

A teal decorative shape in the top-left corner of the slide.

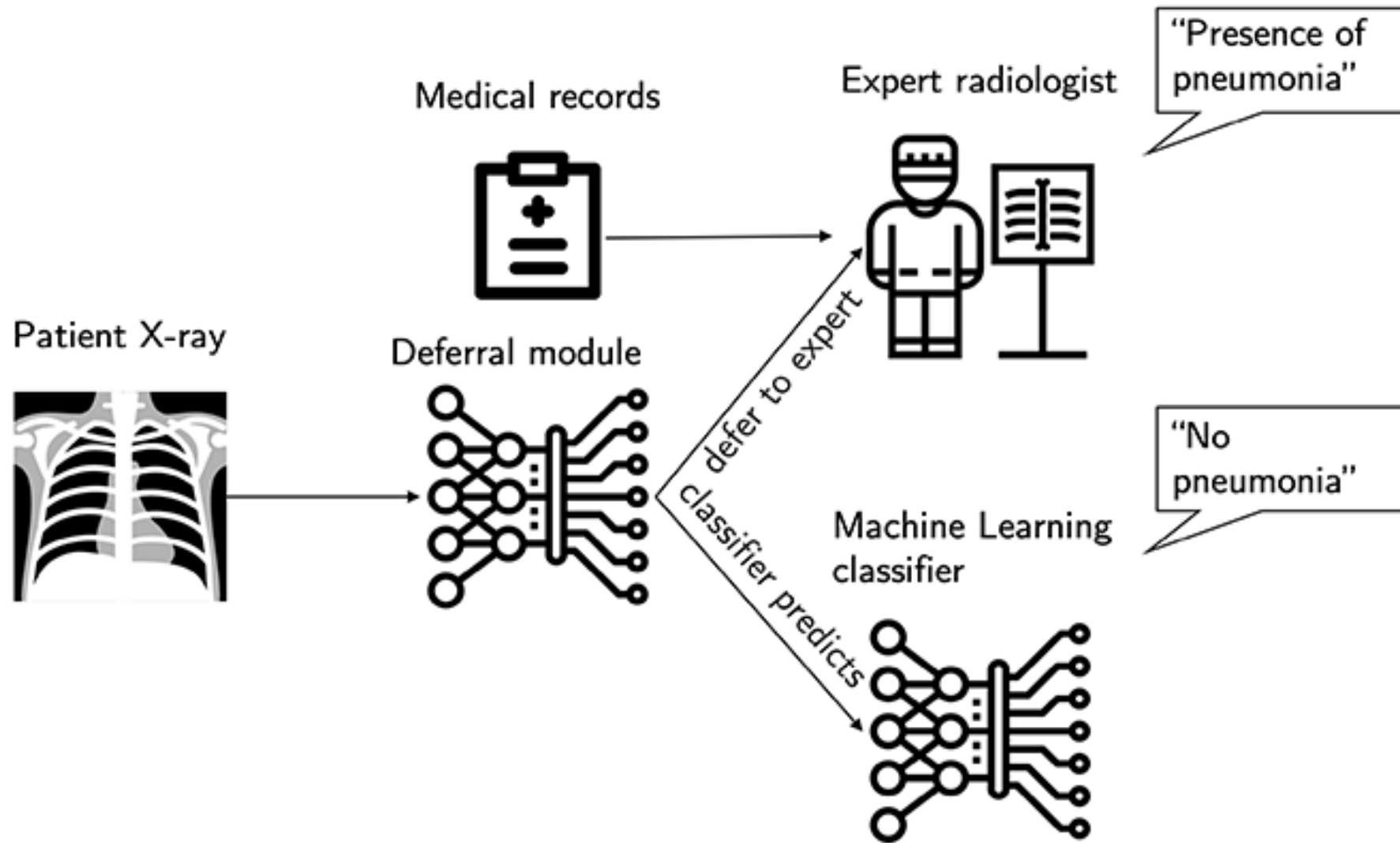
**INTELLIGENZA
ARTIFICIALE E
TRATTAMENTO
DI DATI
PERSONALI
NELL'AI ACT**

A decorative graphic of red lines and dots resembling a circuit board or data flow, located at the bottom left of the slide.A vertical dashed orange line separating the title from the speaker information.

Avv. Ilaria Feriti

Firenze, 10 ottobre 2024

A teal decorative shape in the bottom-right corner of the slide.



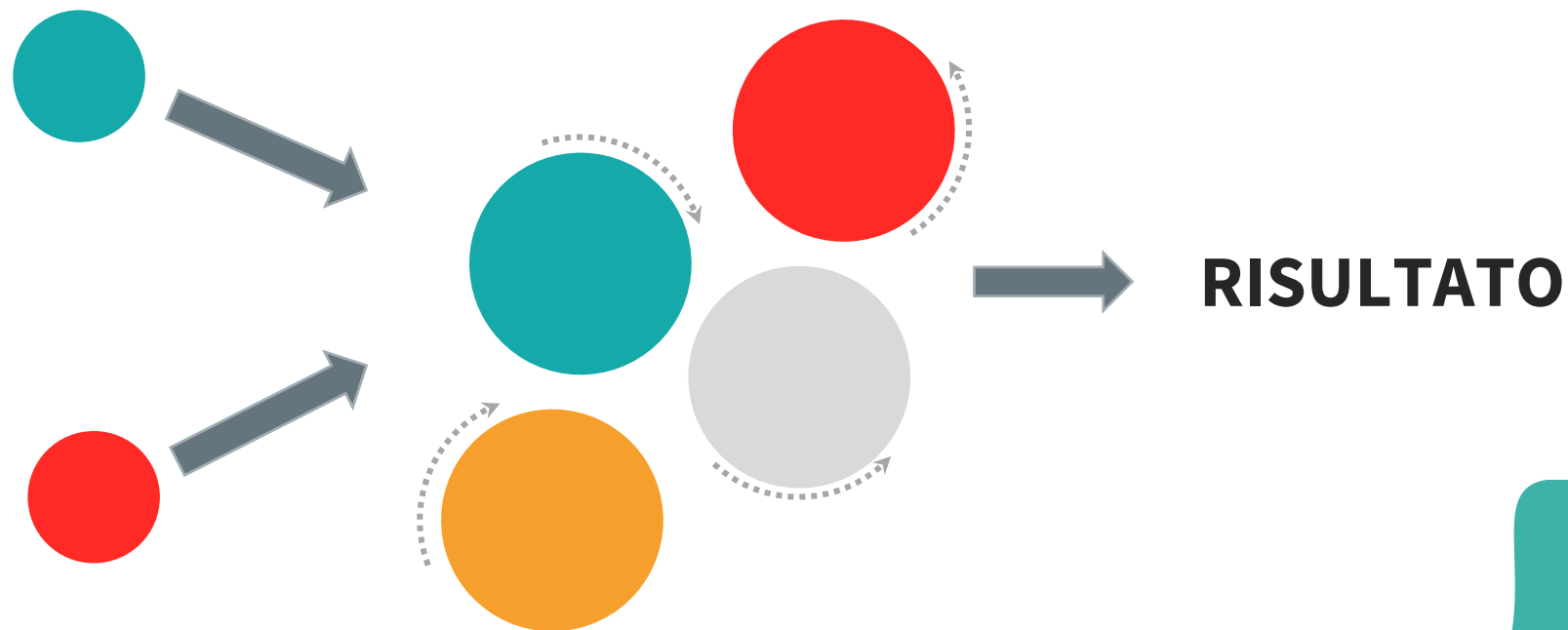
La fase più delicata per il corretto funzionamento di un sistema di intelligenza artificiale è quella di **raccolta dei dati** che compongono il dataset di addestramento

DATI PERSONALI COMUNI

qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente

DATI PARTICOLARI - Art. 9 GDPR

dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona



Relazione di accompagnamento all'AI ACT

« La proposta non pregiudica il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva (UE) 2016/680) e li integra con una serie di regole armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio nonché di restrizioni concernenti determinati usi dei sistemi di identificazione biometrica remota»



I PRINCIPI ART. 5 GDPR

LICEITÀ, CORRETTEZZA E TRASPARENZA

I dati devono essere trattati in modo **lecito**, corretto e trasparente nei confronti dell'interessato

LIMITAZIONE DELLA FINALITÀ

Ossia raccolti per finalità determinate, **esplicite** e legittime

MINIMIZZAZIONE DEI DATI

Devono essere adeguati, pertinenti e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati

ESATTEZZA

I dati trattati devono essere esatti e, se necessario, aggiornati o **rettificati**

LIMITAZIONE DELLA CONSERVAZIONE

I dati vanno conservati per un arco di tempo **non superiore** al conseguimento delle finalità per le quali sono trattati

INTEGRITÀ E RISERVATEZZA

Va garantita adeguata **sicurezza e protezione** dei dati personali, anche mediante misure tecniche e organizzative idonee

OBBLIGO DI INFORMATIVA ART. 13 -14 GDPR

1

Deve essere concisa, facilmente accessibile, di facile comprensione e usare un linguaggio semplice e chiaro

2

Deve contenere tutte le informazioni elencate dalla norma (identità e dati di contatto del titolare, finalità e base giuridica del trattamento, periodo di conservazione, ecc.)

3

Va comunicata l'esistenza di un **processo decisionale automatizzato**, dando informazioni significative sulla logica utilizzata, sull'importanza e sulle conseguenze previste di tale trattamento per l'interessato



**I DIRITTI
DELL'INTERESSATO
ART. 7, 15- 21 GDPR**



----- **Diritto di revocare il consenso**

----- **Diritto di accesso**

----- **Diritto di rettifica**

----- **Diritto all'oblio**

----- **Diritto di limitazione**

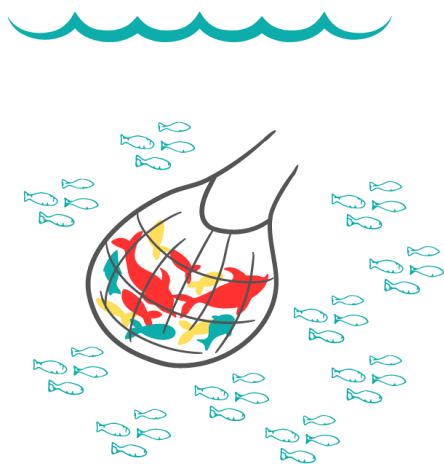
----- **Diritto alla portabilità dei dati**

----- **Diritto di opposizione**

WEB SCRAPING VS GDPR



WEB SCRAPING VS GDPR



La navigazione nel web si basa su protocolli aperti che consentono di reperire **dati pubblicamente disponibili online** oppure resi disponibili in aree ad accesso controllato (es. *social network*).

I dati pubblicamente disponibili possono essere raccolti in maniera sistematica attraverso programmi (c.d. *bot*) che operano in modo automatizzato simulando la navigazione umana.

Alcuni *bot* scandagliano il web al fine di raccogliere i dati e indicizzarli, ad esempio, per garantire il funzionamento dei motori di ricerca.

Nel **web scraping** l'attività di raccolta massiva e indiscriminata di dati (anche personali) è combinata con un'ulteriore attività, che consiste nella memorizzazione e conservazione dei dati raccolti dai *bot* per successivi e diversi utilizzi.

WEB SCRAPING VS GDPR

Il fatto che i dati siano pubblicamente disponibili online non è sufficiente, di per sé solo, a giustificare il *web scraping* finalit  di addestramento perch :

- 1 Vanno rispettati i principi e gli obblighi sanciti dal GDPR;
- 2 Vanno assicurati i diritti riconosciuti agli interessati;

I PRINCIPI ART. 5 GDPR

LICEITÀ, CORRETTEZZA E TRASPARENZA

I dati devono essere trattati in modo **lecito**, corretto e trasparente nei confronti dell'interessato

LIMITAZIONE DELLA FINALITÀ

Ossia raccolti per finalità determinate, **esplicite** e legittime

MINIMIZZAZIONE DEI DATI

Devono essere adeguati, pertinenti e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati

ESATTEZZA

I dati trattati devono essere esatti e, se necessario, aggiornati o **rettificati**

LIMITAZIONE DELLA CONSERVAZIONE

I dati vanno conservati per un arco di tempo **non superiore** al conseguimento delle finalità per le quali sono trattati

INTEGRITÀ E RISERVATEZZA

Va garantita adeguata **sicurezza e protezione** dei dati personali, anche mediante misure tecniche e organizzative idonee

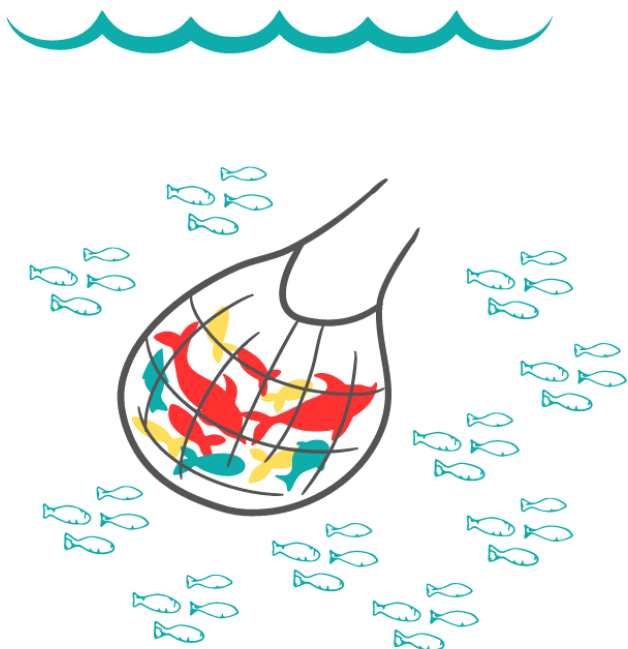
BASE GIURIDICA

ART. 6 GDPR



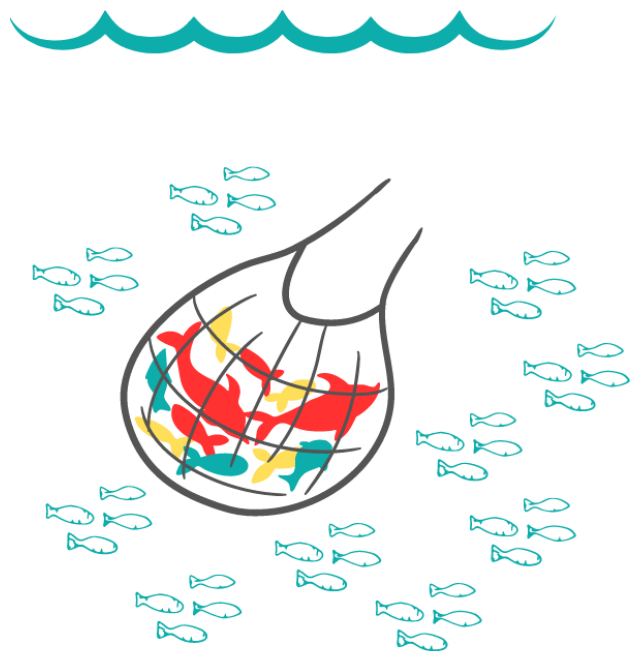
IL TRATTAMENTO È LECITO SOLO SE E NELLA MISURA IN CUI RICORRE ALMENO UNA DELLE SEGUENTI CONDIZIONI:

- a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
- b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte;
- c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;
- d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
- e) il trattamento è necessario per l'esecuzione di un compito di **interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento;
- f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;



IL TRATTAMENTO È LECITO SOLO SE E NELLA MISURA IN CUI RICORRE ALMENO UNA DELLE SEGUENTI CONDIZIONI:

- a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità
- b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte
- c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento
- d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica
- e) il trattamento è necessario per l'esecuzione di un compito di **interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento
- f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore



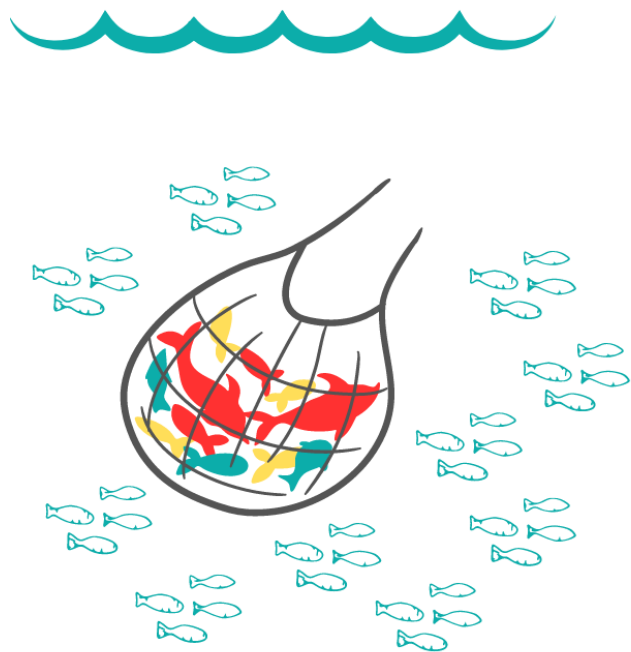
- a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità

Art. 4, n. 11 GDPR

«*consenso dell'interessato*»

qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento





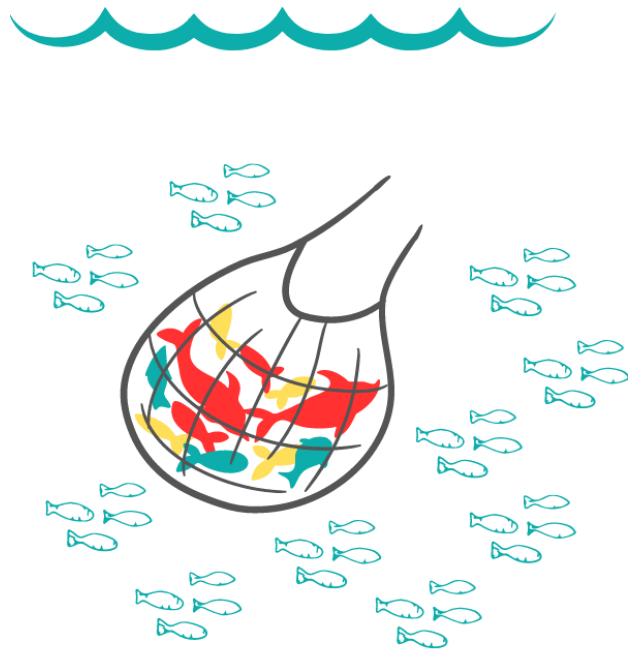
f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi

C. 47 GDPR

«I legittimi interessi di un titolare del trattamento (...) o di terzi possono costituire una base giuridica del trattamento, **a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.** (...)

In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. **Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali».**





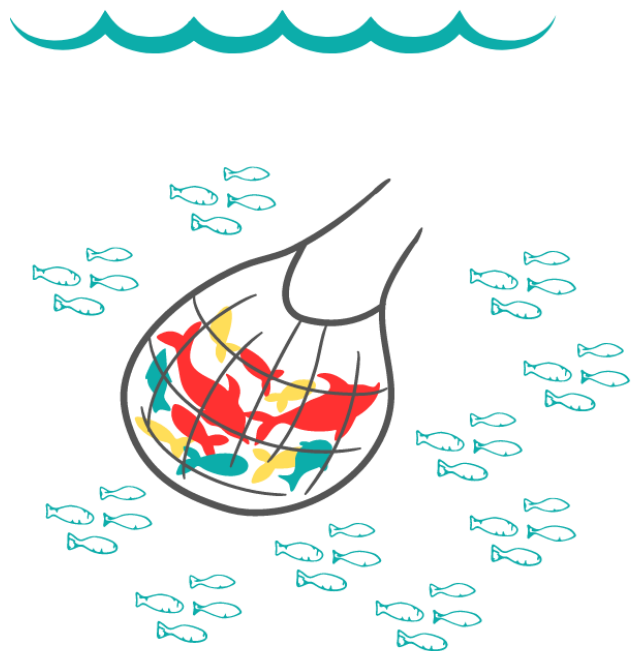
f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi

----- NON È COMUNQUE BASE GIURIDICA IDONEA PER IL TRATTAMENTO DI DATI PARTICOLARI EX ART. 9 GDPR

----- NON VERREBBE COMUNQUE MENO L'OBBLIGO DI FORNIRE UN'ADEGUATA INFORMATIVA

----- DAL PUNTO DI VISTA PRATICO, QUESTA TECNOLOGIA CONSENTE AGLI INTERESSATI DI ESERCITARE I LORO DIRITTI?





e) il trattamento è necessario per l'esecuzione di un compito di **interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento





GPDP

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

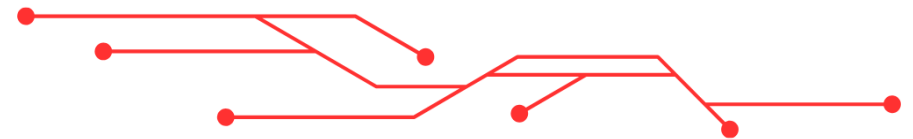
Der Hamburgische
Beauftragte für Datenschutz
und Informationsfreiheit



«Discussion Paper: Large Language
Models and Personal Data»

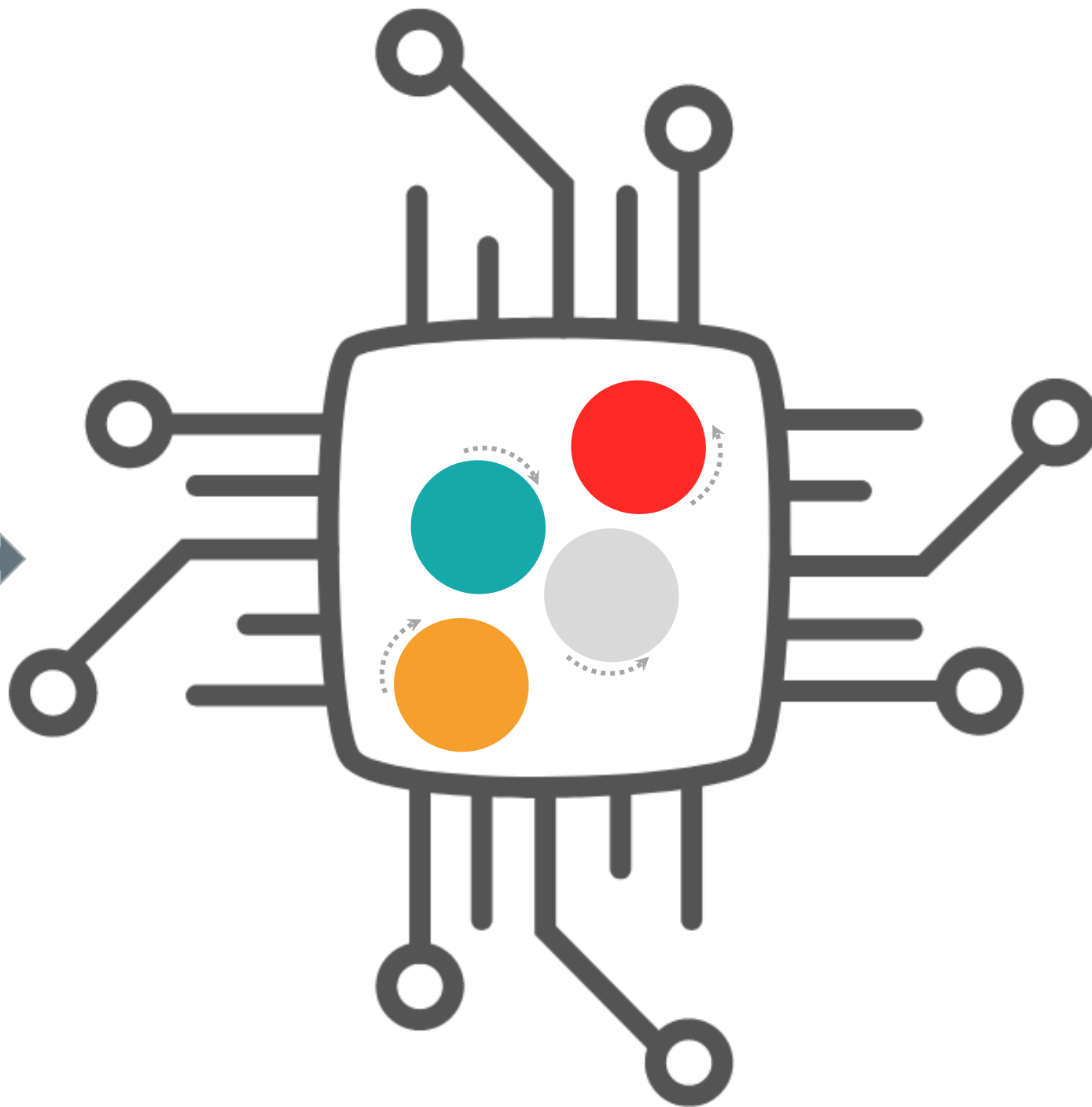
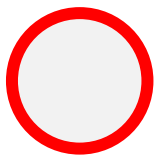
15 luglio 2024

“When an LLM, functioning as a component of an AI system, processes prompts (so-called “in-ference”), the LLM’s output may contain information relating to natural persons, especially if the prompt specifically asks for it. This raises the question of whether personal data is stored in an LLM. (...) Understanding how linguistic information is processed and stored in Large Language Models (LLMs) is vital for addressing the question at hand.”

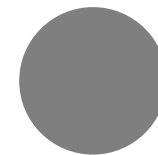




INPUT



OUTPUT



INPUT

TOKENIZZAZIONE + EMBEDDING

«Ist ein LLM
personenbezogen?»



[I] [st] [e] [in] [LL] [M]
[person] [en] [be] [z]
[ogen] [?]

«Mia Müller hat
gelogen.»



[M] [ia] [Mü] [ller] [hat]
[gel] **[ogen]** [.]

«gelb?»

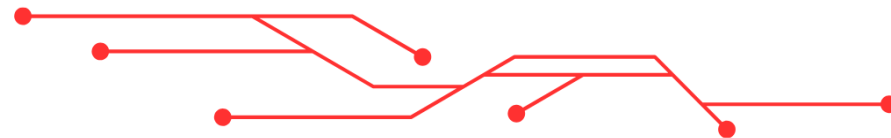


[gel] [b] [?]

[gel] + **[ogen]** → mentire

[gel] [b] → giallo

[M] [ia] [Mü] [ller] →
frammenti linguistici, le relazioni
vettoriali tra questi token
determinano la
probabilità/frequenza con cui si
combinano tra di loro



Der Hamburgische
Beauftragte für Datenschutz
und Informationsfreiheit



«Discussion Paper: Large Language
Models and Personal Data»

15 luglio 2024

*“La semplice detenzione di un LLM non costituisce un trattamento ai sensi dell'articolo 4 (2) del GDPR. Questo perché **negli LLM non vengono memorizzati dati personali**. Nella misura in cui i dati personali sono trattati in un sistema di IA supportato da LLM, il trattamento deve essere conforme ai requisiti del GDPR. Ciò vale in particolare per l'output di tale sistema di IA.*

*«L’addestramento di un LLM che utilizza dati personali deve essere conforme alle norme sulla protezione dei dati. Durante l’addestramento, devono essere rispettati anche i diritti degli interessati. Tuttavia, **le potenziali violazioni durante la fase di addestramento degli LLM non pregiudicano la liceità dell'utilizzo di tale modello all'interno di un sistema di IA.**»*





**Presenta 11 reclami a Garanti europei,
inclusa l'autorità italiana**



**Dati degli utenti usati per l'addestramento del
proprio algoritmo sulla base dell'interesse
legittimo e consentendo l'"opt-out"**

“Worldcoin is designed to become the world's largest privacy-preserving human identity and financial network, giving ownership to everyone. Worldcoin aims to provide universal access to the global economy no matter your country or background, establishing a place for all of us to benefit in the age of AI.”

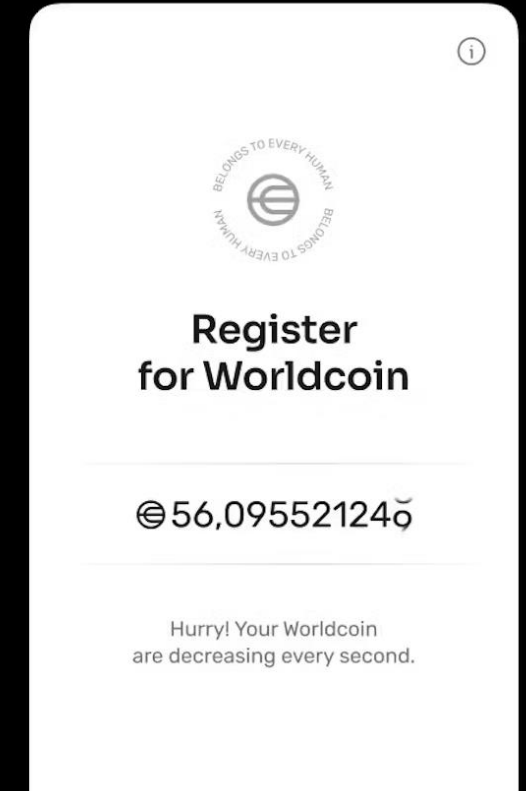
For every human

Privacy-first. Owned by everyone.



Receive Your Worldcoin

Verify now to receive the maximum amount of Worldcoin.
Amount decreases while you wait.



<https://worldcoin.org/>



Commissione
europea



| **GPDP** |

Chiediamolo a ChatGpt...

ci sono dei problemi di coordinamento tra AI act e GDPR?

Sì, ci sono alcuni problemi di coordinamento tra l'AI Act e il GDPR.

1. **Ambito di applicazione:** L'AI Act si concentra sulle applicazioni dell'IA e sui rischi associati, mentre il GDPR si occupa della protezione dei dati personali. Le due normative potrebbero sovrapporsi in aree come il trattamento dei dati per addestrare modelli di IA.
2. **Trasparenza:** Il GDPR richiede la trasparenza nel trattamento dei dati, mentre l'AI Act prevede requisiti specifici per la trasparenza dei sistemi di IA. Trovare un equilibrio tra le due normative può essere complicato.
3. **Responsabilità:** Le questioni di responsabilità per l'uso dell'IA e la protezione dei dati possono creare confusione su chi sia responsabile in caso di violazioni.
4. **Definizioni e terminologie:** Le diverse definizioni utilizzate nelle due normative possono portare a interpretazioni divergenti.

Questi aspetti richiedono un'attenta considerazione per garantire una cooperazione efficace tra le due normative.

Se la risoluzione di questi problemi dovesse essere affidata ad un solo organo, a chi la affideresti?



Affiderei la risoluzione di questi problemi a un'agenzia indipendente europea, composta da esperti in diritto della privacy, tecnologia e etica. Questa agenzia potrebbe facilitare il dialogo tra le autorità di protezione dei dati e le agenzie di regolamentazione dell'IA, garantendo coerenza e coordinamento nell'applicazione delle normative.

perchè non al legislatore europeo?



Affidare la risoluzione al legislatore europeo potrebbe essere problematico per diversi motivi:

1. **Tempo e complessità:** Le procedure legislative possono richiedere molto tempo, e le tecnologie IA evolvono rapidamente. Una risposta agile è necessaria.
2. **Interesse e specializzazione:** Un'agenzia dedicata potrebbe avere esperti specializzati in IA e privacy, mentre il legislatore potrebbe non avere la stessa profondità di conoscenza.
3. **Mediazione e dialogo:** Un organo indipendente potrebbe facilitare meglio il dialogo tra diverse parti interessate (governi, industrie, cittadini), mentre il legislatore potrebbe trovarsi più influenzato da interessi politici.
4. **Implementazione pratica:** Un'agenzia potrebbe concentrarsi sulla pratica e sull'applicazione delle normative, mentre il legislatore si occupa di creare le leggi stesse.

In sintesi, un organo indipendente potrebbe essere più flessibile e reattivo nell'affrontare le sfide emergenti.

A teal abstract shape in the top-left corner of the page.

**GRAZIE PER
L'ATTENZIONE**

A red graphic consisting of several horizontal lines of varying lengths, connected by diagonal lines, with small red dots at the ends, resembling a circuit board or a stylized signature.A vertical orange dashed line separating the two columns of text.

Avv. Ilaria Feriti

Firenze, 10 ottobre 2024

A teal abstract shape in the bottom-right corner of the page.