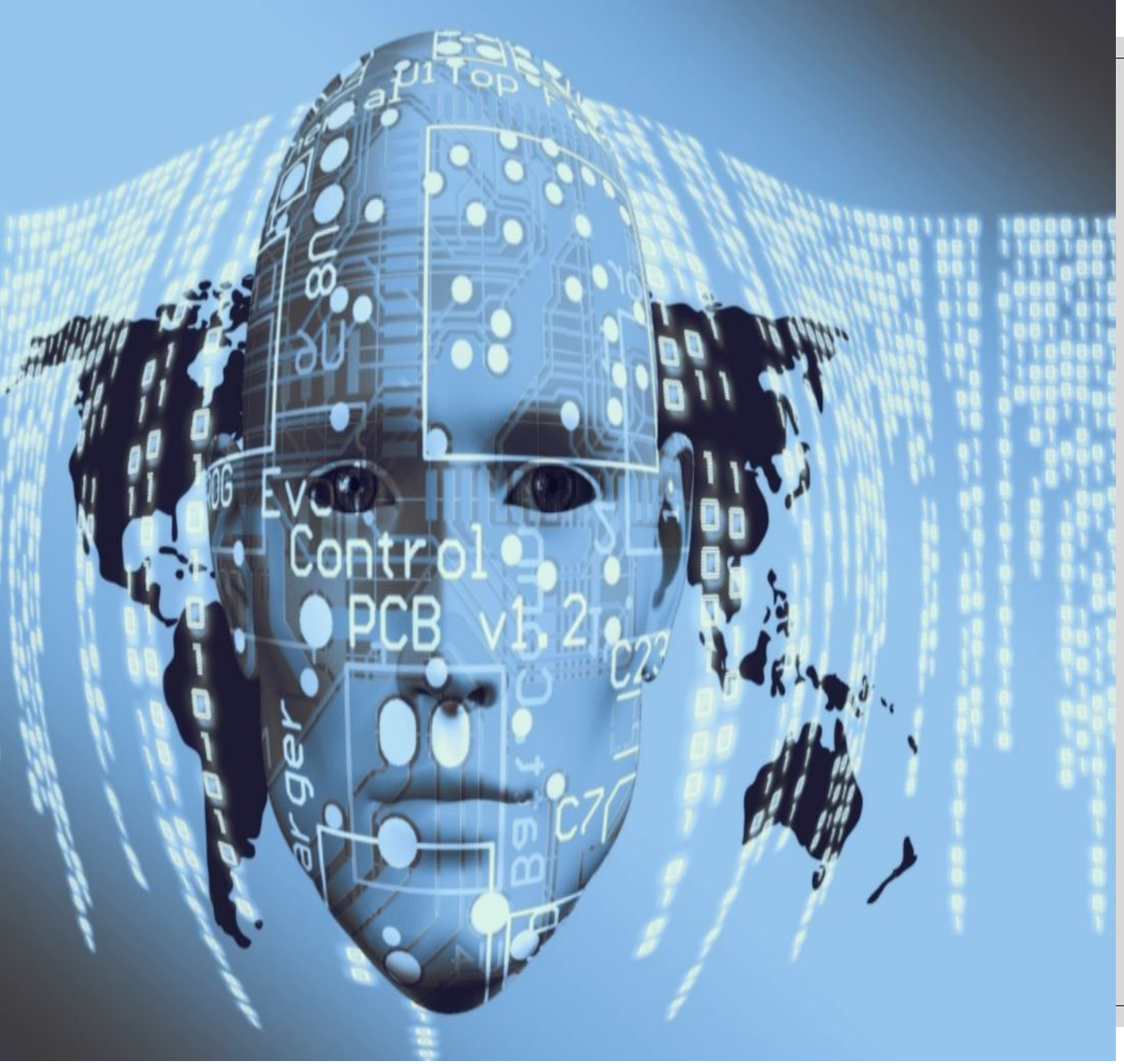
Monica Gobbato
E- Privacy 2023
Roma

Il REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE.

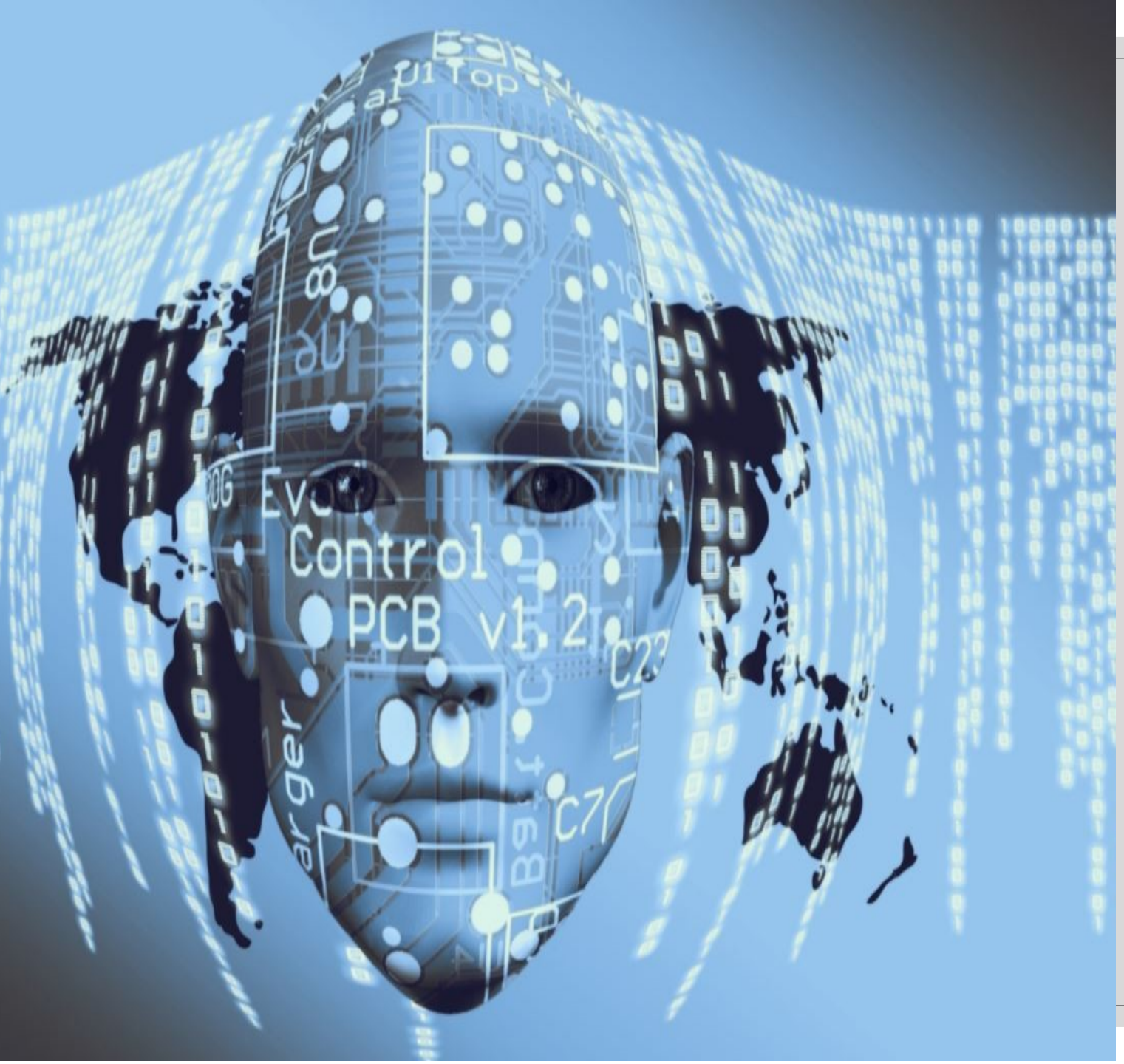


Siamo un’associazione che si occupa di privacy che si è costituita nel 2019, ma la sua Presidente si occupa della disciplina sulla protezione dei dati personali dal 1997.

Perché ESSERE SOCI DA' VANTAGGI

02

- 1 webinar in streaming al mese sulle novità della data Protection e della Digital Law
- 3 eventi fisici l'anno in località bellissime a prezzi speciali con attestato di frequenza delle ore svolte
- Tante Registrazioni accessibili On Line
- Sconti sul corso Avanzato per Dpo da 120 ore
- Accountability dimostrata sia per Dpo Che per Aziende, essendo Privacy Academy tra le prime Associazioni sul tema Data Protection riconosciute dal Garante
- Network di esperti Dpo e Digital Law



21 aprile 2021
La Commissione Europea ha presentato una Proposta di Regolamento in materia di AI.

La Proposta:
- stabilisce norme armonizzate in materia di AI
- Modifica alcuni atti legislativi dell'Unione

PRIVACY ACADEMY

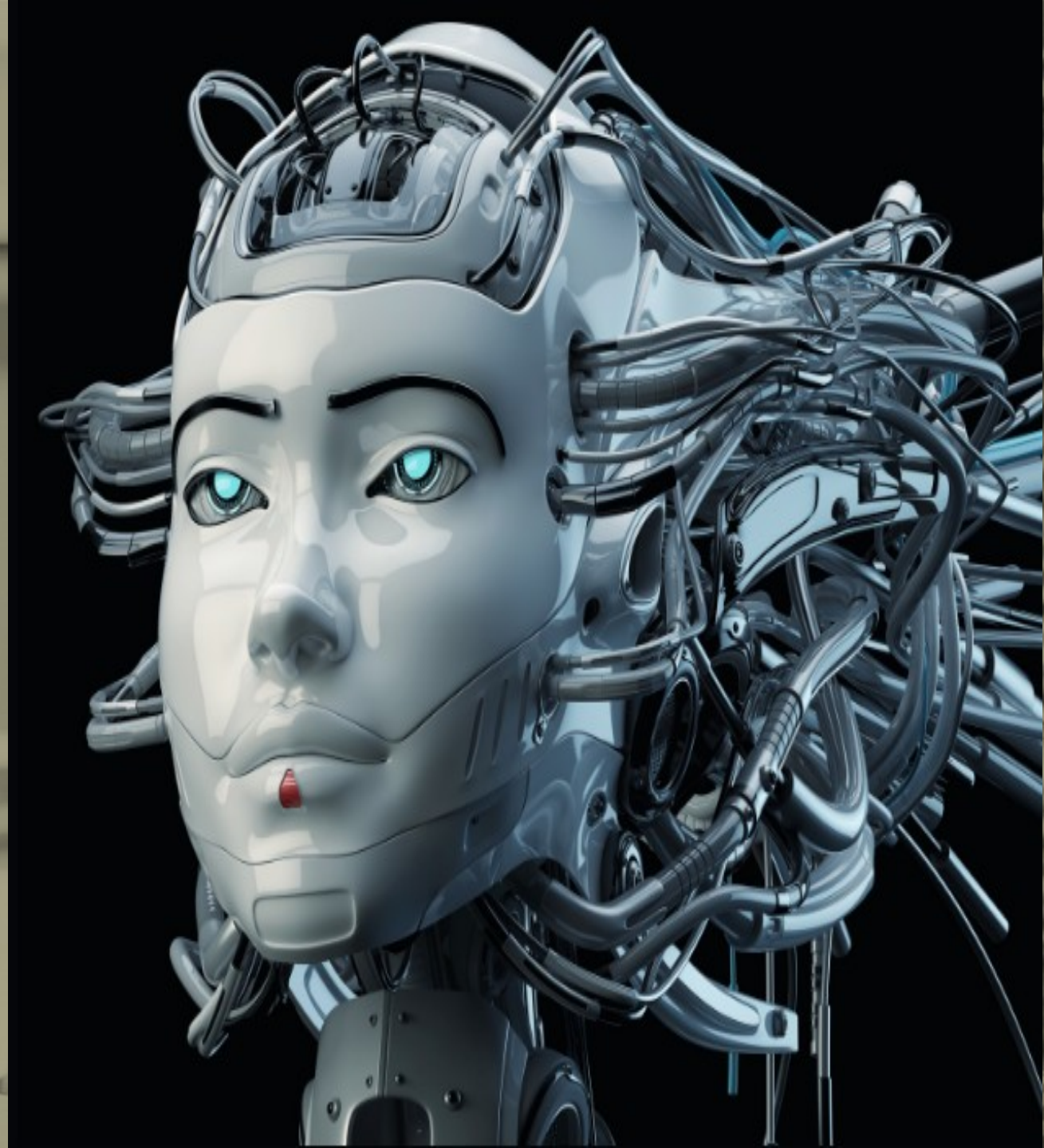
Reg Eu:

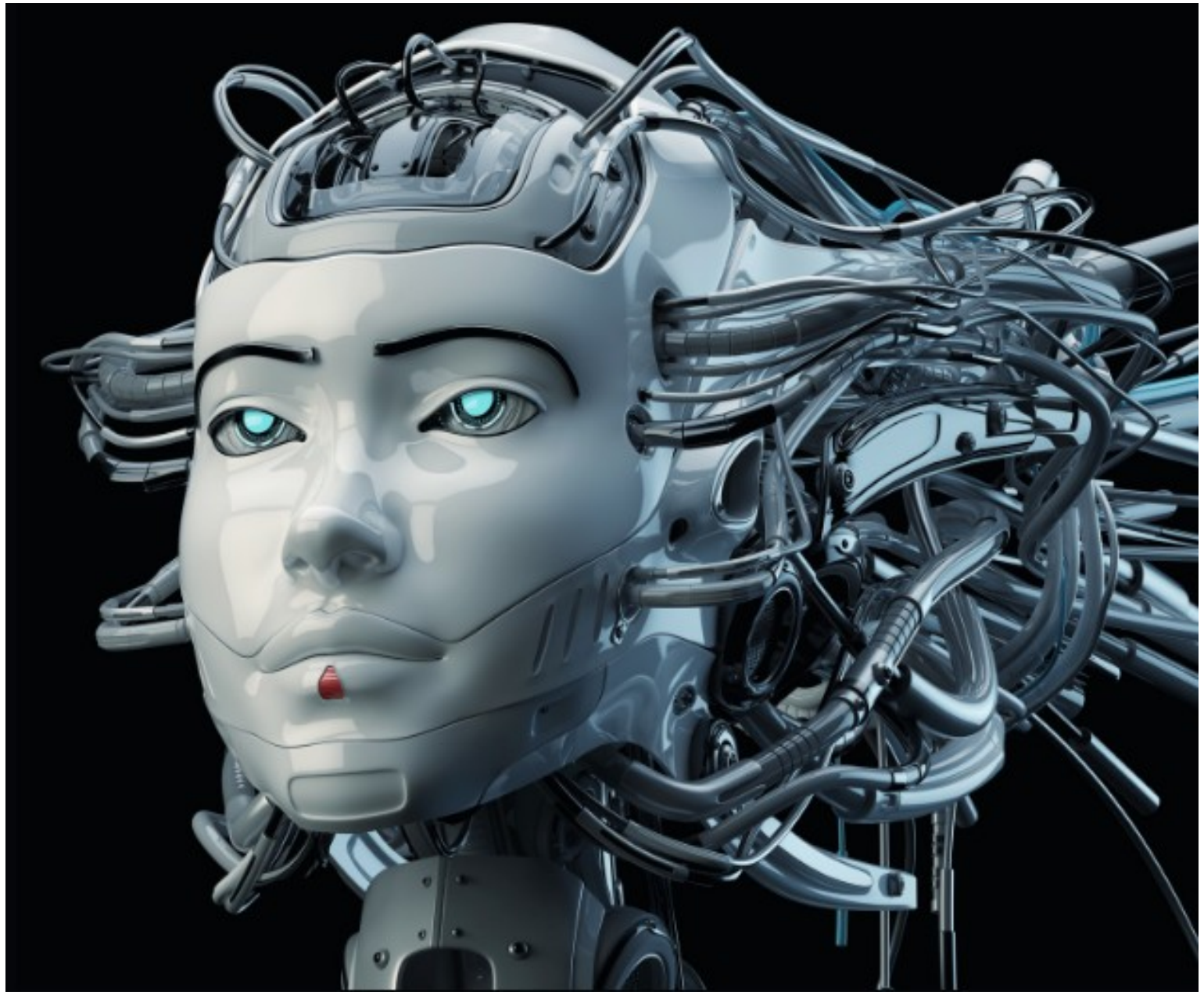
REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE

.

1) I sistemi di IA vietati ed "ad alto rischio"

2) Individuazione degli obblighi e delle responsabilità che dovrebbero essere poste in capo ai fornitori dei sistemi di Intelligenza Artificiale.





Scopo: Incrementare la fiducia sull’AI

Lo scopo: regolamentare lo sviluppo e l’utilizzo dell’AI, al fine di incrementare la fiducia dei cittadini europei verso simili strumenti e garantire che l’utilizzo degli stessi non costituisca una violazione dei diritti fondamentali sanciti dalla normativa europea vigente.

Oggetto del nuovo testo di compromesso:

i sistemi di IA vietati e i c.d. “ad alto rischio”

Individuazione degli **obblighi e delle responsabilità che dovrebbero essere poste in capo ai fornitori dei sistemi di intelligenza artificiale.**

La tabella seguente mostra le soluzioni adottate in base in base alla classificazioni dei prodotti.

Rischi per i diritti fondamentali	Tipi di prodotti classificati in base al rischio	Soluzioni	Rischi per i diritti fondamentali
totale (art. 5)	**prodotti suscettibili di** - causare o poter causare **danni fisici o psicologici manipolando il comportamento umano** per aggirare il libero arbitrio degli utenti; - **imporre il c.d. *'social scoring'* da parte o per conto delle autorità**	**L'uso di questi prodotti è proibito.**	**totale (art. 5)**

https://www.maxrichtermusic.com/albums/nosedive/

Rischio Totale

NoseDive – Black Mirror

SOCIAL SCORING

L'utilizzo dell'intelligenza artificiale per **dare punteggi** alle persone **in base al loro comportamento** è vietato nella proposta di regolamento,
con **un'eccezione per le piccole imprese** contenuta nella bozza approvata dal Consiglio, ma **cancellata** in quella di mediazione redatta dalla commissione Giustizia dell'Europarlamento: *"È opportuno esentare i sistemi di Ai destinati alla valutazione dell'**affidabilità creditizia** e del **merito***

La tabella seguente mostra le soluzioni adottate in base in base alla classificazioni dei prodotti

Rischi per i diritti fondamentali	Tipi di prodotti classificati in base al rischio	Soluzioni	Rischi per i diritti fondamentali
da totale ad alto in base all’uso che si fa del prodotto (art. 5)	i sistemi di identificazione biometrica **a distanza "in tempo reale" in spazi accessibili al pubblico usate dalle forze dell’ordine** rientrano in questa categoria.	Questo tipo di prodotto**, sebbene proibito in linea generale, in casi eccezionali e sotto il controllo di un'autorità, è soggetto alle stesse regole stabilite per i prodotti ad alto rischio**.	da totale ad alto in base all’uso che si fa del prodotto (art. 5)

Sistemi di identificazione biometrica **a distanza "in tempo reale**

Rischio di sostenere regimi che usano l'Ai per la repressione

L'Iran ha annunciato di ***utilizzare il riconoscimento facciale*** *per segnalare le* ***donne che non indossano correttamente il velo****, la Russia per identificare le persone da arrestare*

WIRED

CHECK IN CON RICOSCIMENTO FACCIALE

accesso e fruizione di servizi privati essenziali e di servizi e benefici pubblici

11:51 121 KB/s 63%

Selvaggia Lucarelli

Selvaggia Lucarelli
19 ago 2019 ·

A Cina è Minority Report. Lorenzo Biagiarelli

Mi piace Commenta Condividi

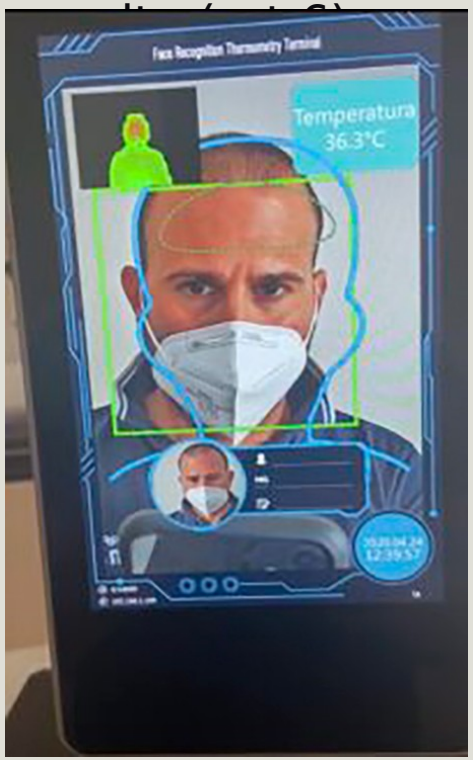
Barbara Vellucci e altre 3.267 persone

Più pertinenti

Fabio Santarelli
La Cina è già la super potenza in tutti i campi. Sono

Commenta come Monica Gobbato

La tabella seguente mostra le soluzioni adottate in base in base alla classificazioni dei prodotti.

Rischi per i diritti fondamentali	Tipi di prodotti classificati in base al rischio	Soluzioni	Rischi per i diritti fondamentali
alto (art.6)..	prodotti - **nei seguenti settori**: **1. identificazione e categorizzazione biometrica delle persone fisiche;** **2. gestione e funzionamento delle infrastrutture critiche;** **3. istruzione e formazione professionale;** **4. occupazione, gestione dei lavoratori e accesso al lavoro autonomo;** **5. accesso e fruizione di servizi privati essenziali e di servizi e benefici pubblici;** **6. applicazione della legge; gestione della migrazione, dell'asilo e dei controlli alle frontiere;**	Al fine di mitigare l'alto rischio, il Regolamento: - **stabilisce che prima di immettere sul mercato tali prodotti, siano rispettati le seguenti condizioni**: **• adozione di un sistema di gestione del rischio** ; **• gestione dei dati affinché siano di alta qualità.** **• adozione di documentazione tecnica che fornisca tutte le informazioni**	

La tabella seguente mostra le soluzioni adottate in base in base alla classificazioni dei prodotti.

Rischi per i diritti fondamentali	Tipi di prodotti classificati in base al rischio	Soluzioni	Rischi per i diritti fondamentali
medio (art. 52)	**prodotti che interagiscono con le persone fisiche**. **prodotti per il riconoscimento delle emozioni o la categorizzazione biometrica**. Prodotti di IA che generano o manipolano immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti,	le persone fisiche devono essere informate che stanno interagendo con una IA. **le persone fisiche devono essere informate che sono esposte a un sistema di riconoscimento delle emozioni o di categorizzazione biometrica.** **Le persone fisiche devono essere**	medio (art. 52)

IMMAGINI DEEP FAKE E CHAT GPT

Nella proposta di compromesso dell'Europarlamento, i **contenuti** generati dall'intelligenza artificiale **che sembrano scritti da una persona**, così come le immagini **deepfake** - sono soggetti a **obbligo di trasparenza** verso gli utenti. Si obbliga a informare gli utenti, durante il momento dell’esposizione al contenuto (chatbot o deepfake) che è stato generato da un algoritmo. "*Questo obbligo di trasparenza è previsto **nella bozza dell'Europarlamento ma non nella posizione del Consiglio***", sotto

WIRED

Medium Risk @deeptomcruise V.

ESEMPIO DI

Prodotto che genera o manipola immagini, contenuti audio o video che assomigliano sensibilmente a persone, oggetti, luoghi o alter entità o eventi esistenti che potrebbero falsamente apparire a una persona come autentici o veritieri.

https://www.tiktok.com/@deeptomcruise/video/7181490100314885382

DeepTomCruise

Rischio Limitato

Sistemi di Ai che hanno interazioni con persone naturali.

In questi casi si ha l’obbligo di:

Informare le Persone

Dpia.

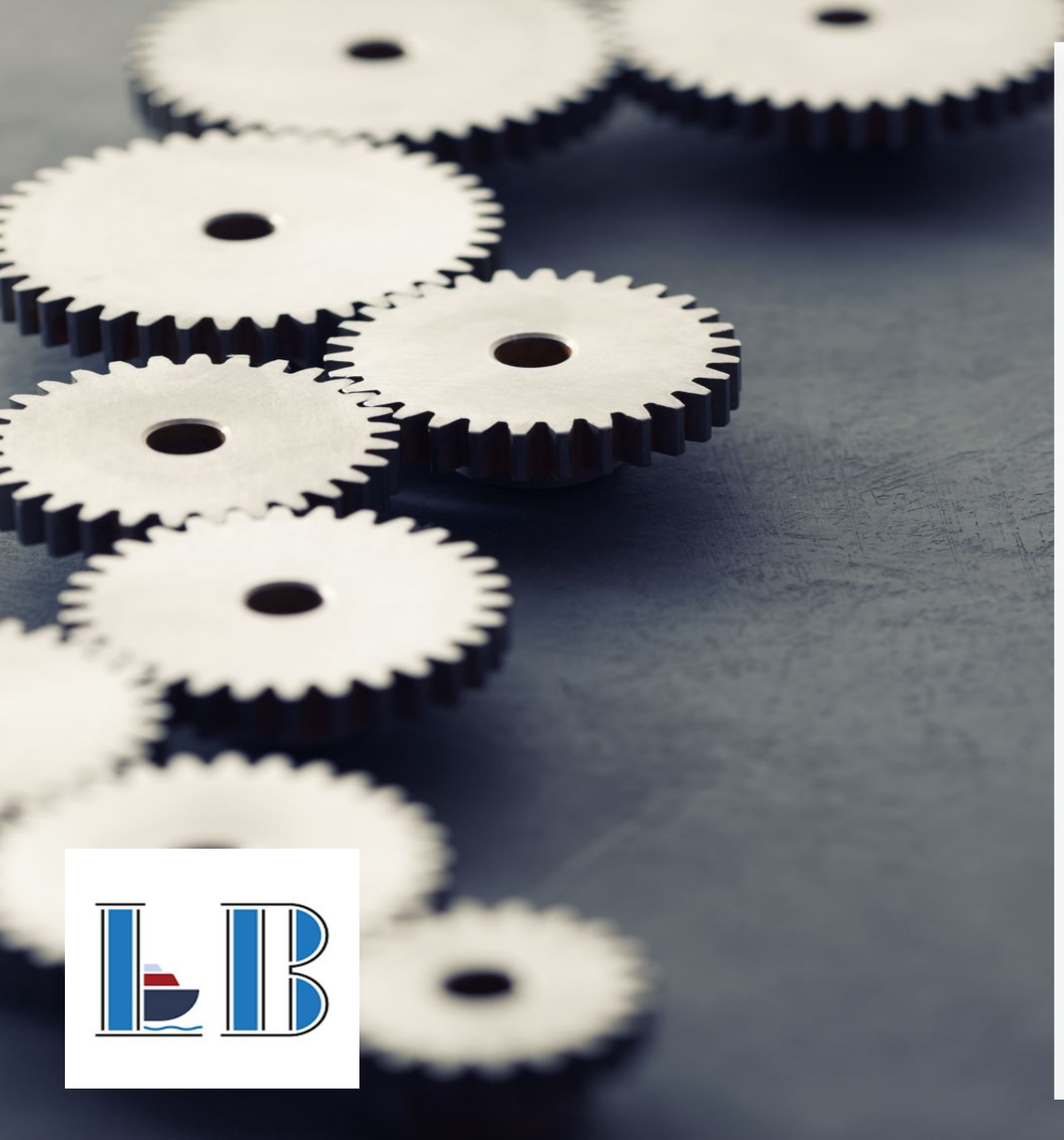
Su base volontaria le Aziende una cer

1)
6 Mesi di LOG

- I fornitori di IA, dovranno conservare i log generati automaticamente dai sistemi per almeno sei mesi.
- COME GIA SUCCEDE IN ITALIA IN BASE AL PROVV. 27 NOV 2008 SUGLI AMMINISTRATORI DI SISTEMA

2)
La catena delle Responsabilità

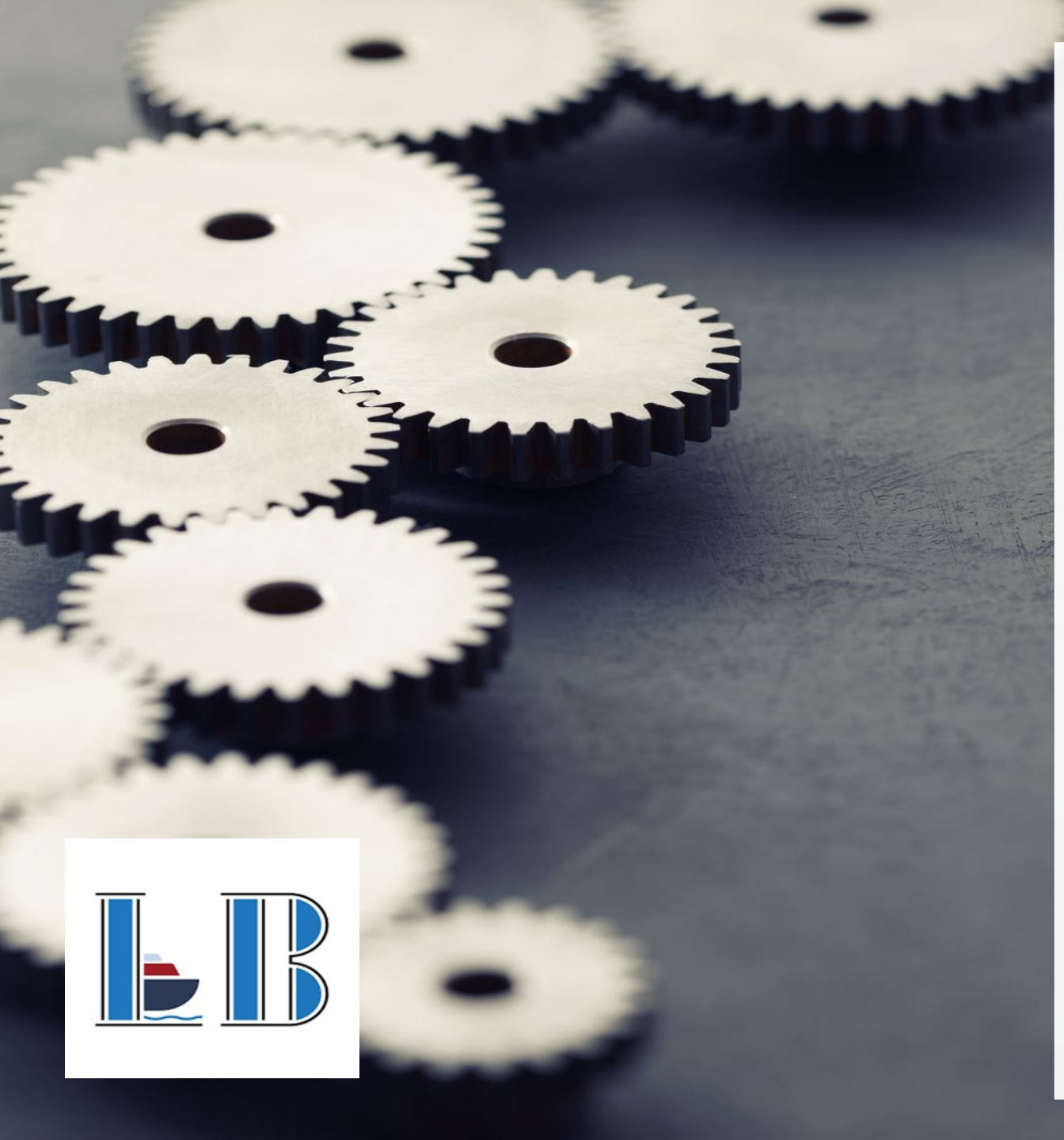
- La proposta emendativa, più in generale, si focalizza, **sulla corretta ripartizione delle responsabilità lungo l’interezza della complessa catena di approvvigionamento dei sistemi di IA.**
- Relativamente a detti sistemi appare particolarmente complesso individuare le ipotesi nelle quali il fornitore possa essere ritenuto responsabile dei risultati ottenuti dall’IA, non potendo lo stesso avere contezza, al momento in cui l’IA è sviluppata ed immessa sul mercato, di quale scopo gli utenti potranno dare ai sistemi finali.
- Per tale ragione, l’argomento non appare ancora pienamente risolto



2)
La catena delle Responsabilità

Il problema dell'AI è la Catena delle Responsabilità in quanto ci sono numerosissimi soggetti che hanno un ruolo:

- Programmatori,
- Svilluppatori,
- Fornitori



2)
Catena delle Responsabilità

In ultimo l’AI migliora e si definisce grazie all’esperienza personale dell’utente finale.

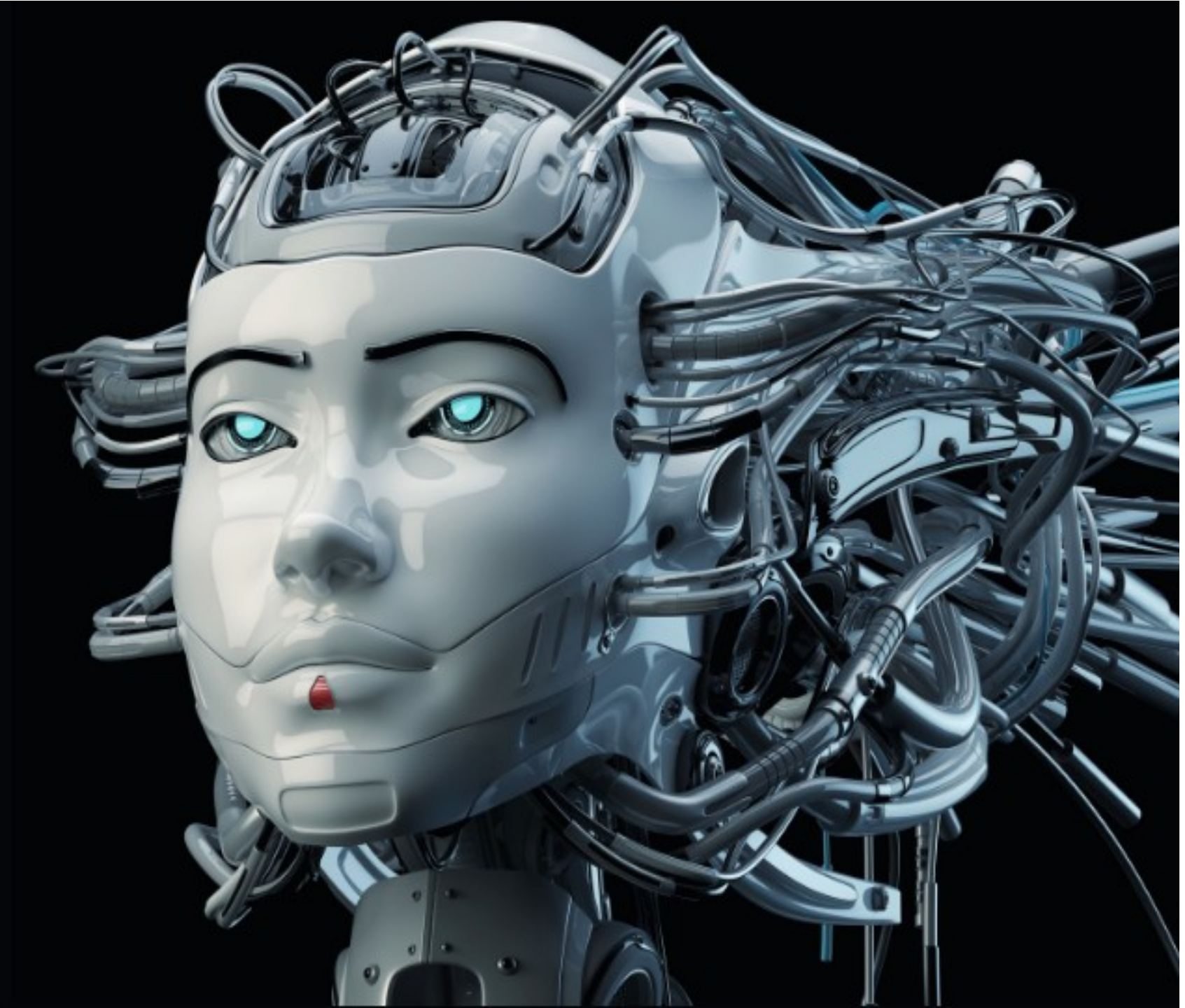
Per queste ragioni la catena delle Responsabilità non è tuttora totalmente definita.

Prerequisito per commercializzare AI

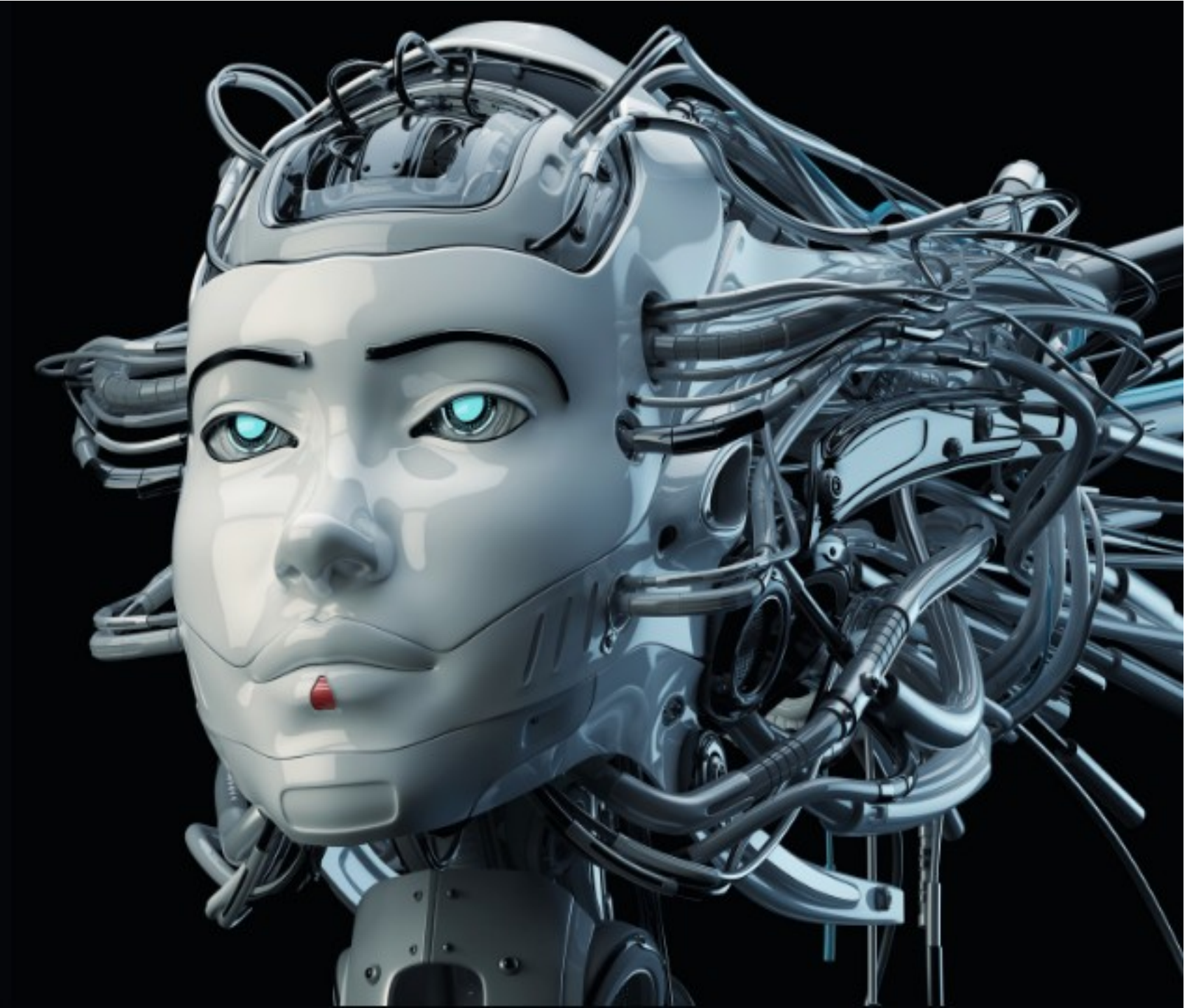
3) Rappresentante Nominato

I fornitori dovranno nominare un rappresentante autorizzato, il quale sarà incaricato di garantire che:

- la procedura di valutazione della conformità del sistema sia stata eseguita,
- tenere a disposizione della autorità nazionale competente tutta la documentazione pertinente, così come la dichiarazione di conformità.



Il Garante suggerisce al Governo di individuare nell'Autorità Protezione dei Dati Personali, le costituende autorità di controllo per l'IA, in linea con quanto emerge nel parere 5/2021 *dell'EDPB e EDPS* .



La designazione delle autorità della protezione dei Dati come un supervisore nazionale dovrebbe assicurare:

- **Un approccio un po’ piu armonizzato e regolamentato** e
- contribuirebbe alla adozione di una interpretazione coerente di **disposizioni in materia di trattamento dei dati nonché a evitare contraddizioni nella loro applicazione nei diversi Stati membri”.**

L’ IDEA DEL GARANTE ITALIANO DELLA PROTEZIONE DEI DATI

Il Garante Italiano ha evidenziato il ruolo centrale che la normativa sulla protezione dei dati assume nel campo dell’IA: il trattamento di dati (in particolare personali) è funzionale all’alimentazione dei sistemi di IA ed errori, imprecisioni o irregolarità nel trattamento dei dati funzionali all’alimentazione della macchina si riflettono in altrettante distorsioni del processo algoritmico.

Nuovo Testo della Proposta

Sono ancora molti i punti caldi della proposta che necessiteranno di ulteriori approfondimenti tecnici, una volta consolidate e chiarite le parti meno “controverse” della proposta medesima

AJ PRIVACY ACADEMY

Il report di ENISA

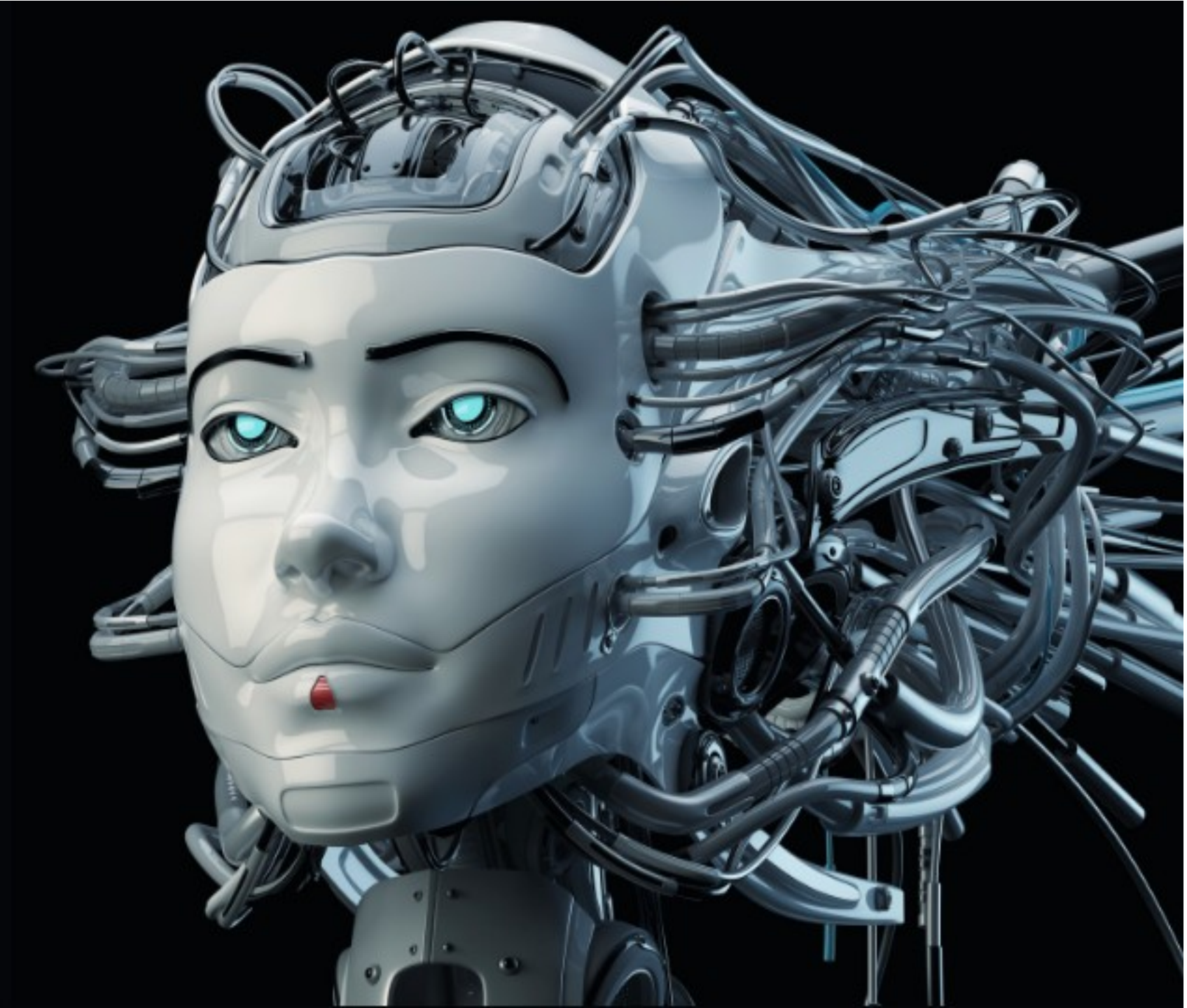
L'obiettivo generale del presente documento è fornire una panoramica degli standard (esistenti, in fase di elaborazione, esame e progettazione) relativi alla sicurezza informatica dell'artificiale intelligence (AI), valutarne la copertura e identificare le lacune nella standardizzazione. Il rapporto è destinato a contribuire alle attività preparatorie all'attuazione della proposta UE regolamento

Il report di ENISA

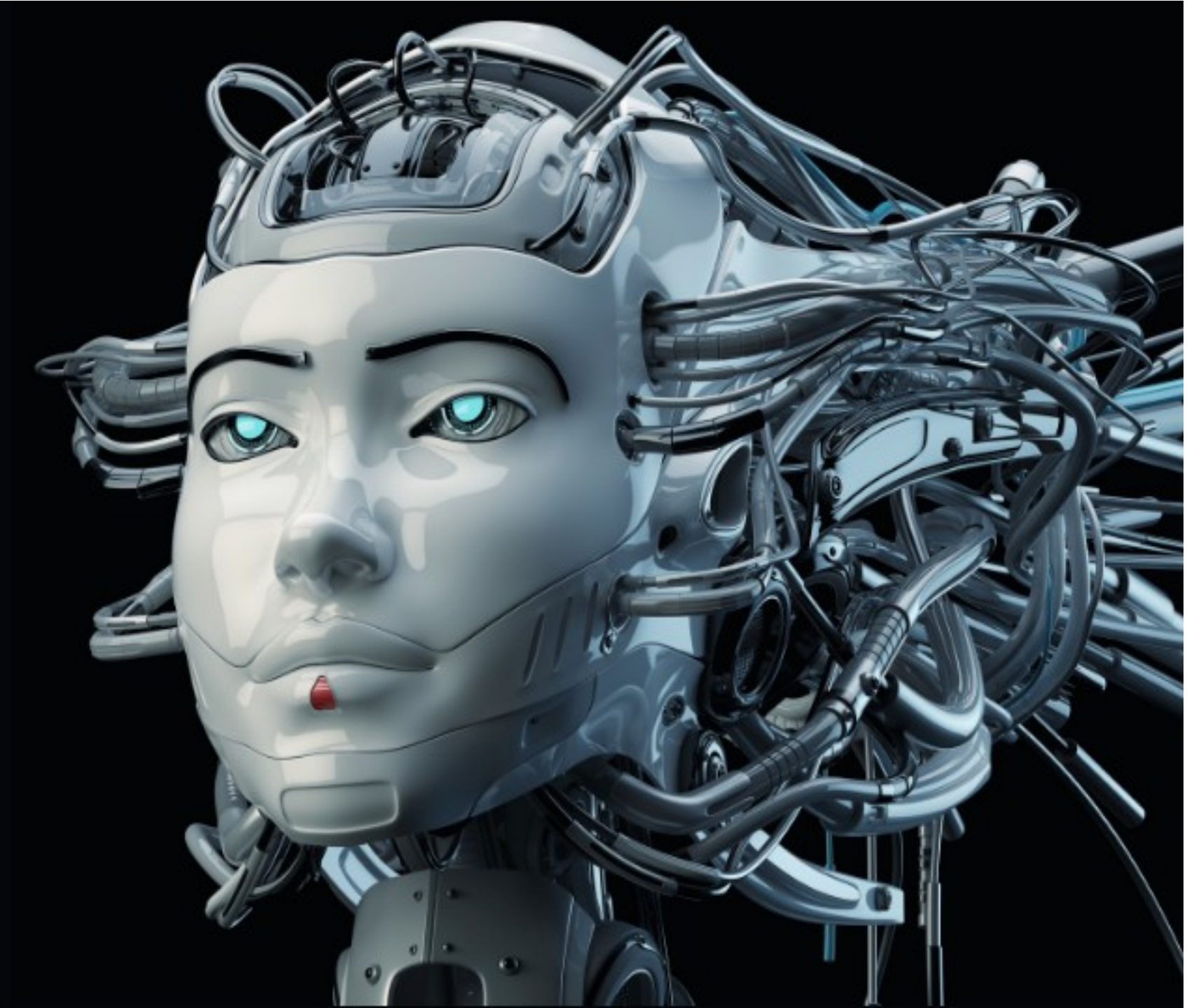
Lo studio suggerisce che gli standard generali per la sicurezza e la qualità delle informazioni gestione (in particolare ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 9001**) può parzialmente mitigare i rischi di cibersicurezza legati alla riservatezza, all'integrità e alla disponibilità dell'IA sistemi.**

Questa conclusione si basa sul presupposto che l'intelligenza artificiale sia nella sua essenza software e pertanto ciò che è applicabile al software può essere applicato all'IA, se viene fornita una guida adeguata.

Questo approccio può essere sufficiente a livello generale, ma deve



Dopo mesi di trattative tra gli eurodeputati, il Parlamento europeo ha raggiunto un accordo politico provvisorio sull’Artificial Intelligence Act, il primo regolamento al mondo sull’Intelligenza Artificiale.

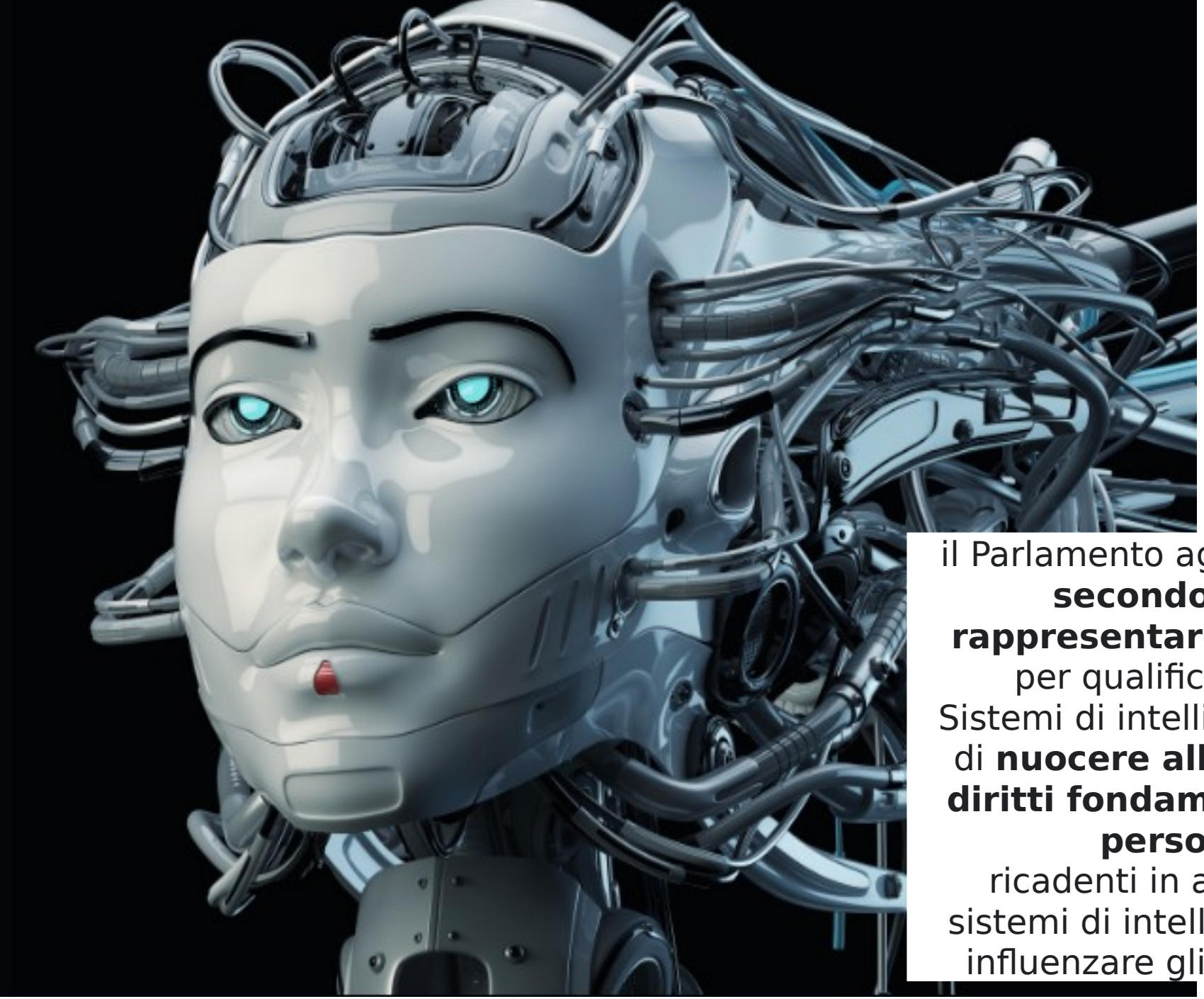


Inoltre c’è anche un documento del Parlamento Europeo del giugno 2023

Parliament's negotiating position on the artificial intelligence act

Le modifiche proposte in questa sede riguardano prevalentemente il sistemi di categorizzazione biometrica che utilizzano caratteristiche sensibili

(ad esempio sesso, razza, etnia, stato di cittadinanza



Inoltre c’è anche un documento del Parlamento Europeo del giugno 2023

Parliament's negotiating position on the artificial intelligence act

il Parlamento aggiunge **l'ulteriore requisito secondo cui i sistemi devono rappresentare un "rischio significativo"** per qualificarsi come ad alto rischio. Sistemi di intelligenza artificiale che rischiano di **nuocere alla salute, alla sicurezza, ai diritti fondamentali o all'ambiente delle persone** considerati sono ricadenti in aree ad alto rischio. Inoltre, i sistemi di intelligenza artificiale utilizzati per influenzare gli elettori campagne politiche

Il report di ENISA

Sono state individuate le seguenti lacune:

- **ad oggi non esistono standard che coprano adeguatamente la cybersecurity e descrivano la competenze delle organizzazioni per l'audit, la certificazione e il collaudo dei sistemi di IA**

Il report di ENISA

il suddetto gap è rilevante ai fini della attuazione del progetto di legge sull'IA, in particolare per quanto riguarda l'avvelenamento dei dati e il contraddittorio

www.privacyacademy.it
www.lawboat.ch
gobbato@privacyacademy.it