L’uso della IA Generativa nelle attività di audit

Giancarlo Butti

- Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
- Referente Inclusion e Regolamento DORA del Comitato Scientifico del CLUSIT.
- Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 170 corsi e seminari presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CA FOSCARI, CEFRIEL, ABI…
- Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei.
- Ha all'attivo oltre 800 articoli e collaborazioni con oltre 40 testate.
- Ha pubblicato 28 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 30 opere collettive nell'ambito di ABI LAB, Oracle/CLUSIT Community for Security, Rapporto CLUSIT.
- Socio e già proboviro di AIEA è socio del CLUSIT, di DFA, di ACFE e del BCI.
- Partecipa a numerosi gruppi di lavoro.
- Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC 27001:2005/2013/2022, LA ISO 20000-1, LA ISO/IEC 42001, CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, DPO UNI CEI EN 17740:2024, CBCI, AMBCI.

L’uso degli strumenti gratuiti di IA a supporto delle attività di AUDIT

Agenda

1. Le possibili applicazioni dell’IA nel contesto delle attività di Audit
2. Le normative rilevanti in ambito IA
3. AI ACT
4. Trattamento dati personali
5. Strumenti per la valutazione di impatto

Note sul copyright

Note sul copyright

Possibili impieghi dell'AI generativa nelle attività di audit

1. Preparazione e pianificazione degli audit

Identificazione dei rischi: ChatGPT può aiutare a identificare i principali rischi legati a specifici processi o settori. Può fornire una base di conoscenze sui rischi comuni e sulle migliori pratiche per la mitigazione.

Creazione di check-list: Basandosi su normative, standard di settore e best practice, ChatGPT può generare check-list personalizzate per l'audit.

Definizione degli obiettivi: Può supportare la definizione degli obiettivi di audit, aiutando a chiarire le aree chiave di interesse e i criteri di valutazione.

2. Supporto nelle fasi di esecuzione

Analisi documentale: ChatGPT può aiutare a esaminare documenti, contratti e report, evidenziando potenziali aree di criticità o non conformità.

Automazione di risposte a domande frequenti: Durante le interviste o i controlli, ChatGPT può rispondere a domande comuni o fornire chiarimenti su termini tecnici, normativa e standard di audit.

Interpretazione di normative e standard: In caso di dubbi sull'applicazione di determinati requisiti, ChatGPT può fornire un'interpretazione di standard, regolamenti e policy, aiutando a garantire la conformità.

3. Analisi e sintesi dei dati

Riepilogo dei risultati: ChatGPT può generare riassunti delle osservazioni e delle conclusioni delle verifiche di audit, facilitando la sintesi dei dati.

Analisi delle deviazioni: Aiuta ad analizzare deviazioni nei processi e nelle procedure rispetto agli standard di riferimento, suggerendo possibili cause e impatti.

Identificazione di tendenze: Attraverso l'analisi di report storici e dati di audit, può aiutare a individuare pattern di rischio e suggerire aree da approfondire nelle revisioni future.

Possibili impieghi dell'AI generativa nelle attività di audit

4. Supporto alla redazione del report di audit

Stesura di sezioni del report: ChatGPT può redigere parti del report di audit, come la descrizione del processo, i punti critici e i rischi identificati, accelerando il processo di scrittura.

Suggerimento di raccomandazioni: In base alle osservazioni, ChatGPT può suggerire raccomandazioni o misure correttive da includere nel report finale, basate sulle best practice.

Verifica della conformità alle linee guida: Può aiutare a controllare che il report sia in linea con le linee guida e gli standard di reportistica dell'azienda.

5. Formazione e supporto continuo

Formazione degli auditor: ChatGPT può fungere da assistente virtuale per la formazione di nuovi auditor, fornendo spiegazioni su metodologie di audit, standard e normative.

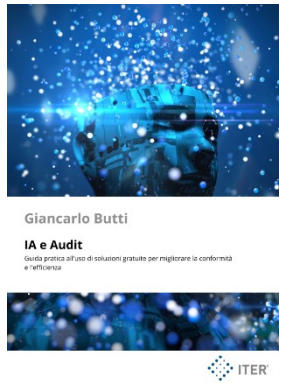
Aggiornamenti normativi: Fornisce aggiornamenti su normative e regolamenti rilevanti per l'audit, mantenendo il team informato sulle nuove leggi e standard di settore.

6. Gestione delle comunicazioni

Risposte alle richieste dei dipendenti: ChatGPT può rispondere a richieste di chiarimenti o informazioni da parte dei dipendenti sui processi di audit, facilitando la trasparenza e la comprensione dei controlli.

Feedback ai team: Durante il processo di audit, ChatGPT può essere usato per generare feedback su specifiche osservazioni in tempo reale, facilitando la comunicazione con i team responsabili.

Casi possibili nell’ambito delle attività di audit



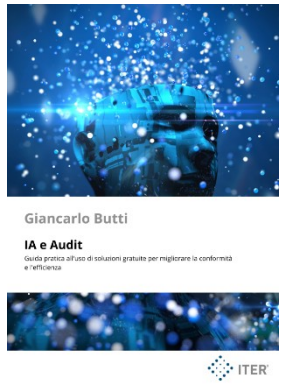
Fase preliminare alle attività di audit

- Che aiuto mi puoi dare per l'esecuzione di un audit
- Come deve essere impostata una richiesta per creare una checklist

Metodologia di audit

- Determinare la dimensione del campione per una popolazione di 5000 elementi e una confidenza del 90%
- Puoi generare del codice per una macro excel che elabori quanto sopra esposto
- Puoi creare del codice per excel al fine di calcolare il numero di campioni da analizzare necessario per avere una confidenza prestabilita?
- Definisci dei criteri con cui valutare i rilievi di un audit
- Definisci dei criteri per valutare il peso di ogni singolo criterio sopra elencato rispetto agli altri, e descrivi le ragioni della tua scelta
- Definisci dei criteri con cui combinare le valutazioni dei singoli rilievi al fine di dare una valutazione complessiva all'audit report. Descrivi le motivazioni delle scelte.

Casi possibili nell'ambito delle attività di audit



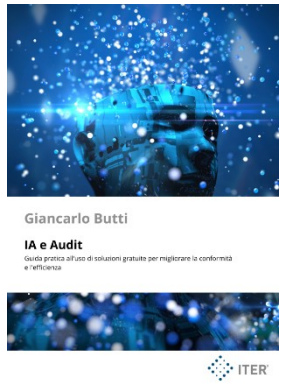
Fase di pianificazione delle attività di audit

- Individua almeno 20 parametri con cui individuare le aree aziendali di maggior rischio, sulle quali eseguire attività di audit
- Per ognuno dei punti sopra riportati elenca una scala di 5 valori che ne permetta la valutazione
- Trasforma i valori qualitativi in range quantitativi
- Individua almeno 20 criteri per identificare quali applicazioni sottoporre ad audit
- Individua almeno 20 criteri per identificare quali processi ICT sottoporre ad audit.

Fase di preparazione dell'audit

- Descrivi come deve svolgersi una attività di audit interno nell'ambito della business continuity
- Come può essere eseguito un audit sulla continuità operativa
- Descrivi un processo ideale per la gestione della business continuity
- Quali sono le fonti che hai utilizzato per descrivere il processo
- Come eseguire al meglio una business impact analysis
- Quali sono i controlli che devo effettuare su una BIA per verificare se è conforme ai requisiti previsti dalla normativa di Banca d'Italia
- Quali sono i controlli che devo mettere in atto per verificare se un piano di continuità operativa sia conforme alle normative EBA e quali sono le normative EBA da prendere in considerazione
- Crea una checklist per svolgere una verifica in ambito business continuity
- Puoi ampliare la checklist ad almeno 100 quesiti
- Crea una checklist di almeno 100 quesiti per un audit sulla business continuity dove nella prima colonna metti il numero della domanda, nella seconda la domanda, oltre ad altre 5 colonne vuote
- Per ogni domanda della checklist precedente predispone 5 risposte che indicano diversi livelli di maturità e compila le colonne della tabella che prima erano vuote
- Genera il codice CSV della precedente tabella
- Crea una checklist per un audit report sulla business continuity basato sulla ISO 22301 per un'azienda manifatturiera di medie dimensioni.

Casi possibili nell'ambito delle attività di audit



Fase di esecuzione di un audit

- Dopo aver individuato i ruoli che in un'azienda sono coinvolti nel processo di gestione della business continuity, genera una serie di domane finalizzate ad intervistare ognuno di loro
- Puoi fare la stessa cosa considerando figure più operative rispetto a quelle elencate in precedenza
- Comportati come un auditor e fammi delle domande considerando che sono il business continuity manager
- Puoi dare un peso alle varie domande e giustificare la tua scelta
- Come deve essere effettuata una verifica sulla conformità di una informativa privacy
- Verifica se la seguente informativa privacy è conforme

Fase di reportistica

- Imposta lo schema di un audit report
- Genera lo schema di un audit report relativo alla business continuity

AI Act

- Oggetto, definizione e ambito di applicazione
- Classificazione dei sistemi di IA e pratiche di IA vietate
- Obblighi di trasparenza per determinati sistemi di IA e modelli di IA per finalità generali
- Eccezioni previste per le autorità di contrasto
- Sistemi di IA per finalità generali e modelli fondativi o di base
- Misure a sostegno dell'innovazione
- Architettura di governance
- Sistemi di IA già immessi sul mercato o messi in servizio
- Sanzioni
- Misure di attuazione
- Entrata in vigore

Oggetto, definizione e ambito di applicazione

Il regolamento ha l'obiettivo di migliorare il funzionamento del mercato interno e promuovere l'adozione di un'intelligenza artificiale affidabile e incentrata sull'uomo, garantendo, nel contempo, un elevato livello di **protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dell'UE**, compresa la democrazia, lo Stato di diritto e la tutela dell'ambiente dagli effetti dannosi dei sistemi di intelligenza artificiale nell'Unione, nonché sostenendo l'innovazione.

Definizione

La definizione di sistema di IA formulata nel regolamento è quella di *“sistema di IA": un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;”.*

Alla Commissione europea è demandata l’adozione di linee guida sull’applicazione della richiamata definizione di sistema di IA.

La definizione originariamente proposta dalla Commissione è stata modificata nel corso del negoziato allo scopo di allinearla all'approccio dell'OCSE.

Composizione

Il nuovo regolamento introduce:

a) regole armonizzate per **l'immissione sul mercato, la messa in servizio e l'uso** dei sistemi di intelligenza artificiale nell'Unione;

b) il **divieto** di determinate pratiche di intelligenza artificiale;

c) **requisiti specifici per i sistemi di IA ad alto rischio** e obblighi per gli operatori di tali sistemi;

d) regole di **trasparenza** armonizzate per alcuni sistemi di IA;

e) **regole** armonizzate specifiche per l'immissione sul mercato di **modelli di IA di uso generale**;

f) **regole sul monitoraggio del mercato, sulla governance e sull'applicazione della vigilanza del mercato stesso**;

g) misure a **sostegno dell'innovazione**, con particolare attenzione alle PMI, comprese le start-up.

Applicabilità

Il regolamento si **applicherà ai soggetti pubblici e privati**, all'interno e all'esterno dell'UE, a condizione che il sistema di IA sia **immesso sul mercato dell'Unione** o che il **suo uso abbia effetti su persone situate nell'UE.**

Riguarderà sia i **fornitori** (ad es. uno sviluppatore di uno strumento di screening dei CV) che gli **operatori** (*deployer*) di sistemi di IA ad alto rischio (ad es. una banca che acquista uno strumento di screening dei CV).

Gli **importatori** di sistemi di IA dovranno inoltre garantire che il fornitore straniero abbia già eseguito l'appropriata procedura di **valutazione della conformità**, che il sistema rechi una **marcatura di conformità europea (CE)** e sia **corredato della documentazione e delle istruzioni per l'uso richieste.**

Classificazione dei sistemi di IA e pratiche di IA vietate

Seguendo un approccio "basato sul rischio", in base al quale tanto maggiore è il rischio, quanto più rigorose sono le regole, la nuova disciplina stabilisce obblighi per fornitori e operatori dei sistemi di IA a seconda del livello di rischio che l'IA può generare:

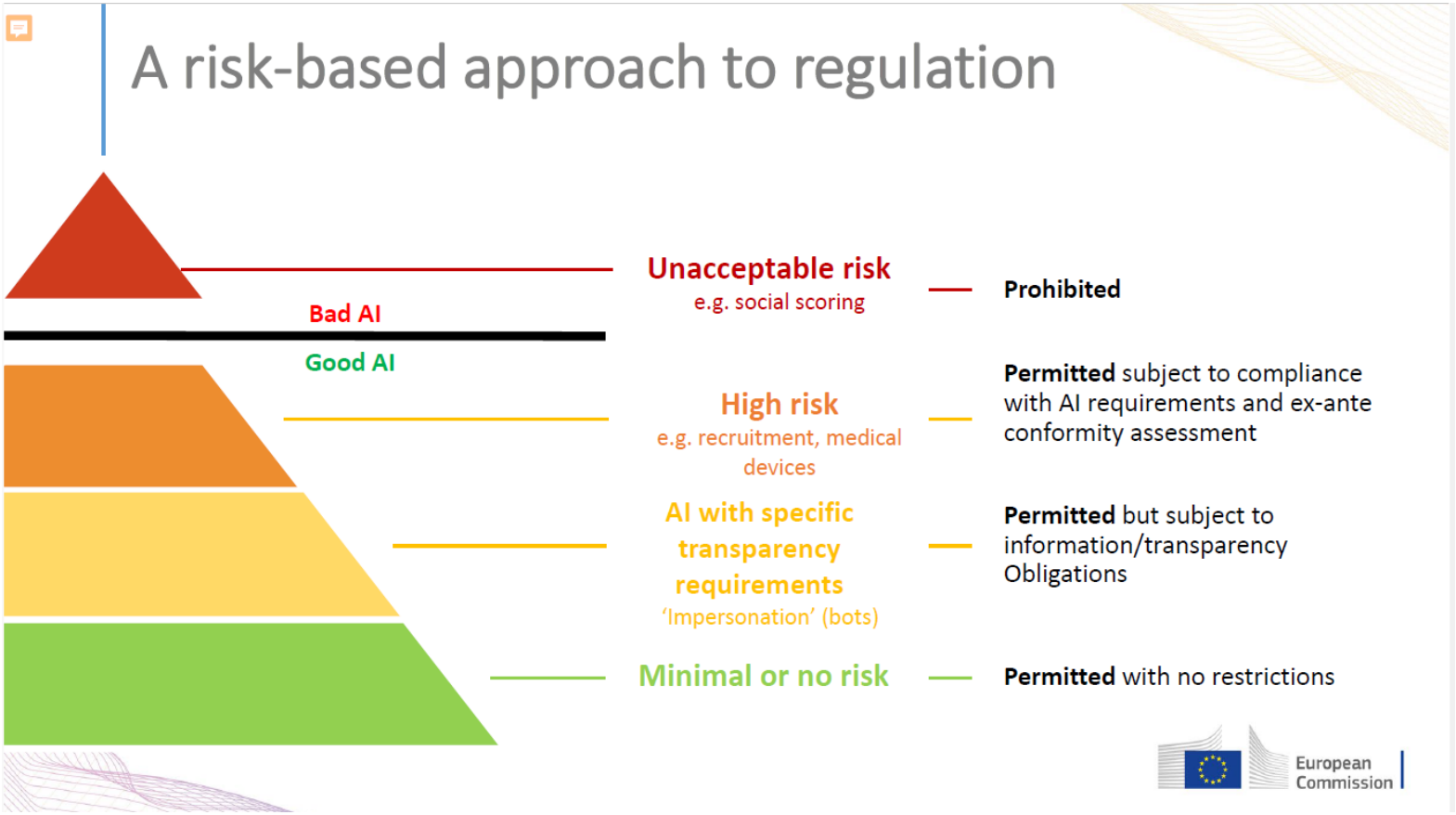
i) un rischio inaccettabile;

ii) un rischio alto;

iii) un rischio basso o minimo.

Sono stabiliti anche obblighi specifici per la trasparenza.

Classificazione dei sistemi di IA e pratiche di IA vietate



Pratiche di IA vietate per rischio inaccettabile

Saranno vietati i sistemi di IA che determinano un rischio inaccettabile per la sicurezza, i mezzi di sussistenza e i diritti delle persone. In questa categoria rientrano i sistemi che **possono manipolare il comportamento umano** come quelli che consentono di attribuire un "punteggio sociale" (social scoring), per finalità pubbliche e private, classificando le persone in base al loro comportamento sociale o alle loro caratteristiche personali, e **determinate applicazioni di polizia predittiva.**

Divieti

Saranno quindi vietati, in particolare:

• i sistemi di **sfruttamento delle vulnerabilità delle persone** e di utilizzo di **tecniche subliminali** ovvero deliberatamente manipolative o ingannevoli;

• i sistemi di **categorizzazione biometrica** delle persone fisiche sulla base di dati biometrici per dedurne o desumerne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale (sarà ancora possibile filtrare set di dati basandosi su dati biometrici nel settore delle attività di contrasto);

• i sistemi di **identificazione biometrica in tempo reale in spazi accessibili al pubblico** (ossia il riconoscimento facciale mediante telecamere a circuito chiuso) da parte delle autorità di contrasto (con limitate eccezioni: vedi oltre);

Divieti

• i **sistemi di riconoscimento delle emozioni** utilizzati sul **luogo di lavoro e negli istituti scolastici**, eccetto per motivi medici o di sicurezza (ad esempio il monitoraggio dei livelli di stanchezza di un pilota);

• l'estrazione non mirata **(scraping) di immagini facciali da internet o telecamere a circuito chiuso** per la creazione o l'espansione di banche dati;

• i sistemi che consentono di attribuire un "**punteggio sociale**" (social scoring), classificando o valutando le persone in base al loro comportamento sociale o alle loro caratteristiche personali.

Sistemi ad alto rischio

Il regolamento considera ad **alto rischio** un numero limitato di sistemi di IA che possono potenzialmente **avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali** (tutelati dalla Carta dei diritti fondamentali dell'UE).

Prima di immettere un sistema di IA ad alto rischio sul mercato dell'UE, **o di farlo entrare in servizio**, i fornitori dovranno sottoporlo a una **valutazione della conformità**. Dovranno, quindi, **dimostrare che il loro sistema è conforme ai requisiti obbligatori per un'IA affidabile (**ad esempio: qualità dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, accuratezza, cibersicurezza e robustezza). Anche **per i sistemi biometrici** è sempre richiesta una **valutazione della conformità da parte di terzi**. La **valutazione dovrà essere ripetuta in caso di modifica sostanziale del sistema o della sua finalità**.

Sistemi ad alto rischio

I sistemi di IA ad alto rischio dovranno essere **tecnicamente robusti** per garantire che la tecnologia sia adatta allo scopo e che i **risultati falsi positivi/negativi non incidano in modo sproporzionato sui gruppi protetti** (ad esempio, per origine razziale o etnica, sesso, età, ecc.). Dovranno, inoltre, essere **addestrati e testati con set di dati sufficientemente rappresentativi** per ridurre al minimo il rischio di integrare **distorsioni inique** nel modello e garantire che, se presenti, queste possano essere **risolte mediante opportune misure di rilevazione, correzione e attenuazione**. Dovranno anche essere **tracciabili e verificabili**, garantendo la **conservazione dell'opportuna documentazione**, compresi i **dati utilizzati per addestrare l'algoritmo**, fondamentali per le indagini ex post.

Sistemi ad alto rischio

Si impone inoltre agli operatori che siano organismi di diritto pubblico o operatori privati che **forniscono servizi pubblici**, nonché agli **operatori che forniscono sistemi ad alto rischio** di effettuare una **valutazione d'impatto sui diritti fondamentali**.

La valutazione deve consistere in una **descrizione dei processi** dell'operatore in cui il sistema di IA ad alto rischio sarà utilizzato, del **periodo di tempo** e della **frequenza** in cui il sistema di IA ad alto rischio è destinato a essere utilizzato, delle **categorie di persone fisiche e dei gruppi** che possono essere **interessati dal suo uso nel contesto specifico**, dei **rischi specifici** di danno che possono incidere sulle categorie di persone o sui gruppi di persone interessati, e in una **descrizione dell'attuazione delle misure di sorveglianza umana** e delle **misure da adottare in caso di concretizzazione dei rischi.**

Sistemi ad alto rischio

I sistemi di IA che costituiscono **componenti di sicurezza di prodotti disciplinati dalla legislazione settoriale** dell'Unione saranno **sempre considerati ad alto rischio**, **se soggetti a una valutazione della conformità da parte di terzi ai sensi della legislazione settoriale stessa.** I fornitori di tali sistemi dovranno inoltre attuare sistemi di **gestione della qualità e del rischio** per garantire la conformità ai nuovi requisiti e ridurre al minimo i rischi per gli utenti e per le persone interessate, anche dopo l'immissione sul mercato di un prodotto.

I sistemi di IA ad alto rischio implementati da **autorità pubbliche o entità che agiscono per loro conto** dovranno essere **registrati in una banca dati pubblica dell'UE**. Ove tali sistemi **non** siano **utilizzati per le attività di contrasto e relative al controllo della migrazione**, dovranno essere registrati in una **parte non pubblica della banca dati,** che sarà accessibile solo alle autorità di controllo competenti.

Sistemi ad alto rischio

Le autorità di vigilanza del mercato **contribuiranno al monitoraggio** successivo all'immissione sul mercato mediante audit e **offrendo ai fornitori la possibilità di segnalare incidenti o violazioni gravi degli obblighi in materia di diritti fondamentali di cui sono venuti a conoscenza**. Qualsiasi autorità di vigilanza del mercato potrà, per motivi eccezionali, autorizzare l'immissione sul mercato di una specifica IA ad alto rischio.

Sistemi ad alto rischio

Tra i sistemi ad alto rischio rientrano, in particolare, quelli:

- di **identificazione biometrica remota, categorizzazione biometrica** e **riconoscimento delle emozioni** (al di fuori delle categorie vietate);
- utilizzati come **componenti di sicurezza** nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale e della fornitura di acqua, gas, riscaldamento ed elettricità;
- finalizzati a **determinare l'accesso**, l'ammissione o l'assegnazione agli **istituti di istruzione e formazione professionale** (ad esempio, per valutare i risultati dell'apprendimento e orientare il processo di apprendimento e il monitoraggio dei comportamenti disonesti);
- relativi alla **valutazione dell'occupazione**, ad ottimizzare la gestione dei lavoratori e l'accesso al lavoro autonomo (ad esempio, per pubblicare annunci di lavoro mirati, analizzare e filtrare le candidature e valutare i candidati);
- usati per determinare **l'accesso a servizi e a prestazioni pubblici e privati essenziali** (come, ad esempio, l'assistenza sanitaria);

Sistemi ad alto rischio

• finalizzati alla valutazione **dell'affidabilità creditizia** delle persone fisiche, alla **valutazione dei rischi finanziari**, nonché alla **determinazione dei prezzi in relazione ad assicurazioni sulla vita e assicurazioni sanitarie**;

• utilizzati nelle **attività di contrasto**, di gestione della **migrazione**, dell'asilo e del controllo delle frontiere, di **amministrazione della giustizia**, nonché nello **svolgimento dei processi democratici** e per la valutazione e **classificazione delle chiamate di emergenza.**

Non sono invece inclusi i sistemi di raccomandazione delle piattaforme online di dimensioni molto grandi (utilizzati dalle aziende online per suggerire agli utenti prodotti, servizi o contenuti che potrebbero essere di loro interesse) in quanto sono già disciplinati da altre normative (regolamento sui mercati digitali e regolamento sui servizi digitali).

L'elenco dei sistemi di IA ad alto rischio, che può essere modificato per allineare la normativa all'evoluzione tecnologica, **è allegato al regolamento**.

Sistemi ad alto rischio nell’ambito di frodi interne

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:

….

b) i sistemi di IA destinati a essere utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro.

Sistemi ad alto rischio nell'ambito di frodi in ambito scolastico

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

…

3. Istruzione e formazione professionale:….

d) i sistemi di IA destinati a essere utilizzati per monitorare e rilevare comportamenti vietati degli studenti durante le prove nel contesto o all'interno di istituti di istruzione e formazione professionale a tutti i livelli.

Sistemi ad alto rischio

High-risk Artificial Intelligence Systems (Title III, Annexes II and III)

Certain applications in the following fields:

1 **SAFETY COMPONENTS OF REGULATED PRODUCTS**

(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation

2 **CERTAIN (STAND-ALONE) AI SYSTEMS IN THE FOLLOWING FIELDS**

- ✓ Biometric identification and categorisation of natural persons
- ✓ Management and operation of critical infrastructure
- ✓ Education and vocational training
- ✓ Employment and workers management, access to self-employment
- ✓ Access to and enjoyment of essential private services and public services and benefits
- ✓ Law enforcement
- ✓ Migration, asylum and border control management
- ✓ Administration of justice and democratic processes

European Commission

Sistemi ad alto rischio

Requirements for high-risk AI (Title III, chapter 2)

Establish and implement **risk management** processes

&

In light of the **intended purpose** of the AI system

- Use high-quality **training, validation and testing data** (relevant, representative etc.)
- Establish **documentation** and design logging features (traceability & auditability)
- Ensure appropriate certain degree of **transparency** and provide users with **information** (on how to use the system)
- Ensure **human oversight** (measures built into the system and/or to be implemented by users)
- Ensure **robustness**, **accuracy** and **cybersecurity**

Rischi privacy

- mancata individuazione di un trattamento di dati personali:
  - per mancata conoscenza della normativa e della definizione di dato personale o di dato particolare
  - anche tramite inferenza
  - anche se i dati sono originariamente anonimi
- mancati adempimenti in conseguenza di un nuovo trattamento con particolare riferimento agli artt.12-14, 24, 25, 32
- accesso illecito ai dati personali (differenza fra accesso legittimo ed accesso lecito)
- profilazione dei dati personali (articolo 22)
- mancato rispetto dei principi, con particolare riferimento alla minimizzazione
- mancata visibilità delle elaborazioni intermedie (trasparenza black box) di dati personali, che limita il diritto di accesso ai dati

Peculiarità del rischio privacy

Il rischio in ambito privacy ha una doppia valenza:

- È un rischio per i diritti e le libertà delle persone fisiche, non un rischio aziendale e come tale non può essere gestito con i normali criteri
  - ad esempio non è possible accettare un rischio alto o trasferire il rischio
- Si traduce in un rischio aziendale in quanto comporta sanzioni e risarcimenti oltre ad un danno di immagine

Problemi: il rispetto della privacy

«dato personale»: **qualsiasi informazione** riguardante una persona fisica **identificata o identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

https://www.mrperugini.it/it/appendici-libri/

Categorie di DATI oggetto di trattamento: GDPR

- «dato personale»: **qualsiasi informazione** riguardante una **persona fisica identificata o identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un
- identificativo come il nome
- un numero di identificazione
- dati relativi all'ubicazione
- un identificativo online

Categorie di DATI oggetto di trattamento: GDPR

o a uno o più elementi caratteristici della sua identità

- fisica
- fisiologica
- genetica
- psichica
- economica
- culturale
- sociale;

Adempimenti privacy

Gli articoli più rilevanti del GDPR che trovano applicazione nei sistemi di IA sono i seguenti:

- Gli articoli 13 e 14 relativi al principio di trasparenza, da cui discende l'obbligo, per il titolare che intende trattare i dati, anche avvalendosi di processi decisionali automatizzati, di informare l'interessato di tale processo, fornendogli altresì informazioni significative sulla logica utilizzata". Tale norma è direttamente collegata al dibattito relativo al tema della explainability dell'IA.
- L'articolo 22 che sancisce il diritto dell'interessato a non essere oggetto di un processo decisionale automatizzato, compresa la profilazione, salvo che tale processo:
  - sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
  - sia autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento [...];
  - si basi sul consenso esplicito dell'interessato (base giuridica la cui dimostrazione è molto complessa in quanto il titolare è tenuto a dimostrare che tale consenso era libero e consapevole; inoltre il titolare deve sempre permettere la revoca del consenso, gestendo nel caso gli effetti della revoca stessa sul trattamento dei dati).

Adempimenti privacy

- L'articolo 25 in forza del quale tutti i processi che trattano dati personali devono sempre rispettare i principi della privacy by design e privacy by default: ne deriva che il rispetto dei principi per il trattamento dei dati deve essere tenuto in considerazione già in fase di progettazione e realizzazione del sistema di IA
- Gli articoli 44 e seguenti che dettano le regole per i trasferimenti dei dati personali al di fuori dello SEE, trattamento molto frequente nei sistemi di IA che operano sul cloud.

Adempimenti privacy

Opinion 4/20 dell'EDPS133 che evidenzia e analizza alcuni profili problematici del rapporto tra GDPR e IA:

1) opacità dell'IA che limita il principio di trasparenza a favore degli utenti che subiscono le decisioni dell'IA senza essere in grado di coglierne appieno le logiche; tale rischio, a volte, coinvolge anche gli stessi produttori dei sistemi;

2) limitazioni del campo di applicazione della legislazione UE esistente;

3) cambiamenti del funzionamento dei sistemi di IA;

4) incertezza riguardo l'attribuzione delle responsabilità

Adempimenti privacy

"Guidance on AI and data protection", pubblicata da ICO135 (autorità privacy inglese) nel 2020.

Tale guida analizza in maniera specifica i seguenti temi:

- la scarsa trasparenza degli algoritmi con cui i sistemi di IA arrivano a prendere decisioni;
- la sicurezza;
- la necessità e la proporzionalità dei trattamenti e la minimizzazione dei dati;
- l'esercizio dei diritti da parte dell'interessato

Rischi privacy
Profilazione (art. 22 GDPR)

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2. Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul consenso esplicito dell'interessato.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Rischi privacy
Profilazione (art. 22 GDPR)

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Linee-guida in materia di intelligenza artificiale e protezione dei dati

(COMITATO CONSULTIVO (CD. T-PD) DELLA CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI A CARATTERE PERSONALE (Convenzione 108)

Linee-guida per sviluppatori, produttori e fornitori di servizi

1.Gli sviluppatori, i produttori e i fornitori di servizi di IA dovrebbero adottare un approccio orientato ai valori nella progettazione dei loro prodotti e servizi, in linea con la Convenzione 108+, in particolare con l'art. 10, par. 2 di quest'ultima, e con gli altri strumenti pertinenti del Consiglio d'Europa.

2.Gli sviluppatori, i **produttori e i fornitori di servizi di IA dovrebbero valutare le possibili conseguenze negative delle applicazioni IA sui diritti umani e le libertà fondamentali** e, alla luce di tali conseguenze, adottare **un approccio precauzionale basato su appropriate misure di prevenzione e attenuazione dei rischi.**

Linee-guida in materia di intelligenza artificiale e protezione dei dati

(COMITATO CONSULTIVO (CD. T-PD) DELLA CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI A CARATTERE PERSONALE (Convenzione 108)

3.In tutte le fasi del trattamento, compresa la raccolta dei dati, gli sviluppatori, i produttori e i fornitori di servizi di IA dovrebbero adottare un approccio volto a **tutelare i diritti umani fin dalla progettazione** dei tali servizi ("human rights by design") ed **evitare qualsiasi potenziale pregiudizio (bias),** anche involontario o occulto, il rischio di discriminazione o altri effetti negativi sui diritti umani e le libertà fondamentali degli interessati.

4.Gli sviluppatori di IA dovrebbero **vagliare accuratamente la qualità, la natura, l'origine e la quantità di dati personali utilizzati**, **riducendo i dati inutili, ridondanti o marginali** durante lo sviluppo e le fasi di addestramento e poi monitorando l'accuratezza del modello man mano che viene alimentato con nuovi dati. L'uso di dati sintetici può rappresentare una soluzione atta a minimizzare la quantità di dati personali trattati dalle applicazioni IA.

Linee-guida in materia di intelligenza artificiale e protezione dei dati

5.Nello sviluppo e nell'utilizzo di applicazioni IA si dovrebbe tenere in adeguata considerazione il **rischio di impatti negativi** sugli individui e la società dovuto all'impiego di dati e **modelli algoritmici decontestualizzati.**

6.Gli s**viluppatori, i produttori e i fornitori di servizi di IA sono invitati a istituire e consultare comitati indipendenti di esperti** provenienti da più ambiti, nonché a collaborare con istituzioni accademiche indipendenti, che possono contribuire alla **progettazione di applicazioni IA fondate sui diritti umani e ispirate a considerazioni di natura etica e sociale,** nonché **all'individuazione di potenziali pregiudizi (biases).** Tali comitati potrebbero svolgere un ruolo particolarmente importante in quei settori ove assicurare la trasparenza e il coinvolgimento degli interessati può risultare più difficile a causa di interessi e diritti confliggenti, come negli ambiti della giustizia predittiva, della prevenzione e repressione dei reati.

Linee-guida in materia di intelligenza artificiale e protezione dei dati

7.Dovrebbero essere incoraggiate **forme partecipative di valutazione del rischio,** basate sul coinvolgimento attivo degli individui e dei gruppi potenzialmente interessati dalle applicazioni IA.

8.Tutti i prodotti e servizi dovrebbero essere progettati in modo tale da garantire il diritto delle persone di non essere sottoposte a una **decisione basata unicamente su trattamenti automatizzati** che abbia effetti significativi su di esse, **senza che le loro opinioni vengano prese in considerazione.**

9.Al fine di rafforzare la fiducia degli utenti, gli sviluppatori, i produttori e i fornitori di servizi IA sono invitati a progettare i loro prodotti e servizi in modo da **salvaguardare la libertà di scelta degli utenti rispetto all'utilizzo dell'IA, fornendo alternative praticabili alle applicazioni IA.**

Linee-guida in materia di intelligenza artificiale e protezione dei dati

10.Gli sviluppatori, i produttori e i fornitori di servizi di IA dovrebbero adottare forme di **vigilanza sugli algoritmi** che promuovano la responsabilizzazione di tutte le parti interessate durante l'intero ciclo di vita di tali applicazioni, al fine di garantire l'osservanza dei principi e delle norme in materia di **protezione dei dati e diritti umani**.

11.Gli **interessati dovrebbero essere informati se interagiscono con un'applicazione IA** e hanno il diritto di **ottenere informazioni sulla logica alla base dei trattamenti di dati che li coinvolgono**. Le informazioni da fornire dovrebbero comprendere le conseguenze derivanti dall'applicazione di tale logica.

12.Dovrebbe essere garantito il **diritto di opporsi** al trattamento basato su tecnologie che influenzano le opinioni e lo sviluppo personale degli individui.

Valutazione di impatto sistema IA

PREMESSA

L'entrata in vigore dell'IA ACT pone, in carico ai soggetti produttori, importatori, utilizzatori… di sistemi basati sull'IA una serie di adempimenti che si aggiungano, nel caso in cui il sistema tratta dati personali, a quelli previsti dalla normativa privacy e, a seconda delle circostanze, da altre normative (ad esempio dalla NIS2).

Fra questi adempimenti in prima istanza occorre valutare in particolare se il sistema di IA rientra fra le categorie dei sistemi IA:

- vietati, che quindi non possono essere utilizzati
- ad alto rischio, per i quali sono richiesti specifici requisiti ed adempimenti.

La seguente valutazione riguarda il sistema realizzato da XXXXXX per l'assistenza di tecnici ed installatore in merito ai propri prodotti

Il sistema è basato su ChatGPT, mediante una personalizzazione basato su dominio di conoscenza specifico basato sulla documentazione tecnica dei prodotti di XXXXXX.

Nel seguito verrà effettuata sia una valutazione del posizionamento del sistema di IA rispetto all'AI ACT e GDPR, sia rispetto ai principali principi previsti dall'IA.

POSIZIONAMENTO DEL SISTEMA RISPETTO ALL'AI ACT

SISTEMI DI IA VIETATI

Sono vietati, in sintesi, iseguenti sistemi:

• i sistemi di sfruttamento delle vulnerabilità delle persone e di utilizzo di tecniche subliminali ovvero deliberatamente manipolative o ingannevoli;

…..

SISTEMI AD ALTO RISCHIO

Tra i sistemi ad alto rischio rientrano, in particolare, quelli:

• di identificazione biometrica remota, categorizzazione biometrica e riconoscimento delle emozioni (al di fuori delle categorie vietate);

….

ESITI DELL'ANALISI DEL SISTEMA DI IA

	SI	NO
Sistemi vietati		x
Sistemi ad alto rischio		x

Descrizione del sistema di IA	Che tipo di sistema IA è in esame (es. Machine Learning, NLP, Reti Neurali)?	ChatGPT con personalizzazione di dominio
Finalità del sistema	Qual è lo scopo principale del sistema IA?	Offrire un'assistenza a tecnici ed installatori
Contesto d'uso	In quale contesto verrà utilizzato (es. settore sanitario, finanziario, industriale)?	Tutti i contesti in cui è richiesta l'installazione dei prodotti XXXXXX
Tipologia di dati trattati	Quali dati verranno utilizzati (es. dati personali, dati sensibili, dati pubblici)?	Dati tecnici dei prodotti Dati personali degli utenti del sistema, limitatamente a indirizzo di posta elettronica, password….

Identificazione degli utenti	Chi utilizzerà direttamente o indirettamente il sistema (es. utenti finali, dipendenti)?	Tecnici ed installatori dei prodotti XXXXX
Coinvolgimento delle parti interessate	Gli stakeholder rilevanti sono stati consultati e coinvolti nel processo?	È stato coinvolto il management dell'azienda
Benefici attesi	Quali vantaggi si prevede che il sistema di IA fornisca ai vari stakeholder?	Per gli utenti il sistema facilita la configurazione degli impianti nel loro insieme ed i loro componenti Per l'azienda il sistema dovrebbe diminuire il ricorso all'assistenza tecnica e dare un'immagine di azienda attenta alla evoluzione tecnologica anche per quanto riguarda i servizi di pre e post vendita.

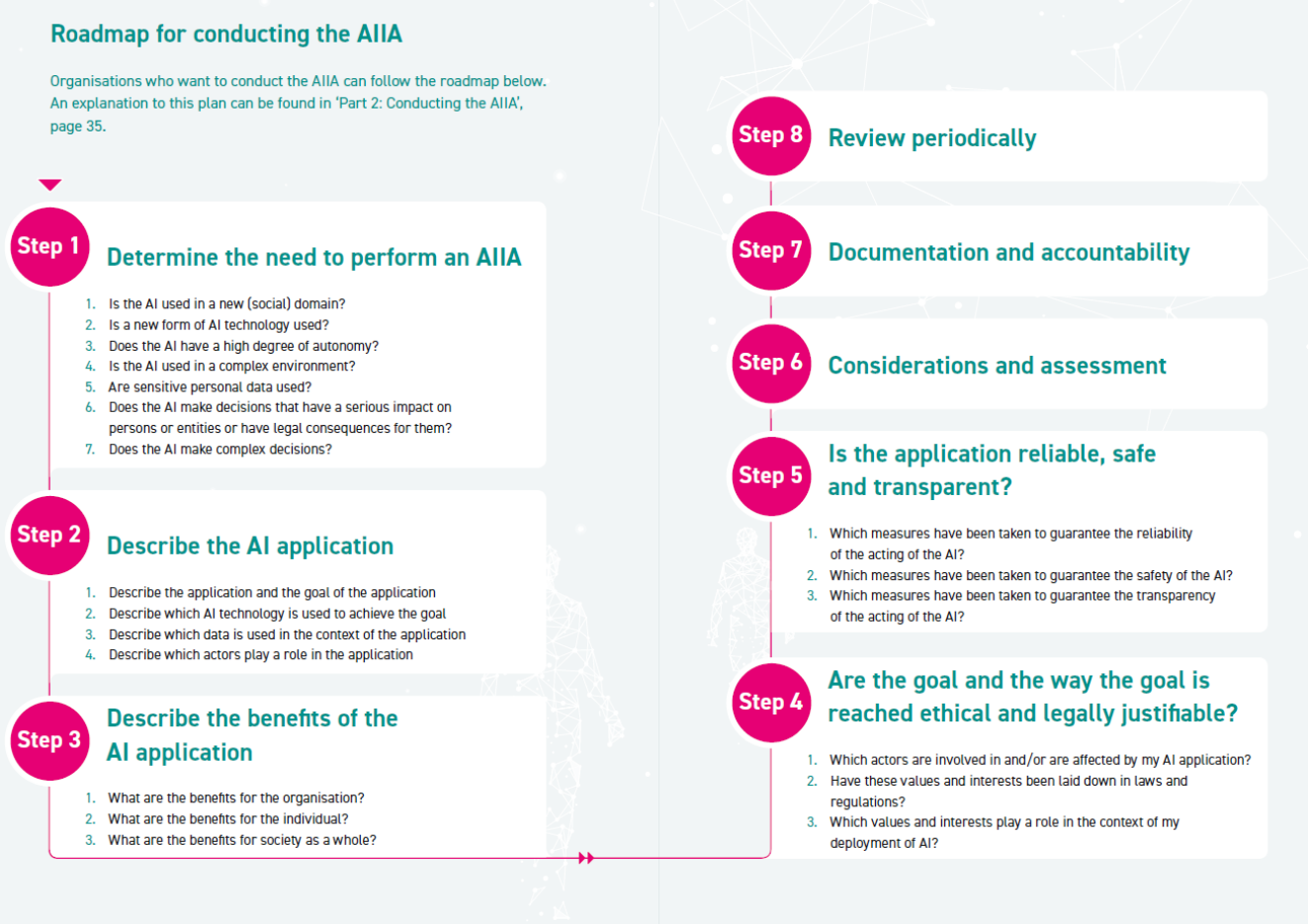
IA Impact assessment (AIIA)

Artificial Intelligence Impact Assessment

THINK BEFORE YOU PRINT

ECP Platform for the Information Society

IA Impact assessment (AIIA)



4 Step 4

Are the goal and the way the goal is reached ethical and legally justifiable?

In questa fase si determina se l'obiettivo e, più specificamente, il modo in cui viene raggiunto è eticamente e legalmente giustificabile.

Il punto di partenza della vostra analisi è il quadro giuridico esistente.

Ma questo quadro può essere incompleto o inadeguato per una buona valutazione etica.

Ecco perché si identificano i valori e gli interessi in gioco nella diffusione dell'intelligenza artificiale.

In particolare, esaminate i possibili rischi della vostra applicazione.

Identificare questi rischi è importante perché ti fa vedere cosa potresti migliorare nella progettazione e nell'implementazione dell'IA.

Le scelte che fai (escluderemo o limiteremo i rischi, quanto rischio residuo accettiamo, accettiamo che la nostra applicazione crei rischi?) sono i compromessi etici dell'organizzazione.

La lente etica con cui si guarda all'applicazione gioca qui un ruolo importante.

4 Step 4

Are the goal and the way the goal is reached ethical and legally justifiable?

Per valutare se l'uso dell'IA è etico, è necessario determinare quali valori e interessi potrebbero essere in gioco nella vostra implementazione dell'IA.

A tal fine puoi porti le seguenti domande:

Quali attori sono coinvolti e/o sono interessati dalla mia applicazione AI?

I valori (onestà, uguaglianza, libertà) sono ideali e motivazioni per cui lottano una società e gli attori al suo interno.

Nell'Allegato 1 si trova il "Codice di condotta sull'intelligenza artificiale" con i principi etici del Gruppo europeo per l'etica nelle scienze e nelle nuove tecnologie, che può fornire linee guida per l'analisi dei valori rilevanti.

Dato che i valori sono astratti, è spesso difficile valutare se l'impiego dell'intelligenza artificiale sia in linea con i valori di una società.

In generale, agire in violazione dei valori significa che gli interessi degli attori vengono danneggiati direttamente o indirettamente (vedi figura 3).

4 Step 4

Are the goal and the way the goal is reached ethical and legally justifiable?

Ad esempio, compromettere il valore “uguaglianza” può significare che una persona o un gruppo sono discriminati.

Ecco perché tradurre i valori in interessi può dare una direzione alla valutazione se un’applicazione di intelligenza artificiale sia etica o meno.

Gli attori sociali hanno interessi diversi.

Attraverso l’intelligenza artificiale, le relazioni di potere esistenti possono cambiare e gli interessi degli attori possono essere danneggiati o rafforzati.

Le applicazioni dell’intelligenza artificiale possono quindi influenzare gli interessi a diversi livelli.

Ad esempio, l’impiego dell’intelligenza artificiale può influenzare in modo molto specifico gli interessi di un individuo (ad esempio, la violazione della sua privacy), ma l’impiego dell’intelligenza artificiale può influenzare anche gli interessi e le relazioni a livello sociale.

Si pensi, ad esempio, ai cambiamenti nell’occupazione attraverso l’impiego dell’intelligenza artificiale.

4 Step 4

Are the goal and the way the goal is reached ethical and legally justifiable?

In questa AIIA l'accento è posto sugli interessi dell'individuo.

Questi corrispondono in larga misura ai diritti fondamentali tradizionali (diritto alla libertà di espressione, alla privacy, ecc.) e ai diritti sociali fondamentali (diritto all'istruzione, al lavoro, ecc.).

Questi valori e interessi sono stati stabiliti in leggi e regolamenti?

Standard, valori e principi etici all'interno di una società sono (parzialmente) cristallizzati in leggi e codici di condotta.

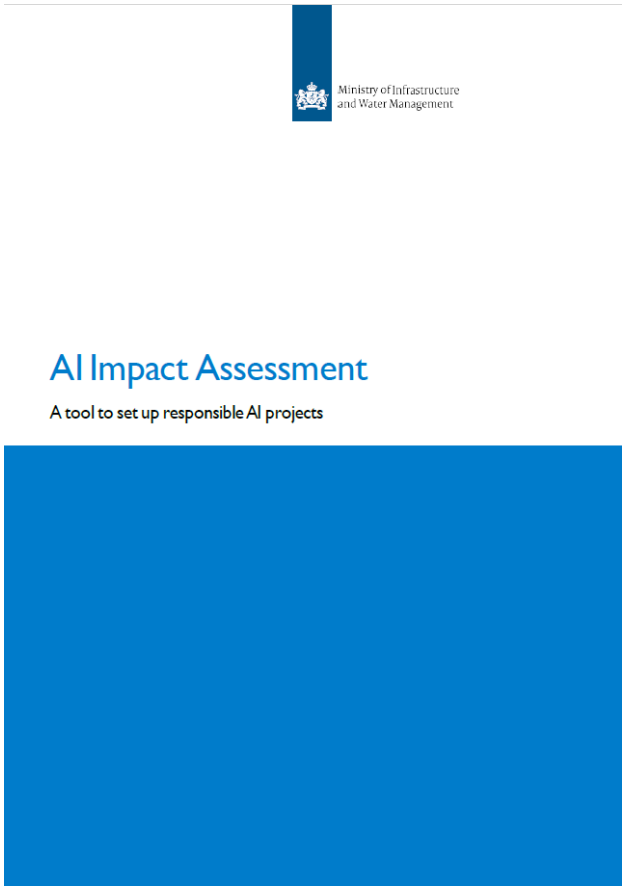
L'obiettivo di queste regole è promuovere il benessere, proteggere i diritti (umani) e organizzare la società.

Queste leggi e regolamenti costituiscono il quadro concreto all'interno del quale deve rimanere la tua candidatura.

Nella misura in cui i quadri non sono chiari o sono incompleti, la progettazione della vostra applicazione deve essere in linea con i valori che si applicano nella società.

Nella misura in cui la vostra richiesta lede gli interessi di terzi, dovete essere in grado di motivare il motivo per cui ciò è giustificato.

Altre metodologie per la valutazione di impatto: Olanda



- Explanatory Notes
  - Guidelines for completion
  - Questionnaire
- Introductory questions
  - Purpose of the system
  - Role within the organisation
- Fundamental rights & fairness
  - Basic rights
  - Bias
  - Stakeholder participation
- Technological robustness
  - Accuracy
  - Reliability
  - Technical implementation
  - Reproducibility
  - Explainability
- Data governance
  - Data quality and integrity
  - Privacy and data protection
- Risk management
  - Risk management
  - Alternative procedure
  - Hacking attacks and corruption
- Accountability
  - Communication
  - Verifiability
  - Archiving
  - Climate adaptation
- Appendices
  - Definitions
  - Who is who
  - Who does what

Reproducibility

t 4. Is the **ai system reproducible**? Has a process been set up to measure this?

Reproducibility refers to the registration of, e.g., which data has been used, the model development process, whether changes in the data have been tracked, whether the same **input (data)** produces consistent results, and whether certain situations or conditions may affect the **output (data)**. Reproducibility is about training, validation, and testing.

Reproducibility is closely related to traceability. The main purpose of **traceability** is the proper documentation of the data sets and processes. Data version management, the algorithm, and the training play a key role in this respect.

to 13. Can you reconstruct, now or in the future, the **output (data)** produced (i.e., have previous versions of the **model**, data sets, and conditions been saved through version management)?

to 14. Can the model be reconstructed on the basis of the given **hyperparameters** and a fixed seed?

to 15. Can the outlines of the **ai system** be reproduced on the basis of documentation?

to 16. How are modifications during the lifespan of the system being documented?

Explainability

t 5. Is the **ai system** sufficiently **explainable** and interpretable to the **developers**?

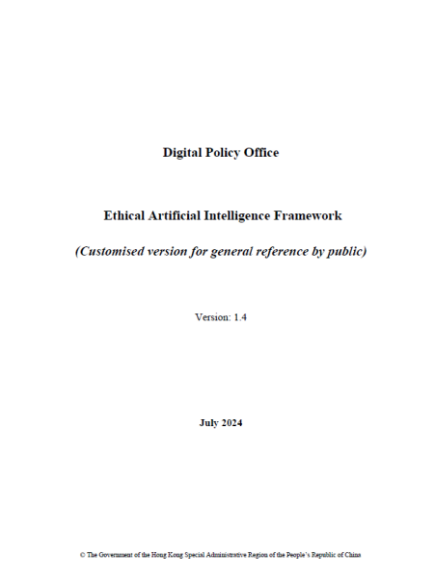
Technical **explainability** refers to the ability to understand both technical processes and related human decisions. Furthermore, the design choices made must be clear, as must the rationale underlying the use of the **ai system**. Cf. "Accountability" for explainability vis-à-vis **involved parties**.

to 17. During he AI system development process, how have you considered the explainability of the model?

to 18. To what extent can the particular way in which the AI system operates be explained to an external AI expert (cf. "Explainability")?

to 19. Has the expertise required for maintenance ofthe AI system been documented?

Altre metodologie per la valutazione di impatto: Hong Kong



Digital Policy Office

Ethical Artificial Intelligence Framework

(Customised version for general reference by public)

Version: 1.4

July 2024

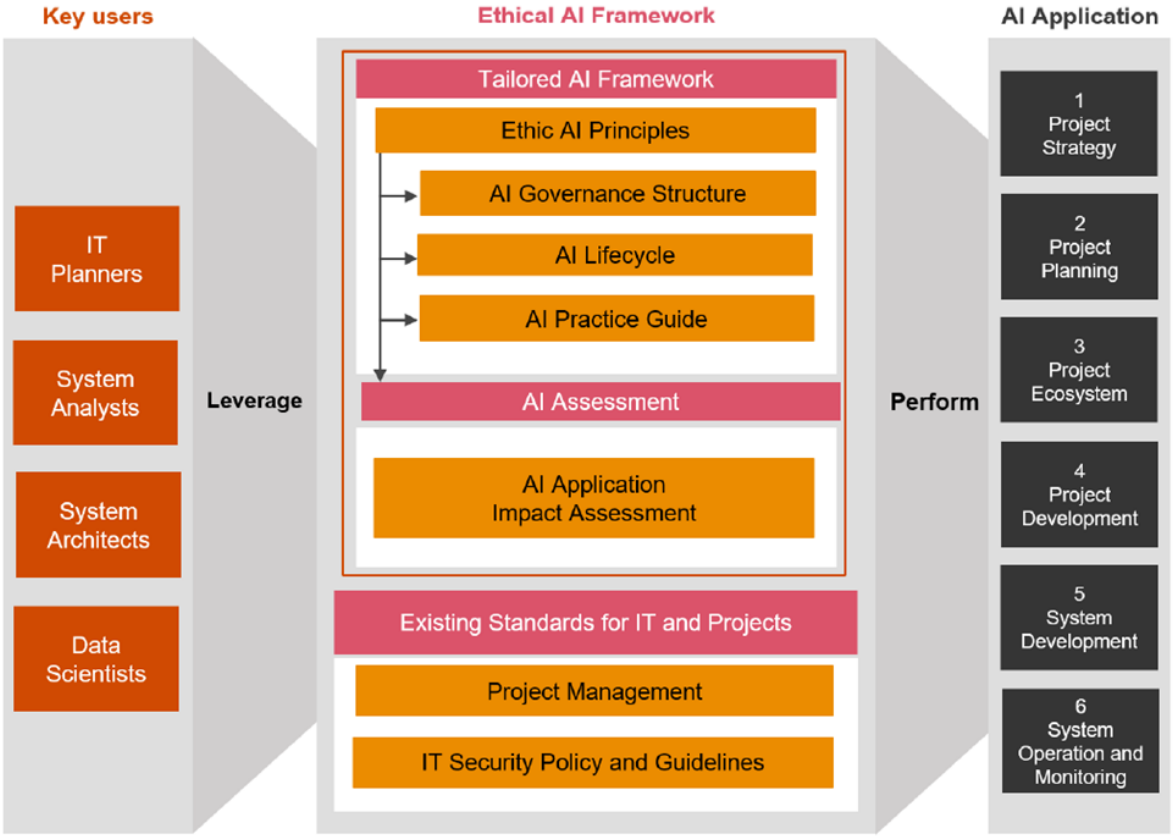


Figure 1: Overview of the Ethical AI Framework

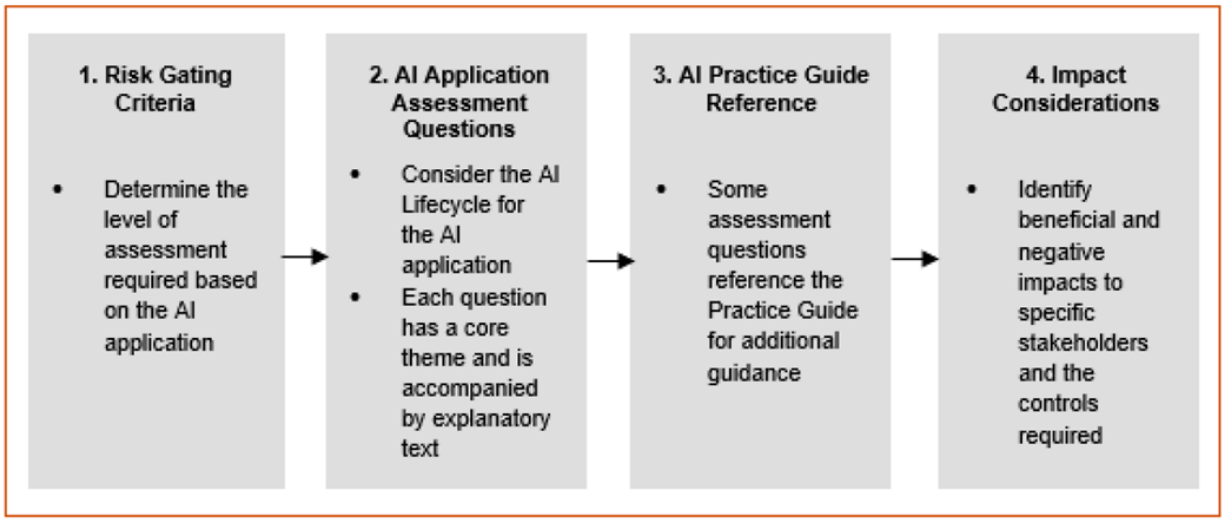


Figure 5: AI Application Impact Assessment Components

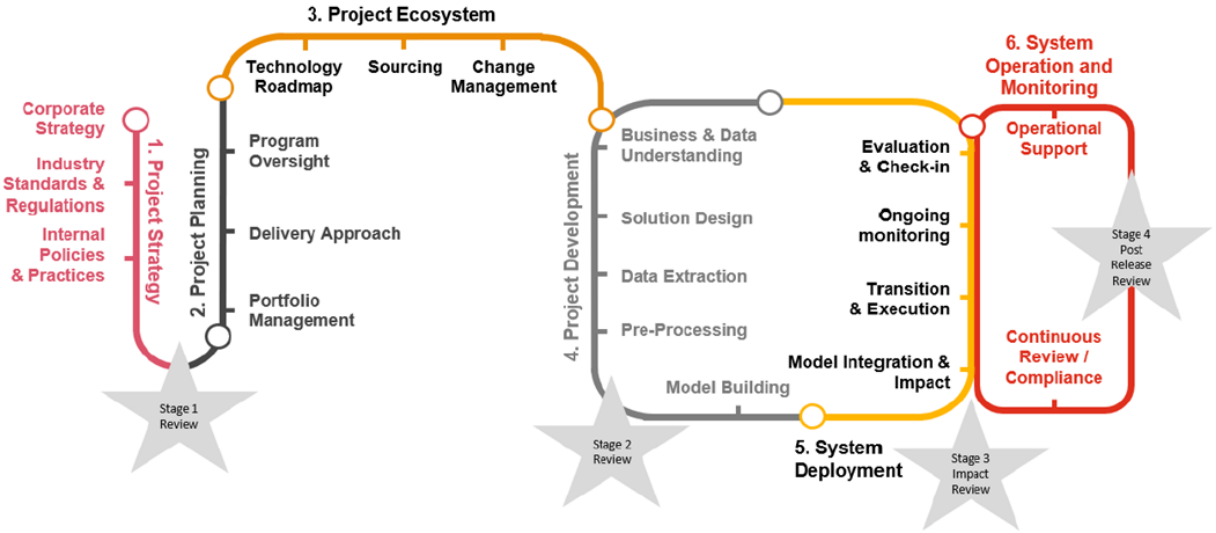


Figure 6: Stages for AI Application Impact Assessment

APPENDIX C – AI APPLICATION IMPACT ASSESSMENT TEMPLATE

Note

Please refer to Section 5.1.1.1 "Process for Completing AI Application Impact Assessment" for details on the process to complete the AI Application Impact Assessment

Legend

- Text covers the core questions that are to be addressed in a qualitative manner
- Italicised text is added context to support the core question and should be used as an aid to provide the qualitative answer

Risk Gating Criteria

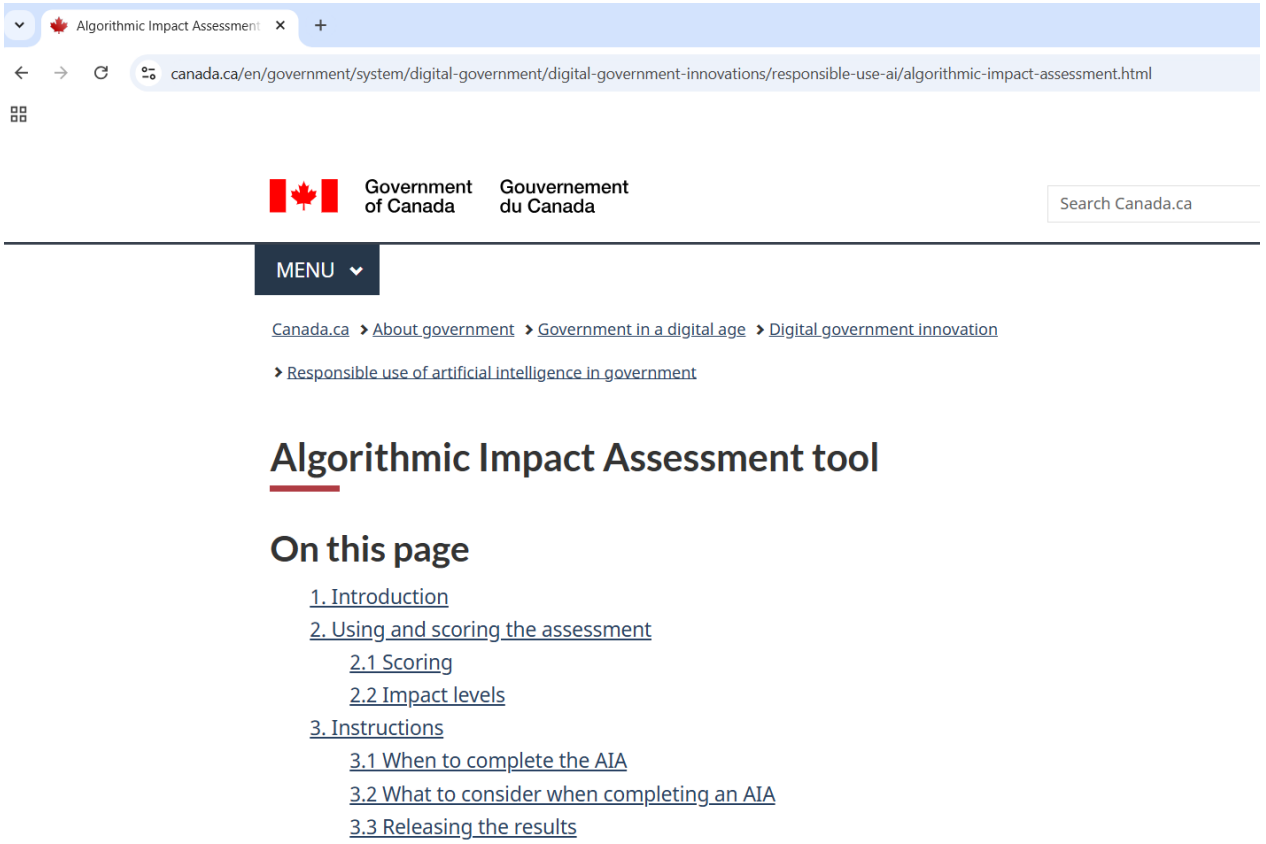
If one or more of the risk gating questions below are triggered, (i.e. the answer is "yes" for the question), the AI Application Impact Assessment should be subject to IT Board/CIO review before project commencement. Please refer to Section 5 "AI Assessment" for details.

Question	Context
a - Is the AI application within an area of intense public scrutiny (e.g. because of privacy concerns) and/or frequent litigation?	*For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy. Examples of such applications include Smart Cities applications:* • *Smart Lighting – intelligent weather adaptive street lighting* • *Smart Traffic Management – Monitoring of vehicles and pedestrian* • *Smart Parking – Monitoring of parking spaces* *Therefore, this requires a IT Board/CIO review of the AI Application Impact Assessment. The combination of facial recognition and a new, sensitive use or potentially controversial use should be considered.*
b - Is the AI application applied in a new (social) domain (i.e. where AI has not been used in Hong Kong)?	*For example, an AI application that is used for the first time in healthcare while previously, it was only used for marketing purposes. Due to the change of domain, it is possible that the AI application will raise (new) ethical questions. When the AI application takes place in a sensitive social area, the risks and the ethical issues are potentially greater. Think of topics such as care, safety, the fight against terrorism or education. Think of vulnerable groups such as children or the disabled.*
c (i) Does the AI application have a high degree of autonomy?	*The more an AI application acts independently with increased freedom to make decisions, the more important it is to properly analyse the consequences of this autonomy. In addition to the freedom to make decisions,*

AI Application Impact Assessment Questions

A. Purpose of AI Application and Accountability	Practice Guide Reference/Responsibility	Assessment results/proposed mitigation plan
1 - What is the business need/goal/objective for this AI and data activity? What is the defined clear purpose for developing the identified AI application (e.g. operational efficiency or cost reduction)? How can the expected benefits outweigh potential risks? What are the acceptance or success criteria for this planned activity? *Does the AI application fit within a larger theme of work that is currently being contemplated or undertaken? Does this initiative fit into your AI and/or Data strategy?*	Section 4.1.2.1: • Map AI projects to the organisation objectives • Select and prioritise AI projects IT Planners/Executives, Business Users	
2 - What are the objectives of this initiative for each group of stakeholders (each entity or group of individuals participating and/or being impacted by the data or technology use scenario)? Explain the objectives in terms of the explicit outcomes/goals and how these outcomes map to the Ethical AI Principles or other external positive justification/validation that is generally accepted by society. Describe the risks that may be created for each stakeholder. • Clearly state the problem that is to be solved. • Clearly state the measurable goal or outcome of the project • Who are the stakeholders who are impacted by this AI application? • What is the interest (high-level) for ALL impacted stakeholders? • What are the risks to affected stakeholders? (To be analysed and documented in question 3) Identify the relevant Ethical AI Principles for the AI application – Confirm that this AI Application does not trigger any of the risk gating criteria (see above).	Section 4.1.2.1: • Map AI projects to the organisation's objectives • Select and prioritise AI projects IT Planners/Executives, Business Users	

Altre metodologie per la valutazione di impatto: Canada



India

Problem Definition and Scoping	
Consideration	Mitigation Strategy
Have you assessed the potential 'degree of harm' from the AI system being deployed in the short term and the long term?	Constitute an ethical committee consisting of sector experts, social scientists, data and other relevant experts to assess the potential degree of harm due to development and deployment of the AI system
	The group may recommend guidelines to follow to ensure social risks are appropriately managed
	Document the concerns identified and plan appropriate measures and incentive mechanisms to mitigate them
Is there an appropriate grievance redressal mechanism for stakeholders who may be impacted by the AI system?	Establish a grievance mechanism for anyone impacted by the AI system
	Document the measures taken to make stakeholders aware of the grievance redressal mechanism through appropriate channels
	The support mechanism should be easily accessible, ideally at no additional cost

India

Have you engaged with the stakeholders to understand the degree of explainability that may be required for individual decisions?	**Identify stakeholders for the AI system and spe in the procurement document**
	Engage with the stakeholders to understand the explanation that may be required
Have you identified mechanism to handle errors in decision by the AI system?	In the procurement document, specify the role a vendor
	Specify individual roles and responsibilities and, if a part of the work is subcontracted, identify roles and responsibilities of each agency
	Specify who has the right to make changes to the system during development, launch and post launch stage to manage any social risks
	If the potential degree of harm for a decision is expected to be high, have appropriate mechanisms in place so stakeholders can contest and humans can get involved in the decision making process
Can the terms of use allow for public auditing to understand behaviour and identify risks without causing unintended consequences	Ensure the terms of service allows for audit by research institutions, audit agencies to probe the system, identify bias, risks and review behaviour
	Consult legal counsel and data science experts to identify means to allow for audit without exposing sensitive and personal information or causing any other unintended harm to the system and its stakeholders
	If data must be made available for audit, ensure steps are taken to expose the data in a manner that preserves privacy, security and protects legal rights of associated people or businesses

Grazie per l'attenzione

giancarlo.butti@promo.it

gbutti@clusit.it

338 9230742