabili:
● redigere bozze di atti, pareri, contratti, deliberazioni, determine o altri documenti in uso all'ente, email, avvisi,comunicati; ● attività di analisi documentale; ● attività di analisi statistica e operativa; ● attività di ricerca per la risoluzione di questioni generali (ricerca di informazioni su argomenti generali, scadenze, norme pubbliche o giurisprudenza, anche tramite le funzioni di ricerca approfondita);

[2] Ad esempio, nel caso della app della posta elettronica su telefono personale o pc/tablet nell'ambito dello smartworking.

- automatizzare attività o processi ricorrenti finalizzati a migliorare l'efficienza operativa e ridurre il margine di errore umano;
- sintetizzare documenti non riservati e non contenenti dati personali;
- efficientare la social media strategy
- traduzione di testi per finalità di informazione multilingua;
- creazione di immagini o di layout grafici per presentazioni, brochure o contenuti da pubblicare sul proprio sito web istituzionale

Attività NON accettabili:

- inserimento di dati personali o informazioni e documenti che contengano dati personali (comuni e/o particolari, giudiziari) o qualificabili come riservati o confidenziali;
- utilizzare sistemi di AI non verificati e non autorizzati dall'ente;
- presentare il risultato elaborato da un sistema AI come proprio lavoro originale e senza indicarne l'uso;
- prendere decisioni o assumere provvedimenti basati esclusivamente sull'impiego di AI, senza supervisione e validazione umana
- inserire ripetutamente prompt nei sistemi di AI generativa (prompt tra loro uguali o solo leggermente diversi l'uno dall'altro) senza prevedere un'adeguata e ragionata revisione a monte che garantisca un risultato maggiormente efficace;
- utilizzare sistemi di AI per la profilazione di cittadini, dipendenti o amministratori;
- utilizzare l'AI per attività o ambiti non di stretta competenza del proprio ruolo/funzione.

1.1. Autorizzazioni e divieti nell'utilizzo di sistemi di AI

È consentito l'utilizzo esclusivamente dei sistemi di AI inseriti nell'elenco presente nell'apposita sezione Intranet, implementato e costantemente aggiornato a cura del Responsabile per la Transizione al Digitale – RTD: tali sistemi possono essere contrattualizzati dall'Ente con uno specifico fornitore (per esempio, funzionalità di AI già presenti nelle suite di "Posta elettronica e collaboration", o sistemi di AI aggiuntivi presenti nei software gestionali in uso negli Uffici, o componenti AI aggiuntive presenti sulle piattaforme web, ecc.) o possono essere messi a disposizione dalla Provincia autonoma di Trento o dalle Società di sistema.
Tali sistemi inoltre devono essere utilizzati esclusivamente nell'ambito delle attività lavorative e istituzionali e non per scopi personali e privati.

È vietato l'utilizzo di account personali (per esempio, tramite indirizzi email privati di Gmail, Outlook, Yahoo, ecc.) per registrarsi o accedere a sistemi di AI forniti dall'Ente. È inoltre vietato l'utilizzo di sistemi di AI gratuiti, non contrattualizzati dall'Ente, per finalità lavorative.

L'Ente privilegia l'utilizzo delle funzionalità di AI integrate nelle suite di produttività individuale già in dotazione.

Tutti i sistemi di AI autorizzati dall'Ente devono:

- essere configurati esclusivamente con account professionali nominali o con riconduzione univoca alla singola persona che li usa;
- essere contrattualizzati con un fornitore che l'Ente provvede a nominare Responsabile del trattamento dati;
- garantire che i dati immessi dagli utenti utilizzatori dell'Ente e/o dai cittadini non vengano utilizzati per l'addestramento dei relativi modelli di AI;
- garantire che i contenuti/risultati generati dai sistemi di AI, come testi, tabelle, immagini, ecc., risultanti a seguito di immissione di specifici prompt da parte degli utenti utilizzatori, non siano coperti da diritti d'autore e siano liberamente utilizzabili dall'Ente (ovvero che il fornitore del modello di AI non ne pretenda la titolarità);
- essere presenti nel catalogo dei servizi cloud qualificati dell'Agenzia per la Cybersicurezza Nazionale (ACN) o, se non direttamente presenti, essere gestiti tramite infrastrutture cloud qualificate/adeguate considerate a norma da tale Agenzia, o che possano offrire analoghe garanzie di sicurezza e conformità.

Gli utenti sono inoltre autorizzati, qualora ce ne fosse la necessità, a interagire con sistemi di AI di soggetti terzi, istituzionali o privati, anche se non direttamente contrattualizzati dall'Ente, se il soggetto terzo garantisce, nell'utilizzo di tali sistemi, il rispetto di tutti i principi elencati nelle presenti Linee guida. Un esempio in tal senso può essere la partecipazione a videoconferenze o webinar in cui vengono attivati componenti/agenti di AI per verbalizzare, sintetizzare, rielaborare i contenuti dell'incontro (riunione, evento, webinar).

In caso non vengano fornite garanzie sulle modalità di raccolta e gestione dei dati da parte di tali componenti, i singoli utenti utilizzatori sono autorizzati a negare il proprio consenso all'utilizzo delle stesse o a chiedere che non vengano attivati per registrare i propri dati, come i dati biometrici di volto e voce, i messaggi in chat, ecc. In caso non sia possibile disattivare tali componenti, l'utente potrà utilizzare i sistemi sopracitati anonimizzando i propri dati, ovvero non abilitando, per esempio, microfono e webcam e accedendo con un nome fittizio.

4.2. Formulazione dei prompt

Ogni richiesta (prompt) inserita in sistemi di AI generativa deve contenere tutti i seguenti elementi fondamentali, per i quali si suggerisce di:

1. ruolo: specificare chi deve "impersonificare" l'AI per la richiesta che si vuole fare ("Agisci come un esperto di semplificazione del linguaggio amministrativo");

2. contesto: fornire informazioni generali sull'attività richiesta ("Devo rispondere a un cittadino che chiede informazioni sull'IMIS, ma il testo originale che ho preparato è probabilmente troppo tecnico");

3. compito specifico: indicare chiaramente l'azione che si chiede di realizzare ("Riscrivi questo paragrafo rendendolo comprensibile a un utente non esperto");

4. vincoli e formato: specificare eventuali limiti da rispettare ("Usa massimo 100 parole, mantieni un tono cordiale ma istituzionale, non citare nomi propri");

5. esempio: aggiungere o allegare un eventuale esempio di ciò che ci si aspetta di ottenere, se disponibile (tramite copia-incolla di testo o documento da allegare).

Nella redazione di un prompt, è vietato inserire dati personali quali nomi e cognomi di cittadini o colleghi, codici fiscali, numeri di telefono, indirizzi specifici, dati sanitari, giudiziari o relativi a situazioni di disagio, password, codici di accesso, segreti d'ufficio o informazioni riservate.

L'Ente si assicura che i dati immessi all'interno dei sistemi di AI mediante i prompt di comando non vengano utilizzati quali dataset di addestramento di sistemi terzi, ma solo ed esclusivamente per il miglioramento dell'AI utilizzata dall'Ente.

4.3. Supervisione umana

La supervisione umana (*Human-in-the-loop*) costituisce un approccio volto a garantire l'intervento umano nei procedimenti automatizzati, al fine di evitare che l'intero processo sia governato dal sistema di AI. Questo metodo, infatti, permette di mantenere un equilibrio tra l'efficienza delle AI e la capacità di giudizio umano, riducendo il rischio di errori e bias algoritmici. Tale approccio dev'essere tale da favorire la trasparenza e la responsabilità in modo che ogni scelta possa essere tracciata e giustificata.

Fermi restando gli utilizzi vietati dall'AI, definiti dall'articolo 5 Regolamento (UE) n.1689/2024[3], l'Ente non assume decisioni affidandosi esclusivamente ai sistemi di AI ma sottopone a una supervisione, valutazione e validazione umana i risultati generati dalla AI.

3

Il primo controllo sull'output direttamente generato dall'AI è rimesso in capo all'Utente, restando comunque salvo l'ulteriore controllo spettante ai responsabili dei singoli Uffici/Servizi. Nello specifico, ogni utilizzo del sistema di AI deve essere sempre corretto, verificato e rivisto dall'Utente umano e non potranno mai essere esternalizzati documenti, atti, scritti o orali, ecc., rivelando esclusivamente la decisione assunta dagli strumenti di AI adottati.

4.4. Responsabilità

Si rammenta che l'utilizzo dell'intelligenza artificiale avviene in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale (art. 14, comma 2, L. 132/2025).

Ogni Utente utilizzatore si assume la responsabilità della decisione finale assunta anche con l'integrazione dei sistemi AI, quale mero supporto del processo decisionale preordinato al raggiungimento di risultati ottimali. Pertanto, a ogni Utente è attribuito un accesso personale e nominativo.

L'eventuale inesattezza, incompletezza o illiceità dell'output generato da un sistema di AI non esonera l'utente utilizzatore dalle proprie responsabilità disciplinari, amministrative ed erariali.

L'utilizzatore ha l'obbligo di verificare l'accuratezza e la veridicità dei dati, l'assenza di pregiudizi (bias) e la correttezza dei riferimenti normativi forniti dall'AI, essendo noti i rischi di "allucinazioni" (generazione di informazioni false ma verosimili) intrinseci a tali tecnologie, prima di utilizzarle in atti, comunicazioni o altri tipi di documento. Ogni Utente, quindi, dovrà avere cura di controllare che l'output ottenuto con l'utilizzo dei sistemi di AI sia conforme ai parametri normativi generali e particolari che disciplinano il caso concreto e procedere a verificarne il contenuto.

4.5. Formazione

- ✓ sistemi che utilizzano tecniche subliminali, manipolative o ingannevoli per influenzare il comportamento delle persone;
- ✓ sistemi che approfittano di persone vulnerabili, come anziani o disabili;
- ✓ sistemi che attribuiscono punteggi sociali basati su condotte o personalità, creando schedature delle persone;
- ✓ sistemi che prevedono la probabilità che una persona commetta un crimine;
- ✓ sistemi che alimentano database di riconoscimento facciale con immagini raccolte indiscriminatamente da Internet;
- ✓ sistemi che leggono le emozioni delle persone sul luogo di lavoro o a scuola;
- ✓ sistemi che classificano e profilano le persone utilizzando dati biometrici;
- ✓ sistemi che identificano a distanza e in tempo reale persone in luoghi pubblici, salvo motivi di giustizia o sicurezza.

L'Ente promuove l'alfabetizzazione digitale del proprio personale e degli amministratori tramite percorsi formativi dedicati all'Intelligenza Artificiale.

La formazione verterà sul funzionamento dei sistemi, sull'uso consapevole e sicuro dell'AI, sulla formulazione efficace dei prompt, ma anche sulle normative di riferimento, sulle implicazioni etiche e operative e sulla consapevolezza dei rischi che potrebbero nascere con l'utilizzo di sistemi di AI (per esempio, il rischio di "allucinazione" con generazione di dati falsi o riferimenti normativi inesistenti o il rischio in tema di protezione dei dati personali).

La partecipazione alla formazione è considerata obbligatoria per il personale e per gli utenti che saranno abilitati dall'Ente all'uso di tali sistemi.

Nessun sistema di AI può essere utilizzato dal personale e dagli utenti utilizzatori dell'Ente se non dopo aver partecipato alla formazione sul suo utilizzo e aver preso visione delle presenti Linee guida.

5. RISERVATEZZA E PROTEZIONE DEI DATI PERSONALI

5.1. Tutela dei dati personali

E' fatto espresso divieto a tutti gli Utenti di inserire in qualsiasi sistema di AI dati personali che rendano identificabili specifici soggetti. Tali dati potranno essere inseriti solamente se previamente anonimizzati.

Ogni input inserito in un sistema di AI dev'essere regolarmente controllato e monitorato per garantire che l'output risultante sia coerente con il prompt inserito. Questo processo di verifica e controllo è fondamentale per mantenere l'affidabilità e l'accuratezza delle risposte generate.

In caso di incertezza riguardo ai dati personali è obbligatorio astenersi dall'inserirli in qualsiasi sistema di AI e procedere a consultare immediatamente il Referente privacy.

In ogni caso, gli Utenti si impegnano ad adottare ogni misura tecnica ed organizzativa adeguata ad assicurare la protezione dei dati, importati nei prompt di comando e generati negli output dei sistemi di AI, da accessi o divulgazioni non autorizzate, perdite, distruzione, alterazione o manomissioni, e ciò anche in conformità alle procedure di prevenzione e gestione dei *data breach* adottate dall'Ente.

6. PROPRIETÀ INTELLETTUALE

L'uso di sistemi di AI dovrà avvenire rispettando ogni vincolo di riservatezza o privativa esistente sulle informazioni in possesso dell'Ente.

È vietato utilizzare come input immagini, video, parti di libri, articoli giornalistici o codici sorgente senza una previa licenza o un'autorizzazione esplicita. Si ricorda che utilizzare o pubblicare i risultati prodotti da una IA senza aver prima accuratamente verificato che esso non contenga contenuti riservati o protetti da diritto d'autore o da altre normative in materia di privative può essere fonte di responsabilità.

7. TRASPARENZA

L'Ente e ogni Utente si impegnano a informare in modo chiaro gli interessati e tutte le parti coinvolte dell'esistenza del sistema di AI nelle attività dell'Ente, spiegandone i benefici, i limiti, le misure di sicurezza adottate e con quali modalità verrà assicurata la protezione dei loro dati personali e dei dati non personali che li riguardano.

Nello specifico ogni Utente utilizzatore sarà tenuto a indicare in modo chiaro e trasparente se, e in che misura, il contenuto generato è stato confezionato con l'ausilio di uno strumento di AI.

Esempi di dicitura potrebbero essere "Testo elaborato con il supporto dell'AI e revisionato da un operatore dell'Ente" o "Immagine generata dall'Ente tramite Intelligenza Artificiale".

Se vengono generate o integrate/modificate foto e/o immagini con sistemi di AI la dicitura va sempre inserita a corredo dell'immagine stessa e, laddove possibile, anche nell'immagine (in questo caso con una dicitura sintetica come "Generata con AI" o "AI" o "Modificata con AI").

Nei casi in cui l'Ente attivi sistemi di AI che abbiano come beneficiari cittadini o altre tipologie di destinatari e che prevedono interazioni con l'AI via chat, email o altra modalità, è necessario informare gli stessi che stanno interagendo con un sistema di Intelligenza Artificiale e, laddove possibile, descrivere la logica decisionale e/o redazionale prevista.

Nei casi in cui l'Ente attivi sistemi di AI che potrebbero coinvolgere, anche solo indirettamente, altri utenti (per esempio, la componente AI presente in alcuni sistemi di videoconferenza per verbalizzare, sintetizzare, rielaborare i contenuti di un meeting) è necessario informare fin da subito gli altri utenti coinvolti e chiedere il consenso all'uso di tali sistemi/componenti.

8. SOSTENIBILITÀ AMBIENTALE

L’adozione dell'Intelligenza Artificiale nell’Ente non è un processo a “costo zero” per l'ecosistema. Ogni singola interazione con i modelli di AI (principalmente prompt) attiva una moltitudine di calcoli complessi in datacenter esterni che richiedono ingenti risorse.

Dal punto di vista della sostenibilità ambientale, si stima che un’interazione di qualche decina di richieste nei confronti di un modello di AI generativa avanzato possa consumare un numero significativo di wattora di energia elettrica e di millilitri di acqua per il raffreddamento dei datacenter stessi. Alcuni studi arrivano a stimare un consumo, nel caso di prompt particolarmente lunghi e complessi, che può arrivare fino a diversi bicchieri d’acqua per la generazione dell’output richiesto. Sebbene sembrino apparentemente delle quantità esigue, se si moltiplicano le stesse per le numerose richieste quotidiane che ogni utente può fare, si ottengono numeri molto significativi che potrebbero danneggiare l'impronta ecologica globale.

Nella redazione dei prompt con cui interagire con l’AI gli utenti utilizzatori sono tenuti pertanto a rileggere e a revisionare i testi delle richieste prima della loro immissione nei sistemi di AI, adottando la massima precisione possibile e un uso consapevole e ragionato, evitando interazioni meramente di prova, ridondanti, non revisionate o non necessarie.

9. Sicurezza informatica e segnalazioni

L'accesso ai sistemi di AI deve avvenire tramite credenziali nominative di lavoro e, quando possibile, tramite autenticazione a due fattori (MFA).

Gli utenti sono tenuti a segnalare tempestivamente al Responsabile per la Transizione al Digitale (RTD) e al Referente Privacy qualsiasi anomalia o sospetta fuga di dati o sospetto incidente derivante dall'interazione con i sistemi di AI.

Il Referente Privacy valuterà l’eventuale necessità di attivazione della procedura di data breach dell’Ente e, in caso venga confermata una violazione, provvederà ad informare tempestivamente il Responsabile per la protezione dei dati (RPD) dell’Ente.

10. VIOLAZIONE POLICY

Il Responsabile per la Transizione al Digitale (RTD), in stretta sinergia con i Responsabili delle Aree e dei Servizi dell’Ente, sovrintende all’applicazione delle presenti Linee Guida, promuovendo il corretto utilizzo dei sistemi di Intelligenza Artificiale al fine di prevenire potenziali rischi informatici, gestionali o reputazionali.

La violazione della presente policy comporta l'adozione di azioni disciplinari nei confronti degli Utenti che se ne rendano responsabili.

11. REVISIONE DELLA POLICY

L'Ente si impegna a rivedere la presente policy al fine di garantire che rimanga aggiornata con le best practices internazionali, le evoluzioni normative e le tecnologiche involgenti il settore dell'AI.