Privacy Consulting

L'IMPATTO SUL GDPR DEL AI ACT

Linux Day 2023

28 ottobre 2023

Università degli Studi di Palermo
Teatro Gregotti

Privacy Consulting

Dott. Adriano Bertolino

Delegato Regionale per la Sicilia

ASSO DPO
Associazione Data Protection Officer

Data Protection Officer | Privacy & Cybersecurity Advisor

assodpo.it

Mi occupo dei temi della privacy e della data protection dal dal 2004, in riferimento alla compliance alle norme nazionali (Codice della Privacy) e comunitarie (GDPR 2016/679), fornendo consulenza tecnico-giuridica, manageriale e formazione in materia di protezione dei dati personali e con particolare attenzione alla cybersecurity e alla sicurezza delle informazioni, per Pubbliche Amministrazioni, multinazionali e imprese operanti in tutti i settori di mercato, incluse Startup e PMI Innovative.

BUREAU VERITAS 1828

Certificato CEPAS-Bureau Veritas
Responsabile protezione dati n° 0449
Lead Auditor ISO-IEC 27001:2013 n° 166

Certificato TÜV Italia
Privacy Officer n° CDP_272

TÜV SÜD

Privacy Consulting

10 ANNI DI ASSO DPO

Da anni ASSO DPO sostiene e promuove l'attività dei Data Protection Officer, dei Consulenti della Privacy e dei Chief Privacy Officer, attraverso il confronto e lo scambio di informazioni tra i suoi associati. L'Associazione offre numerosi forum di discussione, eventi e workshop per favorire la condivisione di esperienze e l'apprendimento reciproco tra i professionisti del settore.

In questo modo l'Associazione Data Protection Officer contribuisce a sviluppare una comunità di professionisti qualificati e competenti nella gestione della privacy e della protezione dei dati.

9 congressi internazionali

30 soci onorari

+870 follower Facebook

675 associati

450 professionisti certificati UNI 11697

+2500 membri LinkedIn

10 Anniversary
ASSO DPO
Associazione Data Protection Officer

assodpo.it

Dott. Adriano Bertolino

I PRINCIPALI OBIETTIVI

ASSO DPO
Associazione Data Protection Officer

assodpo.it

1. Promuovere la ricerca e la diffusione delle conoscenze in materia di controlli di legittimità e di conformità alla normativa Privacy, etica ed Information Technology.

2. Confrontarsi sulle tematiche relative alla normativa in materia di Privacy ed alla sua applicazione, interpretazione ed evoluzione.

3. Sviluppare soluzioni condivise ai problemi applicativi posti dalla normativa in materia di Privacy e, in particolare, ai problemi connessi all'operatività della funzione nelle aziende e negli enti, eventualmente anche mediante l'elaborazione di "standard" e "best practice".

4. Promuovere la valorizzazione del ruolo di Data Protection Officer e favorirne la crescita professionale.

LE SEDI TERRITORIALI

12	Delegati regionali
8	Referenti provinciali

Siamo presenti in **15** regioni

- Piemonte
- Lombardia
- Veneto
- Emilia Romagna
- Toscana
- Marche
- Campania
- Friuli Venezia Giulia
- Umbria
- Abruzzo
- Lazio
- Molise
- Calabria
- Sicilia
- Sardegna

CEDPO

www.cedpo.eu

Dal 2018 ASSO DPO, quale unica associazione italiana, fa parte di CEDPO | Confederation of European Data Protection Organisations, storica confederazione delle associazioni europee dei data protection officer che lavora a fianco delle realtà più grandi e importanti d'Europa del settore protezione dei dati.

La collaborazione con CEDPO contribuisce attivamente al raggiungimento degli obiettivi dell'associazione e a tenere rapporti con le istituzioni europee.

Austria | ARGE Daten

Francia | AFCDP

Germania | GDD

Irlanda | ADPO

Italia | ASSO DPO

Paesi Bassi | NGFG

Polonia | SABI

Romania | ASCPD

Portogallo | AEPD

Spagna | APEP

assodpo.it

Privacy Consulting

L'IMPATTO SUL GDPR DEL A.I.

Argomenti

- *Nozioni del Regolamento UE 2016/679 (GDPR);*
- *Nozioni del A.I. ACT;*
- *Problematiche e rischi dell'IA*
- *Privacy e Intelligenza Artificiale;*
- *Rischi sui dati personali nell'AI;*
- *Compliance organizzativa e tecnica dell'AI al GDPR;*
- *Anonimi e Dati sintetici.*

Dott. Adriano Bertolino

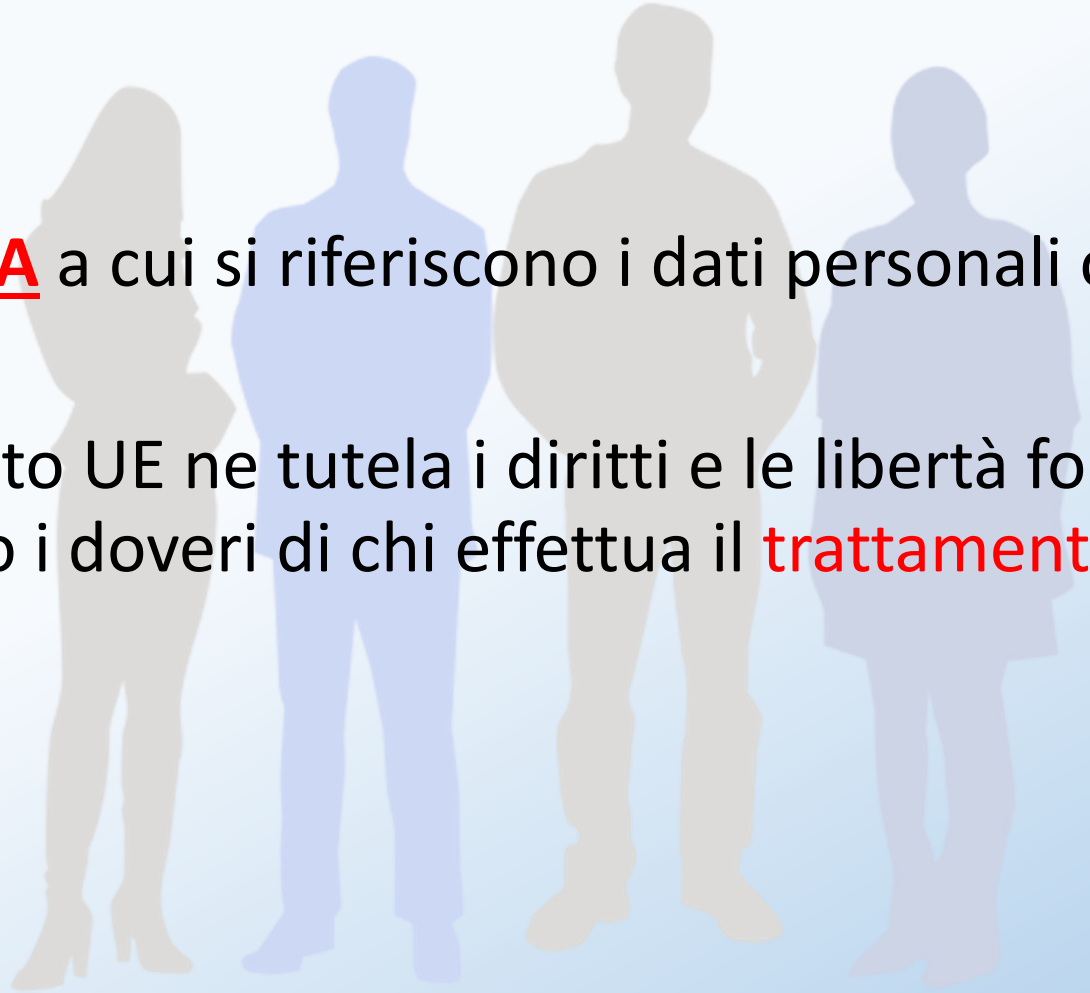
REGOLAMENTO (UE) 2016/679

Privacy Consulting

Disciplina unica applicata in tutti gli Stati membri UE a **protezione dei diritti dei cittadini** europei, e di coloro che risiedono nell'Unione Europea

Privacy Consulting

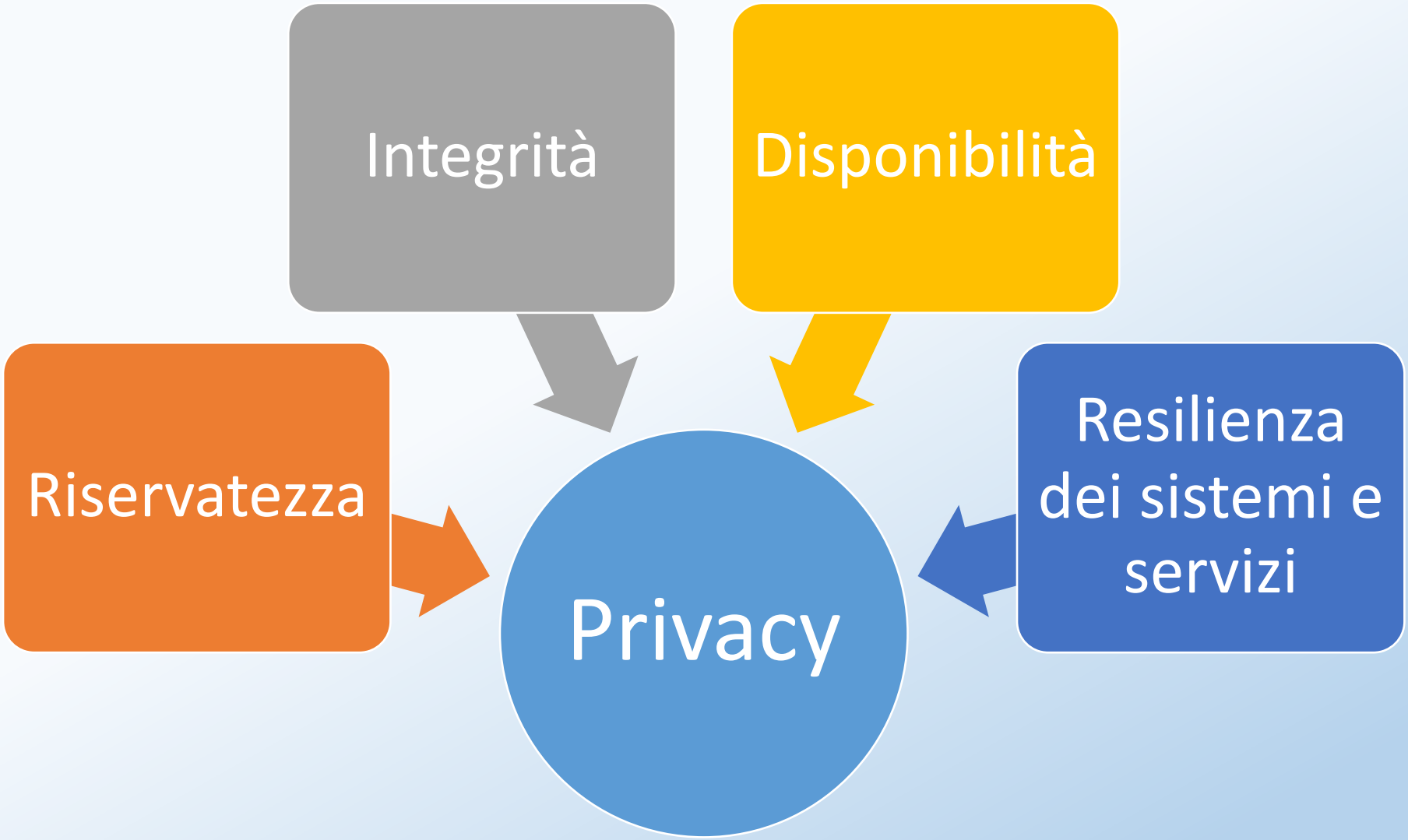
L'INTERESSATO



La **PERSONA FISICA** a cui si riferiscono i dati personali oggetto di trattamento

Il Regolamento UE ne tutela i diritti e le libertà fondamentali, a cui corrispondono i doveri di chi effettua il trattamento di **dati personali**

Come intende la norma la «PRIVACY»



Dott. Adriano Bertolino

…LA SUCCESSIONE DEGLI EVENTI

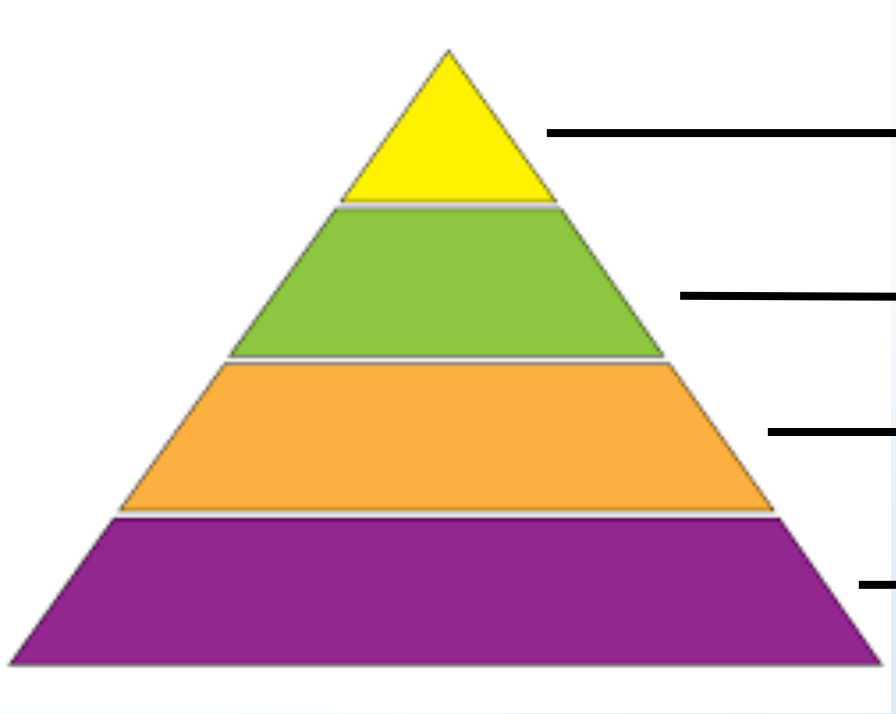
A.I. ACT

Per Intelligenza Artificiale si intende un «Software che può generare risultati sotto forma di contenuti, previsioni, ipotesi, raccomandazioni, o decisioni che influenzano gli ambienti con cui interagiscono».

[art. 3 – AI ACT]

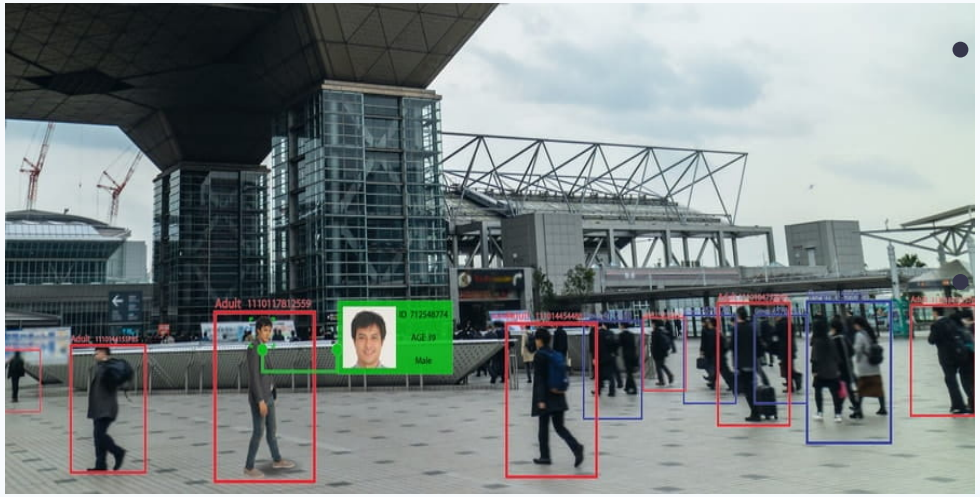
APPROCCIO BASATO SUL RISCHIO

L'A.I. Act si fonda su un approccio proporzionato basato sul rischio, prevedendo oneri e gradi di tutele crescenti all'aumentare del livello di rischio



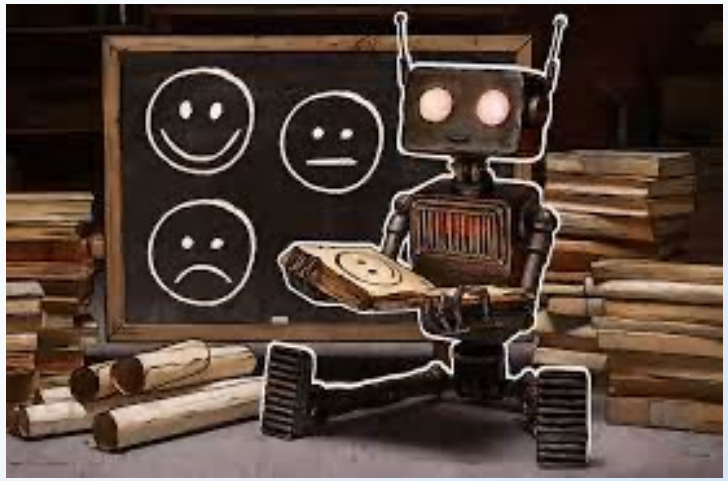
- Sistemi a rischio inaccettabile
- Sistemi ad alto rischio
- Sistemi a rischio limitato
- Sistemi a rischio minimo o nullo

Sistemi IA a rischio INACCETTABILE



- **manipolazione comportamentale cognitiva di persone o gruppi vulnerabili specifici,** come i bambini;

classificazione sociale delle persone in base al comportamento, al livello socio-economico e alle caratteristiche personali;



- sistemi di **polizia predittiva basati su profilazione, posizione o comportamento criminale pregresso**;

- **sistemi di identificazione biometrica in tempo reale e a distanza**, come il riconoscimento facciale.

Dott. Adriano Bertolino

Sistemi IA ad ALTO rischio

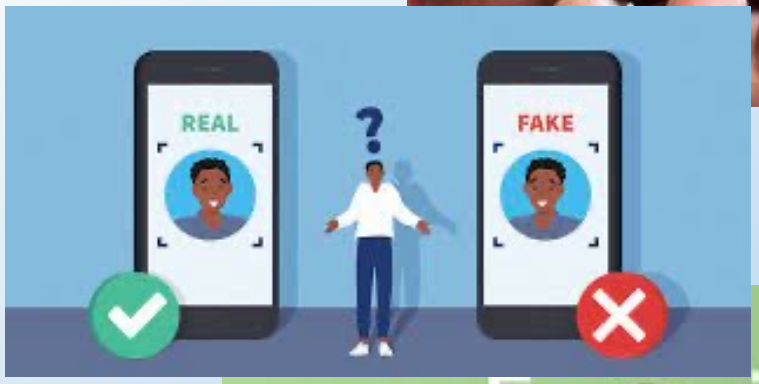
La *predisposizione di una valutazione dei rischi, la garanzia sulla tracciabilità dei risultati, e tutta la* **documentazione adeguata contenente tutte le informazioni necessarie per le Autorità**

- **infrastrutture critiche** (ad esempio i trasporti, energia, gas, acqua), che potrebbero mettere a rischio la vita e la salute dei cittadini;
- **istruzione o formazione professionale**, che può determinare l'accesso all'istruzione e al corso professionale (ad esempio, il punteggio degli esami);
- **componenti di sicurezza dei prodotti** (ad esempio applicazione di IA in chirurgia robotizzata);
- **gestione dei lavoratori e accesso al lavoro** (ad esempio software di selezione dei CV per le procedure di assunzione o valutazione performance);
- **applicazione della legge** che può interferire con i diritti fondamentali delle persone (ad esempio valutazione dell'affidabilità delle prove).

Sistemi IA a rischio LIMITATO

ESEMPI:

- Deepfake
- Chatbot



Dovranno essere adottati sistemi di trasparenza che consentano agli utenti di prendere decisioni informate

Sistemi IA a rischio MINIMO

Videogiochi abilitati per l'IA

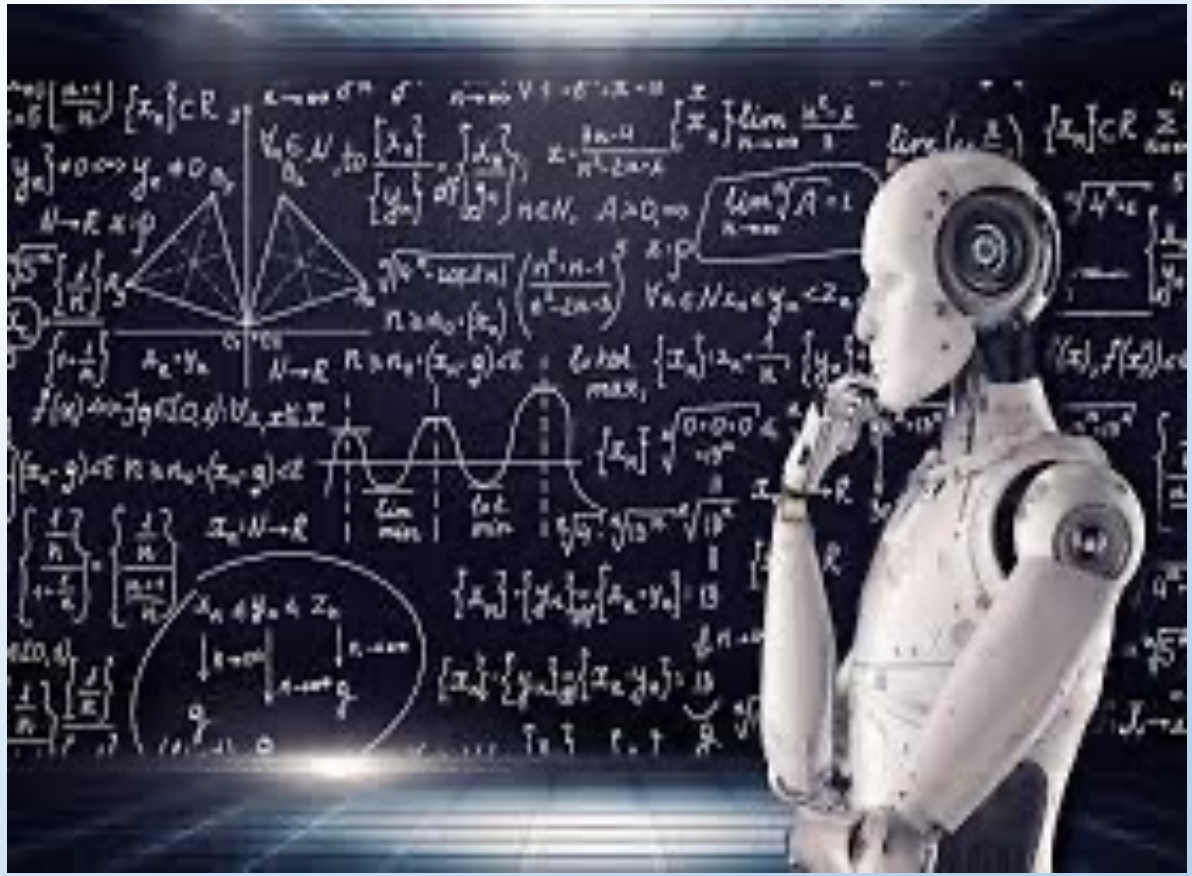
Filtri antispam o sicurezza informatica

non sono previsti obblighi ed è consentito il libero utilizzo dell'IA

PROBLEMATICHE E RISCHI DELL'IA: IL MACHINE LEARNING

- Le capacità di analisi di una IA dipendono soprattutto:
  - dal modello decisionale adottato;
  - dal *training* effettuato;
  - dalla capacità computazionale del computer che la esegue.

- Maggiore sarà il data set di training, in termini di qualità e quantità dei dati (Big Data), migliore sarà la capacità di analisi dell'IA.



PROBLEMATICHE E RISCHI DELL'IA: ESEMPI

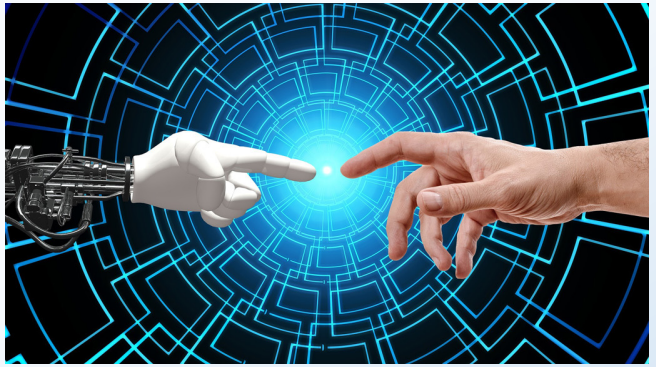
- ***Bias***: errori decisionali sistematici
  - per cui un allenamento effettuato con dati non rappresentativi, allenerà l'IA a prendere decisioni non corrette

- ***Black Box:***
  - è difficile, e a volte impossibile, comprendere il perché l'IA abbia preso una determinata decisione

- ***Discriminazione****:*
  - *il processo decisionale dell'algoritmo è caratterizzato dallo stesso pregiudizio che si applica alle decisioni umane e influenzato dalla cultura, dai punti di vista e dagli stereotipi di chi li "alimenta"*

Privacy Consulting

Privacy e Intelligenza Artificiale

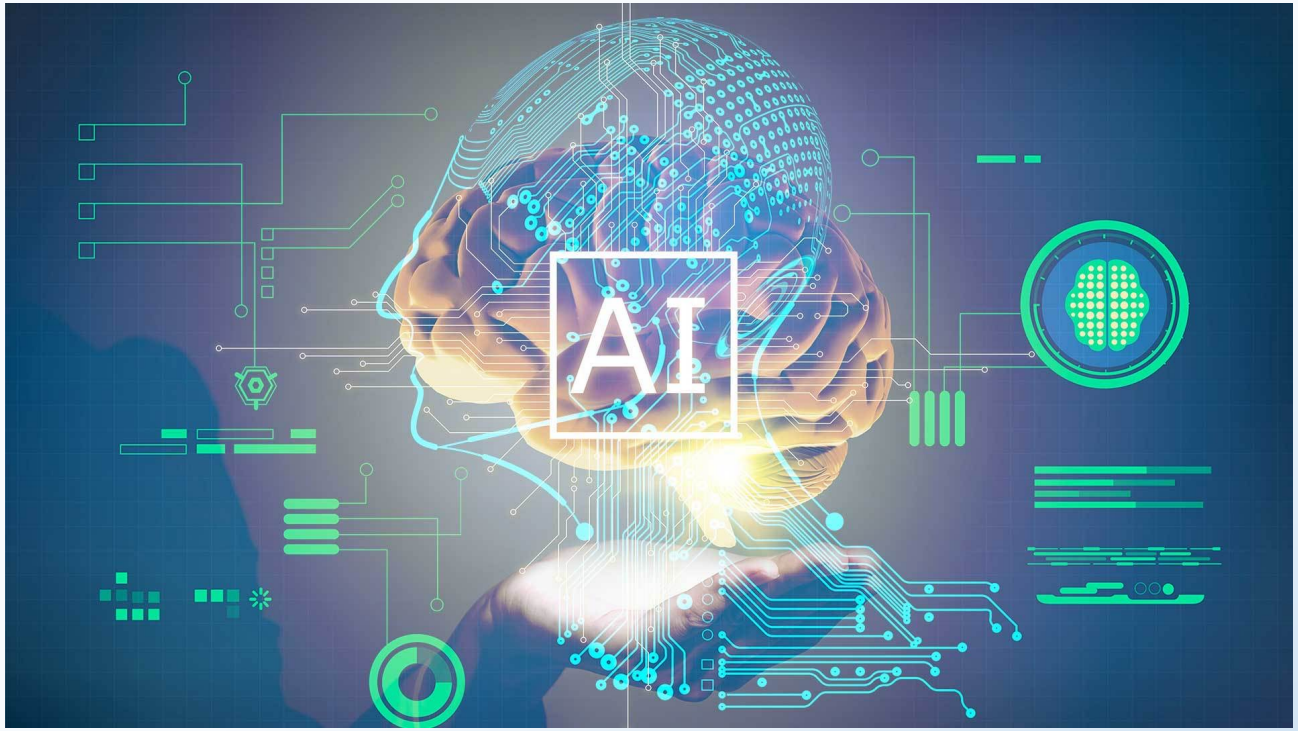


European Data Protection Supervisor – Opinion 4/2020

‘‘L’IA, come qualsiasi altra tecnologia, costituisce un semplice **strumento** e dovrebbe essere progettata per servire l’umanità. L’IA […] presenta vantaggi e svantaggi e le autorità pubbliche e le entità private dovrebbero valutare caso per caso se un’applicazione dell’IA sia l’opzione migliore per raggiungere i propri obiettivi.’’

Privacy Consulting

L'IMPATTO DELL'INTELLIGENZA ARTIFICIALE NELLA PROTEZIONE DEI DATI PERSONALI



Quando sono trattati dati personali nell'uso di tecnologie di Intelligenza Artificiale?

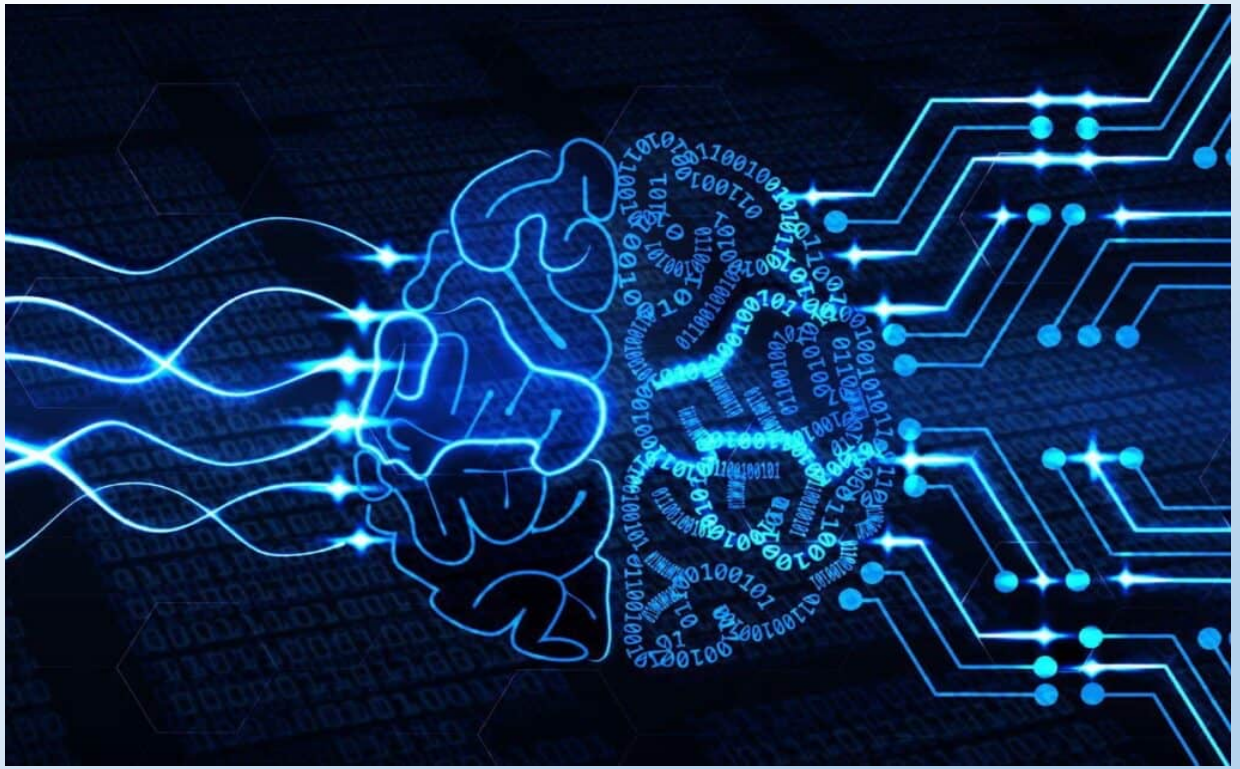
- Nell'addestramento attraverso data set reali o sintetici;
- Nella distribuzione del prodotto e nell'interazione con l'utilizzatore;
- Nei modelli di AI ad apprendimento continuo;

Dott. Adriano Bertolino

Privacy Consulting

FONTI DEI DATI PERSONALI

- Dati raccolti da internet (web scraping)
- Forniti spontaneamente (chatbot);
- Forniti da Terzi (broker dati o dati aziendali interni);
- Dati disponibili agli sviluppatori per l'addestramento (data set).



RISCHI PER GLI INTERESATI

Dati non accurati ed inesatti ->

- Discriminazione (bias)

Diffusione dati di training ->

- Limitazione della finalità

Impossibile controllare la tracciabilità ->

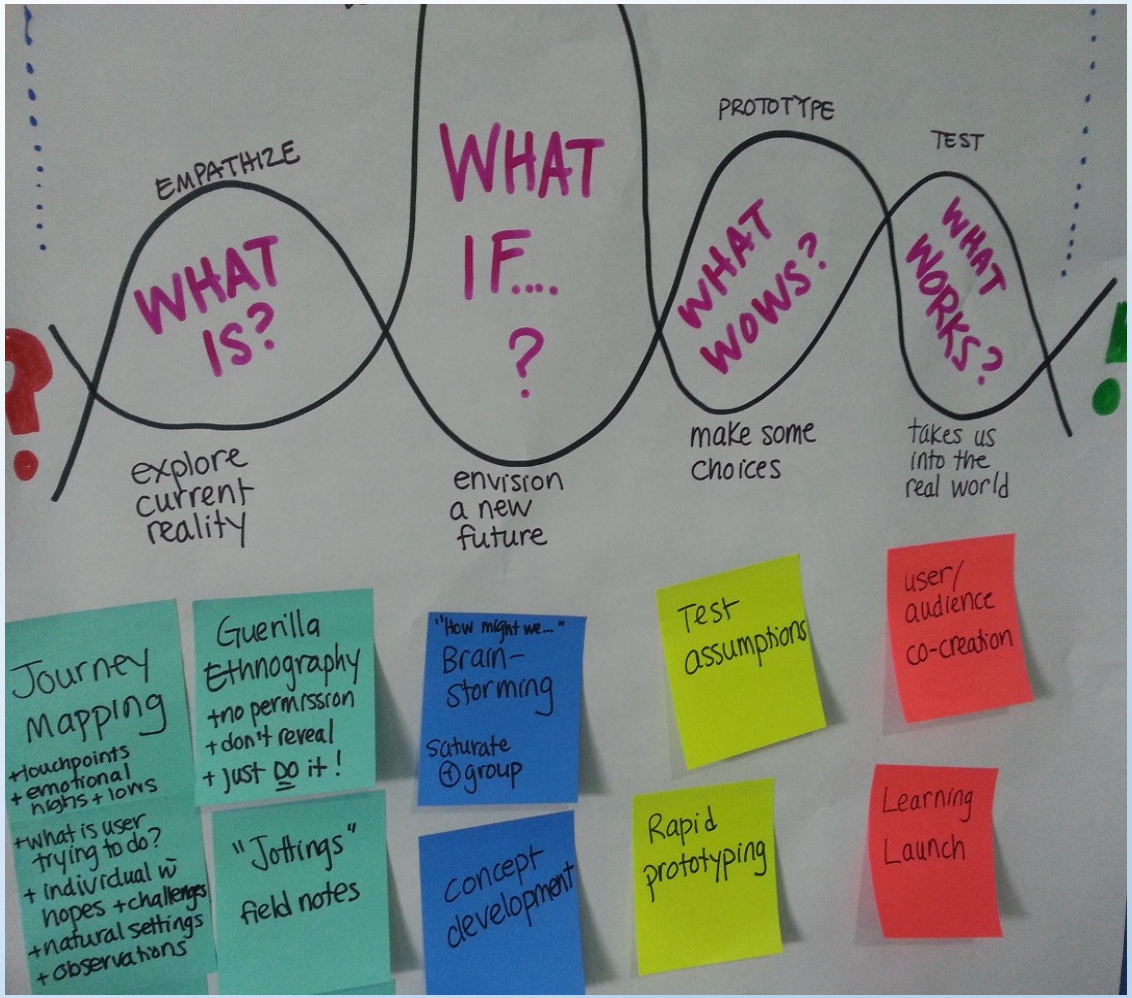
- Impossibilità di esercitare i diritti es. il «diritto all'oblio»

Privacy Consulting

PRIVACY BY DESIGN

Protezione dei dati personali già dalla fase di ideazione e progettazione di un trattamento, in modo da *prevenire* possibili rischi di violazione

[art. 25 - GDPR]



Privacy Consulting

COMPLIANCE **ORGANIZZATIVA** GDPR NELLE TECNOLOGIE AI - I

- Trasparenza (spiegabilità del processo decisionale automatizzato);
- Minimizzazione dei dati;;
- Formazione del personale in materia di protezione dei dati personali;
- Verifiche di qualità e esattezza dei dati utilizzati;
- Predisporre piani di audit interni regolari;
- Effettuare un DPIA e una FRIA sul sistema AI;
- Integrare metodologie di etica per un uso responsabile dei dati personali in AI;
- Non diffusione dei dati di addestramento

Privacy Consulting

COMPLIANCE **TECNICA** GDPR NELLE TECNOLOGIE AI - II

Valutazione e mitigazione del rischi di discriminazione per gli interessati;

Adozione e verifica continua delle Best practices di sicurezza **avanzata**;

Adottare tecniche Privacy-enhancing technologies (PET)

Mappatura e etichettatura dei dati per tracciare l'origine della raccolta;

Tecniche di versioning per un rapido ed efficace rollback;

Tecniche di deduplicazione;

Utilizzo di dati sintetici o anonimi;

Non diffusione dei dati di addestramento;

Dott. Adriano Bertolino

Privacy Consulting

DATI SINTETICI E ANONIMI

Dati Sintetici

- *Non* si applica il GDPR
- Generati artificialmente da algoritmi generativi, che producono campioni di dati che approssimano il comportamento dei dati reali senza rivelare informazioni personali
- Possono essere utilizzati per addestrare i modelli di Machine Learning al posto dei dati reali

Più sono vicini a replicare dati reali e più è proporzionale il rischio di re-identificazione

Anonimi

- *Non* si applica il GDPR
- Utilizzati per statistiche generali
- Non è presente il rischio di re-identificazione
- Aiuta a tutelare la privacy degli individui senza compromettere l'utilità dei dati per l'analisi ed il Machine Learning

Dott. Adriano Bertolino

BILANCIAMENTO

L'obiettivo finale è trovare un equilibrio tra l'uso avanzato dell'Intelligenza Artificiale e la tutela della privacy delle persone coinvolte.

Privacy Consulting

Questions & Answers

WHAT?

WHO?

WHERE?

WHEN?

WHY?

HOW?

Dott. Adriano Bertolino

Privacy Consulting

Dott. Adriano Bertolino

+39 3477167484

info@adrianobertolino.it

it.linkedin.com/in/adrianobertolino