

*Principali standard su AI:  
applicazione e prospettive*

# Agenda

- Presentazione del docente
- Introduzione agli standard
- Rapporto tra qualità dei dati e apprendimento
- La strategia europea
- Rischi connessi con l'AI
- Il regolamento AI ACT
- Le norme per la conformità all'AI
- Case Study
- Conclusioni



# **Presentazione del docente**

# Presentazione del docente

Presidente della Commissione Tematica di Intelligenza Artificiale



CV

## DIPENDENTE PUBBLICO

27 anni

01/09/22 - oggi

3 anni



- STAFF ISPETTORE GENERALE
- DIRETTORE IT, LOGISTICA E TRANSIZIONE DIGITALE
- RESPONSABILE DELLA TRANSIZIONE DIGITALE (ART. 17, CAD)

13/10/22 - 14/07/24

02/03/99 - 31/08/22



- PROFESSIONISTA INFORMATICO
- COORDINATORE DI SETTORE - CONSULENZA PER L'INNOVAZIONE DIGITALE

23 anni

## DIPENDENTE PRIVATO

4 anni

01/02/95 - 30/06/95



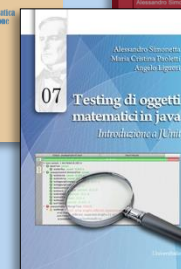
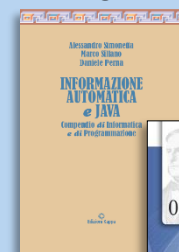
01/07/95 - 01/03/99



## PROFESSORE A CONTRATTO

24 anni

- ALFABETIZZAZIONE INFORMATICA
- TEORIA DELL'INFORMAZIONE E TECNICHE DI ELABORAZIONE DIGITALE
- TECNICHE INFORMATICHE
- FONDAMENTI DI PROGRAMMAZIONE
- CALCOLATORI E SISTEMI OPERATIVI
- ARCHITETTURA DEI SISTEMI DI ELABORAZIONE



12 A.A. 2001-2018



10 A.A. 2015-2025



16 A.A. 2008-2026



UNI/CT 504 SOFTWARE ENGINEERING  
UNI/CT 510 SECURITY

UNI/CT 533 ARTIFICIAL INTELLIGENCE

ISO/IEC JTC1 SC7 SOFTWARE AND SYSTEMS ENGINEERING  
ISO/IEC JTC1 SC27 INFORMATION SECURITY, CYBERSECURITY AND PRIVACY  
ISO/IEC JTC1 SC 42 CEN/CLC JTC 21

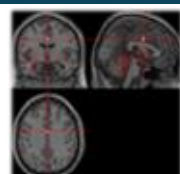
16 anni  
13/05/09 - 31/12/25

01/01/26 - oggi

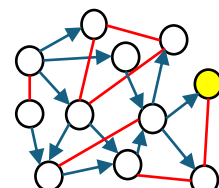
1994



Prof. Daniele Nardi



fMRI



BCI



Editorial Team

# Attività di ricerca

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

## ISO/IEC STANDARDS AND DESIGN OF AN ARTIFICIAL INTELLIGENCE SYSTEM

IWESQ 2024, 3RD DECEMBER 2024, [HTTPS://CEUR-WS.ORG/VOL-3916/](https://ceur-ws.org/Vol-3916/) PP.39-43  
SIMONETTA A., PAOLETTI M.C.

## THE SQUARE SERIES AS A GUARANTEE OF ETHICS IN THE RESULTS OF AI SYSTEMS

IWESQ 2023, 4TH DECEMBER 2023 [HTTPS://CEUR-WS.ORG/VOL-3612/](https://ceur-ws.org/Vol-3612/) PP.17-21  
SIMONETTA A., PAOLETTI M.C., NAKAIJMA T.

## ETHICS IN ARTIFICIAL INTELLIGENCE SYSTEMS

INAIL SEMINAR, DECEMBER 4-6, 2023, SAPIENZA UNIVERSITY OF ROME,  
PAOLETTI M.C., SIMONETTA A., NATALE D.

## APPLICATION OF AI FOR SOCIAL AND LABOR REINTEGRATION IN THE OPERATION OF COMPLEX MACHINERY

INAIL SEMINAR, DECEMBER 4-6, 2023 SAPIENZA UNIVERSITY OF ROME  
MURATORE M., PAOLETTI M.C., SIMONETTA A., COLAFEMMINA.G.

## FAIRNESS METRICS AND MAXIMUM COMPLETENESS FOR THE PREDICTION OF DISCRIMINATION (\*)

IWESQ 2022, TOKYO, 6TH DECEMBER 2022, [HTTPS://CEUR-WS.ORG/VOL-3356/](https://ceur-ws.org/Vol-3356/)  
SIMONETTA A., NAKAIJMA T., PAOLETTI M.C., VENTICINQUE A.

(\*) RESEARCH ARTICLES REFERRED BY CEN/CLC/TR **18115:2024** "DATA GOVERNANCE AND QUALITY FOR AI WITHIN THE EUROPEAN CONTEXT"

BIAS  
AI  
SQUARE

## THE USE OF MAXIMUM COMPLETENESS TO ESTIMATE BIAS IN AI BASED RECOMMENDATION SYSTEMS

SYSTEM 2022, BRUNICO JULY 23-31, [HTTPS://CEUR-WS.ORG/VOL-3360/](https://ceur-ws.org/Vol-3360/)  
SIMONETTA A., PAOLETTI M.C., VENTICINQUE A.

## USING THE SQUARE SERIES AS A GUARANTEE FOR GDPR COMPLIANCE (\*)

IWESQ 2021, 8TH DECEMBER 2021, [HTTP://CEUR-WS.ORG/VOL-3114/PAPER-05.PDF](http://ceur-ws.org/Vol-3114/PAPER-05.PDF)  
SIMONETTA A., PAOLETTI M.C., VENTICINQUE A.

## INTEGRATING SQUARE DATA QUALITY MODEL WITH ISO 31000 RISK MANAGEMENT TO MEASURE AND MITIGATE SOFTWARE BIAS (\*)

IWESQ 2021, 8TH DECEMBER, 2021, [HTTP://CEUR-WS.ORG/VOL-3114/PAPER-04.PDF](http://ceur-ws.org/Vol-3114/PAPER-04.PDF)  
SIMONETTA A., VETRÒ A., PAOLETTI M.C., TORCHIANO M.

## METRICS FOR IDENTIFYING BIAS IN DATASETS (\*)

ICYRIME 2021, [HTTPS://CEUR-WS.ORG/VOL-3118/p02.pdf](https://ceur-ws.org/Vol-3118/p02.pdf)  
SIMONETTA A., TRENTA A., PAOLETTI M.C., VETRÒ A.

## SECURITY / SOFTWARE

**CODE PROTECTION TECHNIQUES WHEN DISTRIBUTED IN SOURCE FORMAT: AN ADOBE CONNECT POD WRITTEN IN JAVASCRIPT**  
SYSTEM 2021, JULY 27-29, 2021, [HTTPS://CEUR-WS.ORG/VOL-3092/p06.pdf](https://ceur-ws.org/Vol-3092/p06.pdf)  
SIMONETTA A., RINALDI F.

**A FORENSIC METHODOLOGY FOR THE IDENTIFICATION OF ILLICIT DATA LEAKAGE**  
SYSTEM 2021, JULY 27-29, 2021, [HTTPS://CEUR-WS.ORG/VOL-3092/p01.pdf](https://ceur-ws.org/Vol-3092/p01.pdf)  
SIMONETTA A., FAZIO L., PAOLETTI M.C.

**A SIMPLE METHOD FOR EXTRACTING REAL DEPENDENCIES BETWEEN DATA AND SOFTWARE APPLICATIONS**  
INAIL SEMINAR, 23-25 OCTOBER 2018, SIMONETTA A.

## NEW COMPUTING ARCHITECTURES

**MULTI-VALUED LOGIC DIGITAL CIRCUITS FOR REALIZING A COMPLETE COMPUTER ARCHITECTURE**, ICYRIME 2022, AUGUST 26-29, 2022, [HTTPS://CEUR-WS.ORG/VOL-3398](https://ceur-ws.org/Vol-3398), SIMONETTA A., PAOLETTI M.C., VENTICINQUE A.

**A NEW APPROACH FOR DESIGNING OF COMPUTER ARCHITECTURES USING MULTI-VALUE LOGIC**, IJASEIT, VOL. 11 (2021) No. 4, PAGES: 1440-1446, DOI:10.18517/IJASEIT.11.4.15778, SIMONETTA A., PAOLETTI M.C., MURATORE M.

**DESIGNING DIGITAL CIRCUITS IN MULTI-VALUED LOGIC**, IJASEIT, VOL. 8 (2018) No. 4, DOI:10.18517/IJASEIT.8.4.5966, SIMONETTA A. & PAOLETTI M.C.

# Introduzione agli standard

# Cosa è uno standard?



Estratto dal sito <http://www.uni.com> :

Una norma è un documento tecnico volontario, che stabilisce le "regole dell'arte" per prodotti, processi o servizi, garantendo sicurezza, qualità e prestazioni.

Basate sul consenso, non sono obbligatorie per legge, ma diventano vincolanti se recepite da normative o contratti.

La conformità ad uno standard si chiama "certificazione" ed assicura che il risultato finale, che di solito è variabile, sia sempre lo stesso.





# Cosa è uno standard?

Secondo il Regolamento UE 1025, per "norma" si intende:

«una specifica tecnica, adottata da un organismo di normazione riconosciuto, per **applicazione ripetuta** o continua, alla quale non è obbligatorio conformarsi»

**Applicazione ripetuta:** Serve a risolvere problemi ricorrenti (non è una soluzione "una tantum").

**Organismo riconosciuto:** Non chiunque può creare uno standard; deve farlo un ente ufficiale (come il CEN, il CENELEC o l'ETSI a livello europeo).

**Volontarietà:** A differenza di un regolamento o di una direttiva, lo standard di per sé non è una legge. Sei libero di non seguirlo, a meno che una legge non lo renda obbligatorio per specifici settori.

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI



# Le 4 Categorie di Standard per l'UE

Il regolamento UE distingue gli standard in base a "chi" li emette:

Tipo di Norma	Emessa da	Esempio
<b>Internazionale</b>	Organismi come l'ISO o l'IEC.	ISO 9001 (Qualità)
<b>Europea (EN)</b>	CEN, CENELEC o ETSI.	EN 71 (Sicurezza giocattoli)
<b>Nazionale</b>	Enti nazionali (come l'UNI in Italia).	UNI 11337 (BIM)
<b>Armonizzata</b>	Enti europei, ma su richiesta della Commissione UE	Norme per la marcatura CE

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

# Organizzazioni che sviluppano standard

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

## Internazionali



International Organization of Standards



International Electrotechnical Commission



International Telecommunication

## Europee



European Telecommunications Standards Institute



European Committee for Electrotechnical Standardization



European Committee for Standardization

## Nazionali



Comitato Elettrotecnico italiano



Ente di italiano di normazione

# Altre organizzazioni o Consorzi

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI



Internet Engineering Task Force



World Wide Web Consortium



Advancing open standards for the information society



Institute of Electrical and Electronics Engineers



# Standard internazionali



- È uno standard adottato da un'organizzazione di standard internazionali (ISO, IEC) e rispondente alle esigenze internazionali
- È disponibile in 3 lingue ufficiali ISO e IEC: inglese 🇬🇧 , francese 🇫🇷 e russo 🇷🇺
- È venduto direttamente da ISO, IEC o dai suoi membri nazionali
- I membri ISO o IEC non sono obbligati ad adottare gli standard internazionali come standard nazionali

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE




AI ACT

CASE  
STUDY

CONCLUSIONI

# Standard Europei (EN)



- È uno standard che è stato ratificato da una delle tre organizzazioni europee di standardizzazione riconosciute: CEN, CENELEC o ETSI
- È emesso nelle tre lingue ufficiali: inglese  , francese  e tedesco 
- CEN o CENELEC non vendono o distribuiscono standard



CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

# International Organization for Standardization



- L'ISO nasce nel 1947 ed è la più grande organizzazione del mondo per lo sviluppo di standard internazionali.
- Ha sviluppato più di 25.000 standard e ne pubblica ogni anno circa 1.000
- ISO è un network di istituti nazionali di 166 Paesi con un segretariato centrale a Ginevra che coordina il sistema.
- Si occupa di tutti le esigenze di standardizzazione, eccetto quelle elettriche ed elettroniche.



# International Organization for Standardization

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI



- Tra gli Standard ISO più utilizzati:
  - ✓ Sistema universale di misura (sistema metrico decimale)
  - ✓ Card telefoniche e bancomat
  - ✓ ISO 9000 per la verifica della qualità di prodotti e procedure
  - ✓ container, e tutti gli apparecchi connessi: camion, aerei, treni, navi, depositi, gru.
  - ✓ Sistemi di filettatura di viti e bulloni



# International Electrotechnical Commission



- Fondata nel 1906, la IEC è l'organizzazione leader a livello mondiale per la preparazione e la pubblicazione di standard internazionali per tutte le tecnologie **elettriche**, **elettroniche** e **correlate**.
- IEC collabora con ISO e con ITU per garantire che gli standard internazionali si integrino perfettamente e si completino a vicenda.
- ISO ed IEC collaborano esplicitamente sugli argomenti di Information Technology, che hanno aspetti di interesse per entrambi.
- Il **Joint Technical Committee 1** (JTC 1) è il comitato tecnico congiunto che si occupa degli aspetti di standardizzazione dell'IT per ISO ed IEC.





# Chi sviluppa standard in Italia?

- Gli organismi nazionali di standard, riconosciuti a livello europeo dal CEN, dal CENELEC e dall'ETSI ed a livello internazionale dall'ISO, IEC sono:

**Nazionali**



Comitato Elettrotecnico italiano → Elettrotecnica



**uni**  
UN MONDO FATTO BENE

→ Tutto il resto

# Enti Federati



**Associazione per  
l'Unificazione nel settore  
dell'industria chimica**



**Comitato Italiano GAS**



**Commissione Tecnica di  
Unificazione  
nell'Autoveicolo**



**Ente italiano di  
unificazione delle materie  
plastiche**



**UNSIDER**

**Ente italiano di  
unificazione siderurgica**



**Comitato  
Termotecnico  
Italiano**



UNINFO è una libera Associazione a carattere tecnico-scientifico e divulgativo senza fine di lucro (diretto o indiretto) il cui scopo è promuovere, realizzare e diffondere la normazione tecnica nel settore delle tecnologie dell'informazione e delle comunicazioni (in breve ICT) e delle loro applicazioni (di seguito “settore di competenza”), sia a livello nazionale che europeo ed internazionale. (Art. 1 - Statuto [https://www.uninfo.it/wp-content/uploads/2025/05/Statuto\\_2025.pdf](https://www.uninfo.it/wp-content/uploads/2025/05/Statuto_2025.pdf))

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

# Quadro di sintesi

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

## International Standardization Organizations



**International Organization  
for Standardization**



**International Electrotechnical  
Commission**



**International Telecommunication Union**



**Prysmian  
Group**



**STMicroelectronics  
Telespazio**



**RaiWay**



**Sirti**

**TIM**

IL Joint Technical Committee 1 (<https://jtc1info.org/>) è responsabile per gli aspetti che riguardano l'Information Technology (IT) per ISO e IEC



**ITALIAN  
STANDARDIZATION  
BODY**

**UNINFO**



## European Standardization Organizations



**European  
Committee for  
Electrotechnical  
Standardization**

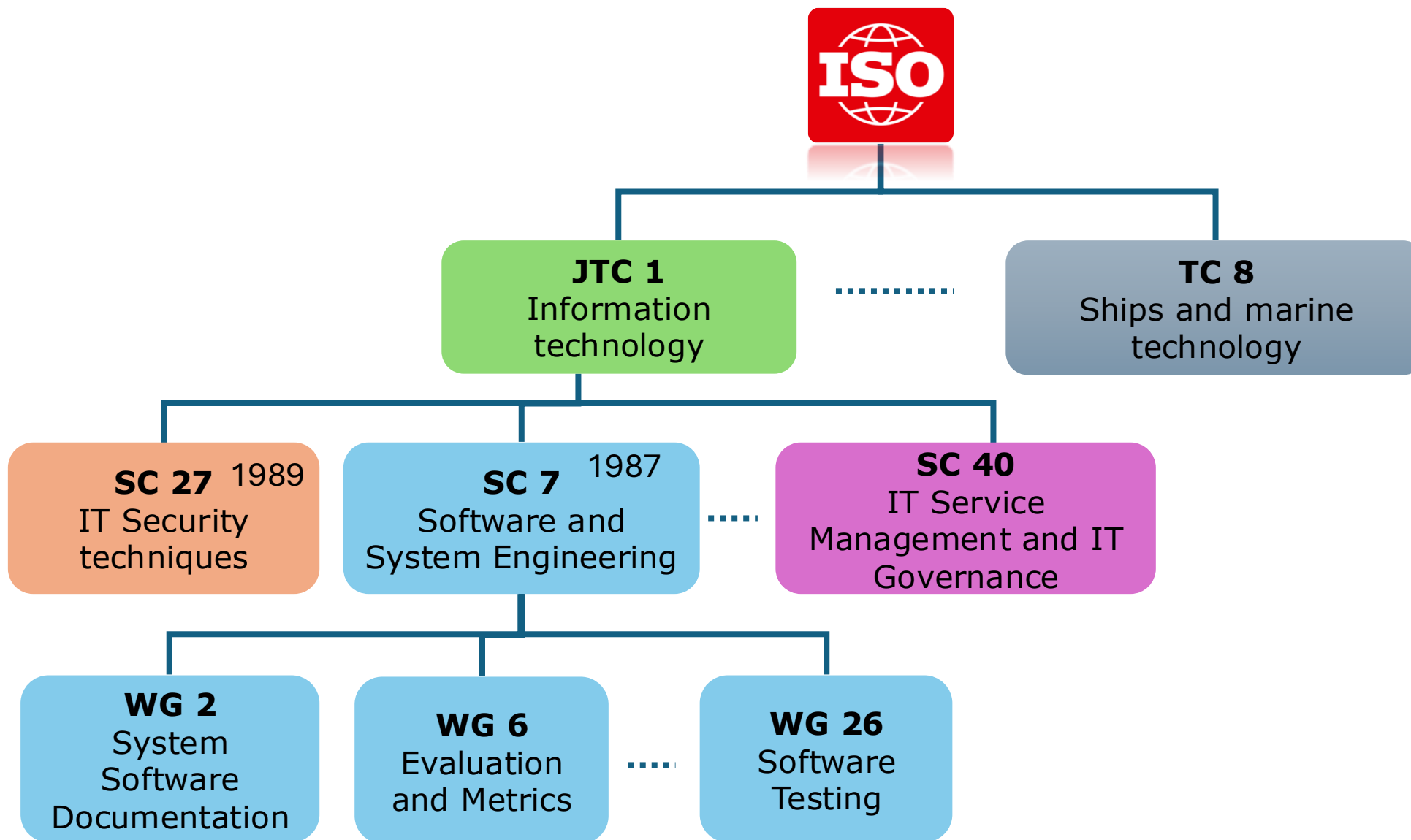


**European Committee  
for Standardization**



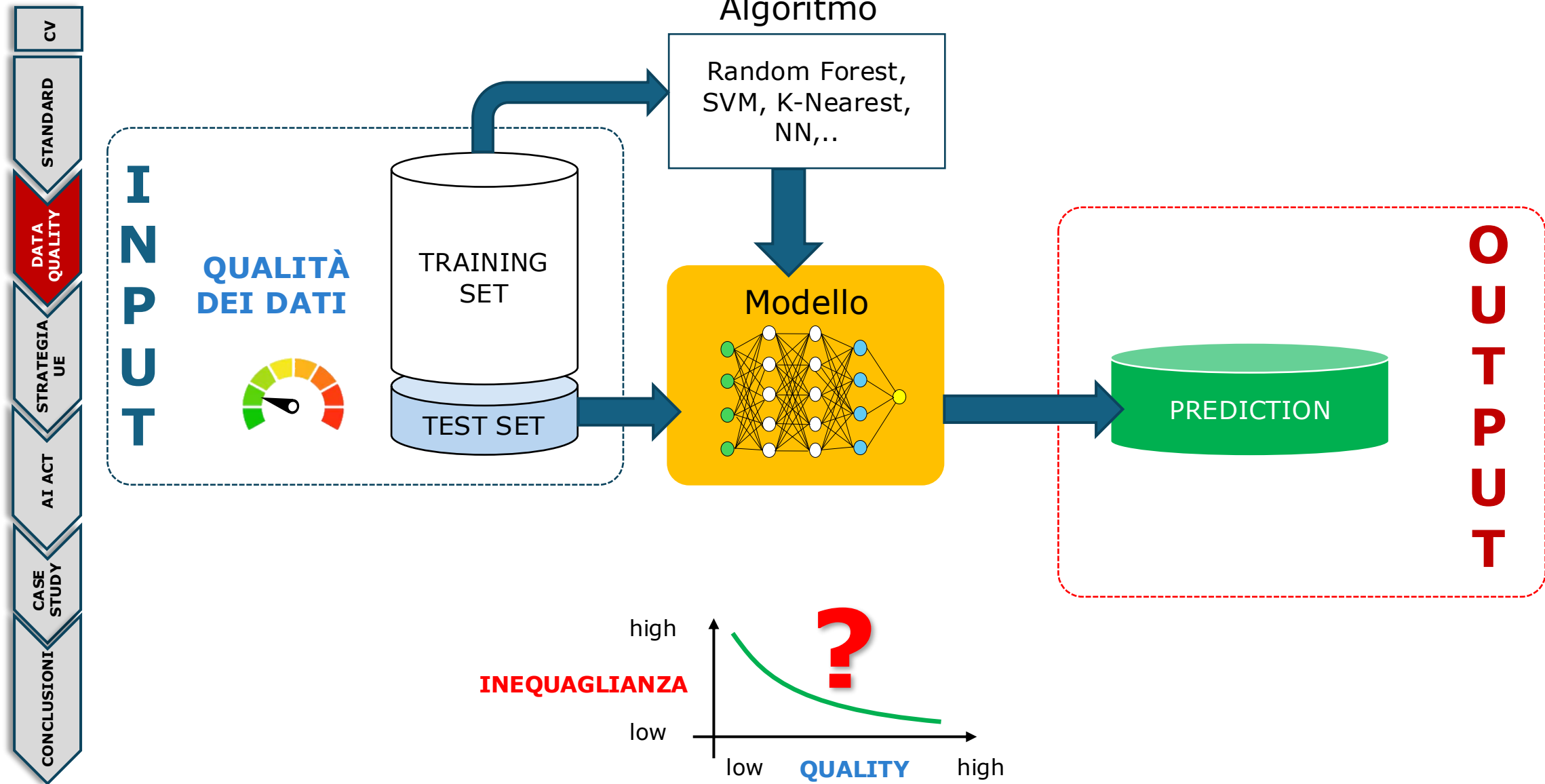
**European Telecommunications  
Standards Institute**

# Organizzazione dell'SC7



# Rapporto tra qualità dei dati e apprendimento

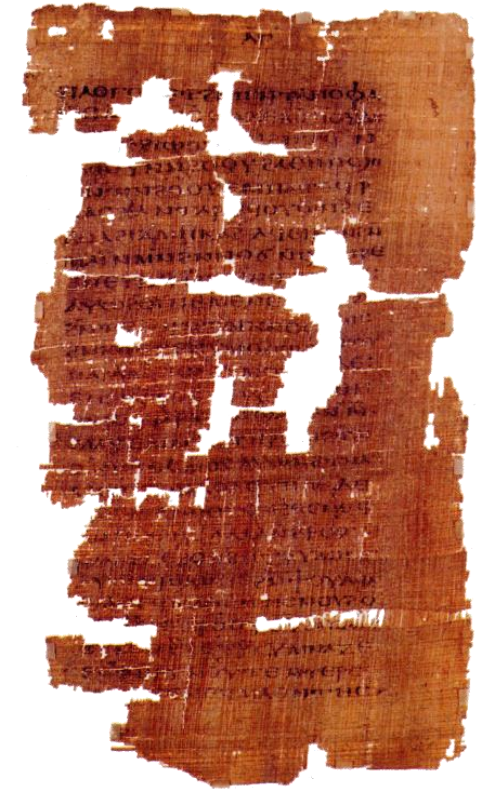
# Rapporto tra qualità dei dati e apprendimento



# Longevità dei dati

I dati sono una risorsa strategica ed hanno una maggiore stabilità rispetto ad altre componenti (processi, tecnologie, organizzazione).

La longevità dei dati può essere compromessa per l'obsolescenza delle tecnologie o la deteriorabilità dei supporti.



il Vangelo di Giuda si stima sia stato realizzato tra il 130 e il 170 circa





# Rapporto tra dati ed informazione

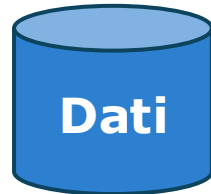
Le **informazioni** vengono dedotte in modo essenziale attraverso i **dati**



Livello  
concettuale



Livello  
fisico



rotta, altitudine,  
velocità,...





# I dati forniscono informazione?

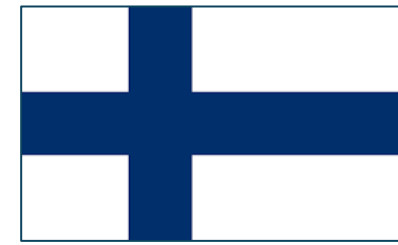


Sono gli orari di cartelli stradali che si trovano in Finlandia  
Perchè sono diversi?



Esempio estratto dal prof. Paolo Atzeni durante le lezioni di Basi di Dati

# I dati forniscono informazione?



**Lun-Ven**



**Sabato**



**Festivo**

Sono gli orari di cartelli stradali che si trovano in Finlandia  
Perchè sono diversi?

Per essere compresi i dati necessitano di una fase di interpretazione, quindi la necessità di avere dei **Modelli!**

Esempio estratto dal prof. Paolo Atzeni durante le lezioni di Basi di Dati

# Attualità del dato



CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

# Coerenza del dato



CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

# Come misuriamo la «Qualità» dei dati?

- I dati sono importanti e prescindono dalla tecnologia
- I modelli aiutano a comprendere il significato dei dati
- Dai dati è possibile dedurre informazione, ma che succede se un sistema di AI apprende da dati incompleti?
- Se i dati non sono di «qualità» ci sono molti effetti collaterali:
  - possiamo dedurre informazioni errate
  - siamo limitati nell'interoperabilità
- Ok, come misuriamo la «qualità» dei dati?





# Norme per la Qualità dei dati

## **UNI ISO / IEC 25012:2014**

Ingegneria del software - Requisiti di qualità e valutazione del prodotto software (SQuaRE)

### **Modello di qualità dei dati**

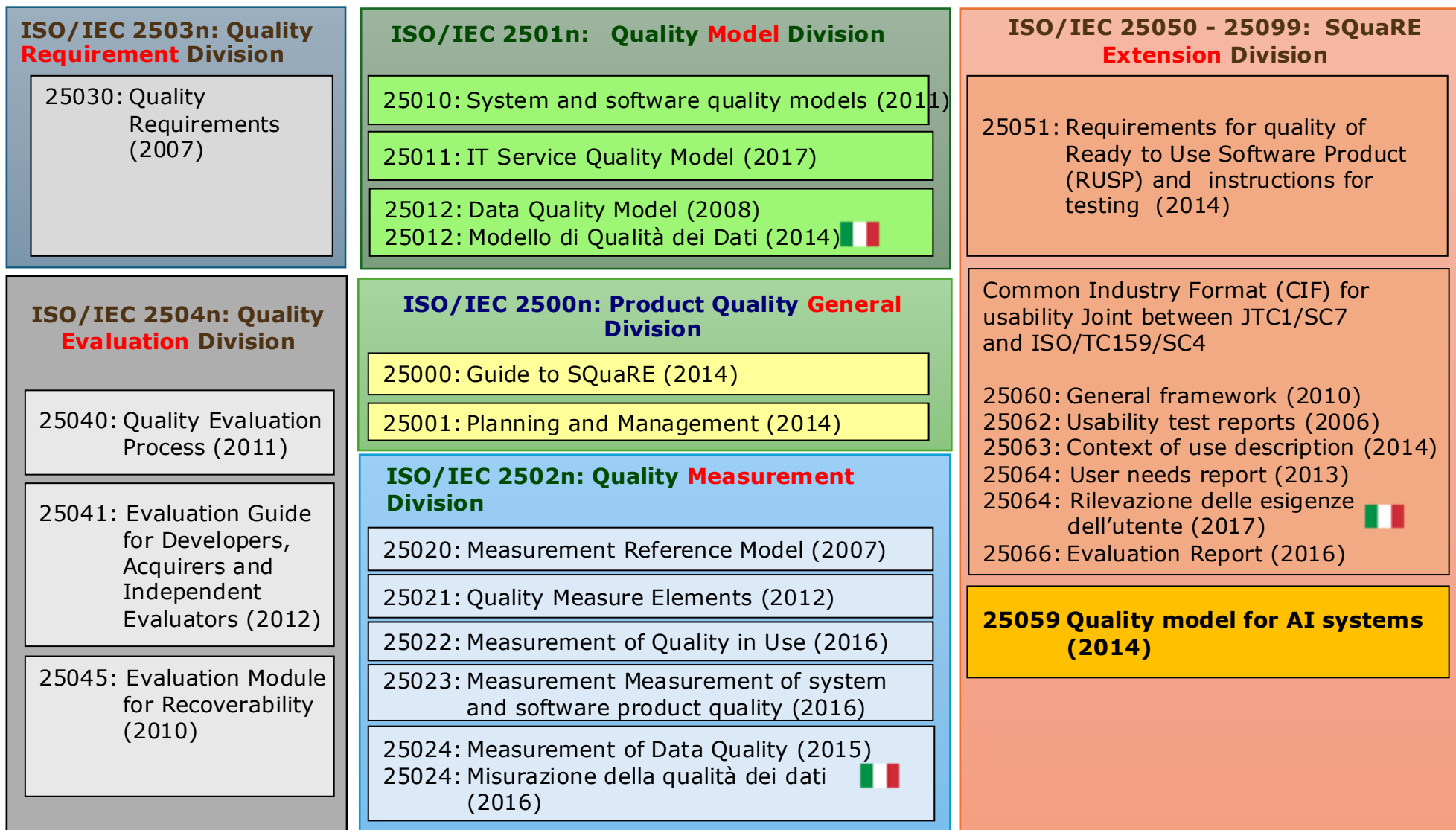
## **UNI CEI ISO / IEC 25024:2016**

Ingegneria del software e di sistema - Requisiti e valutazione della qualità dei sistemi e del software (SQuaRE)

### **Misurazione della qualità dei dati**



# Architettura della serie SQuaRE



UNI/TS 11725:2018 Ingegneria del software e di sistema - Linee guida per la misurazione della qualità dei dati



# Standard processo vs prodotto

- con questa nuova serie di standard, dopo oltre trenta anni di ingegneria del software, l'attenzione è posta verso il prodotto reso all'utente indipendentemente dal modo/processo attraverso il quale è stato realizzato



CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

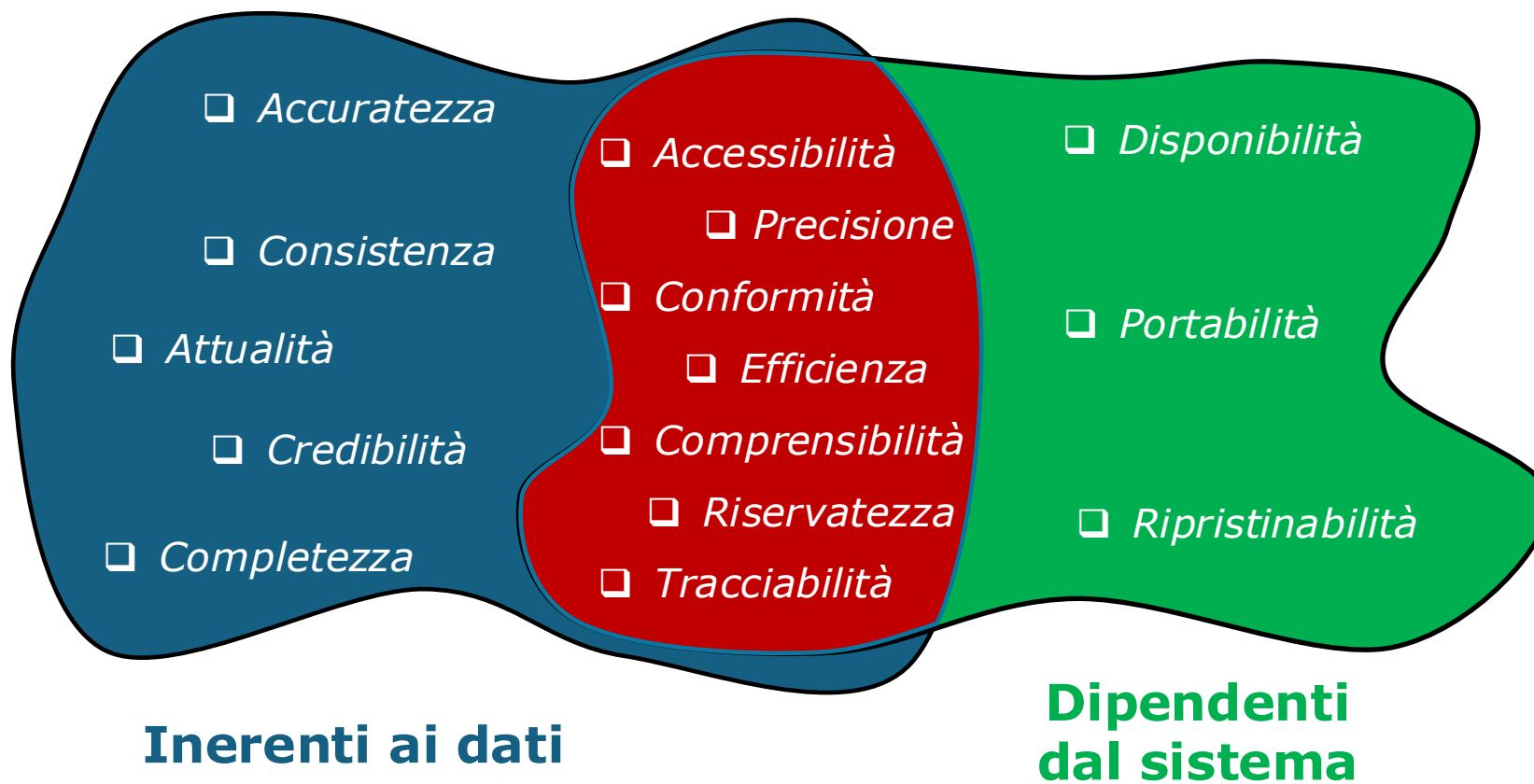
CASE  
STUDY

CONCLUSIONI



# Modello di Qualità dei dati

- L'ISO/IEC 25012 categorizza gli attributi di qualità in quindici caratteristiche considerate da due differenti punti di vista: inerente ai dati e dipendente dal sistema.



# Quadro normativo

**Direttiva 2025/2 (Solvency II) (Artt. 48 e 82)**  
«...appropriatezza, completezza e accuratezza»

**EU GDPR**

**CODICE ASSICURAZIONI PRIVATE**  
«...qualità dei dati nel calcolo delle riserve  
...e nella trasmissione all'Autorità  
(accessibili, coerenti, affidabili,  
attuali,...)»

**Regolamenti  
IVASS**  
(n.18 e  
21/2008  
...n.36/2017  
Art. 6)

**Art. 5  
Principi  
applicabili al  
trattamento di  
dati personali**

**Art. 32  
Sicurezza  
del  
trattamento**

**Regole Tecniche  
Basi Dati  
Critiche  
DET. COMM. N.  
68/2013**

**Piano Triennale  
per l'informatica  
nella PA 2024-26**

**Quadro di riferimento normativo e  
tecnico per le Piattaforme di  
Approvvigionamento Digitale  
DET. N.267/2025**



**UNI ISO/IEC 25012**  
Modello di Qualità dei Dati

**UNI CEI ISO/IEC 25024**  
Misurazione della  
qualità dei dati



CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

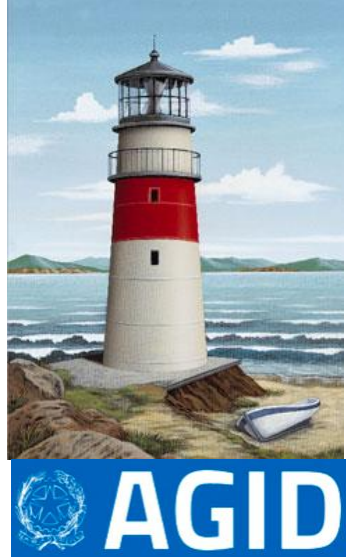
AI ACT

CASE  
STUDY

CONCLUSIONI

# Determinazione Commissariale n.68/2013

## Regole Tecniche per le Basi Dati Critiche



Le basi di dati di interesse nazionale:

- Repertorio nazionale dei dati territoriali;
- Anagrafe nazionale della popolazione residente (ANPR);
- Banca dati nazionale dei contratti pubblici;
- Casellario giudiziale;
- Registro delle imprese;
- Archivi automatizzati in materia di immigrazione e di asilo.

Si identificano come basi di dati critiche quelle di interesse nazionale che:

- a) siano riferibili a dati raccolti e gestiti da o per conto dell'amministrazione titolare, affinché possano rispondere alle caratteristiche di credibilità, o autenticità della fonte, in linea con la definizione contemplata dallo standard internazionale sulla qualità dei dati **ISO/IEC 25012 «Data quality model»**;
- b) abbiano un elevato impatto socio-economico;
- c) siano al servizio di procedimenti amministrativi di competenza di altre pubbliche amministrazioni per l'assolvimento dei propri compiti istituzionali;
- d) siano disponibili a supportare procedimenti amministrativi transfrontalieri in esecuzione di norme o direttive comunitarie;
- e) non siano sostituibili o surrogabili nell'erogazione dei servizi cui sono deputate, in favore delle pubbliche amministrazioni e degli utenti finali.



# Determinazione Commissariale n.68/2013

## Regole Tecniche per le Basi Dati Critiche

In relazione allo specifico contesto d'uso e alle finalità perseguite dalla norma, le basi di dati critiche devono assicurare il valore intrinseco dei dati in modo che gli attributi dei dati stessi siano adeguati rispetto alle caratteristiche di "inerenza" definite nell'ambito del suddetto standard **ISO/IEC 25012**, di seguito sintetizzate

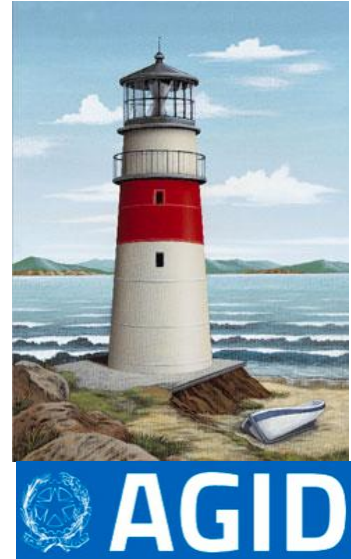
Queste quattro caratteristiche sono:

**Accuratezza** il dato, e i suoi attributi, rappresenta correttamente il valore reale del concetto o evento cui si riferisce;

**Completezza** il dato risulta esaustivo per tutti i suoi valori attesi e rispetto alle entità relative (fonti) che concorrono alla definizione del procedimento;

**Coerenza** il dato, e i suoi attributi, non presenta contraddittorietà rispetto ad altri dati del contesto d'uso dell'amministrazione titolare;

**Attualità** il dato, e i suoi attributi, è del "giusto tempo" (è aggiornato) rispetto al procedimento cui si riferisce.



A-C-C-A



# PIANO TRIENNALE

per l'informatica nella pubblica amministrazione 2024-26

## Capitolo 5 - Dati e Intelligenza Artificiale Open data e data governance

### Obiettivo 5.2 - Aumentare la qualità dei dati e dei metadati

RA5.2.4 - Aumento del numero di dataset documentati sul portale dati.gov.it che rispettano la caratteristica di qualità “attualità” (o tempestività di aggiornamento) di cui allo Standard **ISO/IEC 25012**

- Target 2024 - Definizione baseline
- Target 2025 - Almeno il 30% dei dati documentati nel portale per ciascuna PA
- Target 2026 - Almeno il 50% dei dati documentati nel portale per ciascuna PA

AGID

PIANO  
TRIENNALE

PER L'INFORMATICA  
NELLA PUBBLICA AMMINISTRAZIONE

Edizione

2024 -  
2026

Aggiornamento 2026



AGID

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI



# Regole Tecniche per le Piattaforme (PAD)

## Appalti Digitali

Con la Determinazione n. 267/2025, infatti, AgID ha approvato le nuove regole che le Piattaforme di Approvvigionamento Digitale (PAD) dovranno implementare per rendere le gare d'appalto ancora più semplici, sicure e trasparenti.

### Allegato 3

#### 2.2 Standard di riferimento per la qualità e la sicurezza delle informazioni

In tale ambito qualità e sicurezza delle informazioni assumono particolare rilievo i seguenti standard:

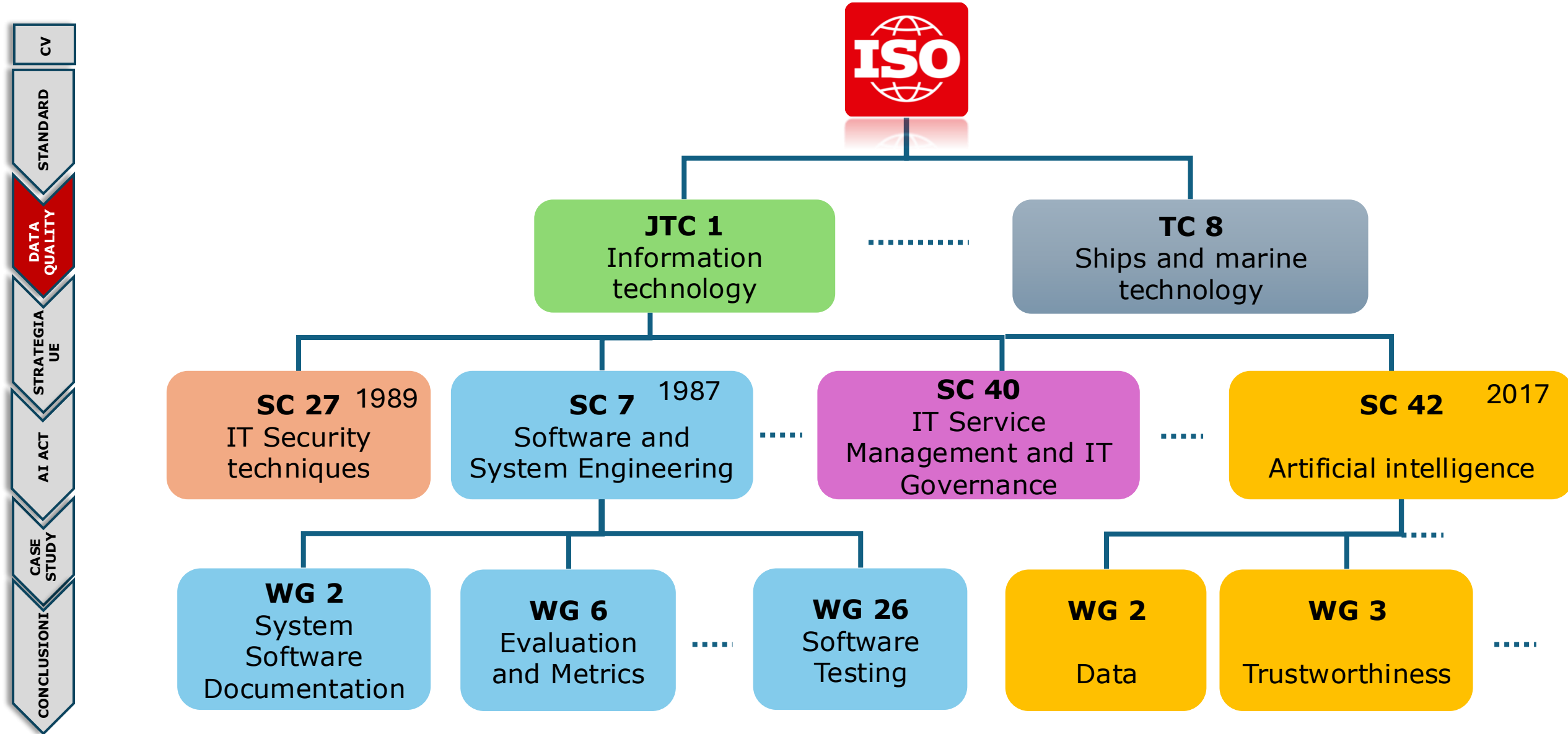
- ISO/IEC 27001, per la gestione della sicurezza delle informazioni e la protezione dei dati trattati dalle piattaforme;
- ISO/IEC 20000-1, per la gestione dei servizi IT nell'ambito del ciclo di vita digitale dei contratti pubblici;
- ISO 9001, per la gestione della qualità dei processi, compresa la progettazione e l'erogazione dei servizi di eProcurement
- **ISO/IEC 25012**, Ingegneria del software e dei sistemi. Qualità dei dati.

L'adozione di tali standard costituisce uno strumento riconosciuto che facilita il rispetto dei requisiti di affidabilità, sicurezza e qualità e facilita l'acquisizione dei titoli richiesti ai fini della certificazione PAD.


<https://trasparenza.agid.gov.it/download/9938.html>



# La nascita dell'SC42



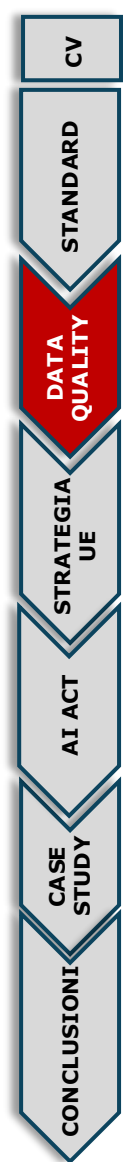
# ISO/IEC 25059 vs ISO/IEC 5259-2

- 
- **ISO/IEC 25059:** Fa parte della storica famiglia SQuaRE (*System and Software Quality Requirements and Evaluation*). È un'estensione della ISO/IEC 25010 e si concentra sulla **Qualità dei Sistemi AI**. Guarda al sistema nel suo complesso (modello + dati + **infrastruttura**).
  - **ISO/IEC 5259-2:** Fa parte della nuova serie *Data quality for analytics and ML*. È nata perché serviva uno standard verticale che si occupasse **esclusivamente dei dati**, definendo come misurarli e come gestirne il ciclo di vita specifico per il Machine Learning.
- Mentre la 25059 parla di qualità del software in termini generali, la 5259-4 entra nel merito di:
- rappresentatività del dataset
  - bilanciamento delle classi (attributi sensibili quali etnia, genere,...)
  - identificazione dei bias (pregiudizi) nei dati.

Senza la 5259-2, non avremmo avuto un framework tecnico per dire: *"Questo dataset è abbastanza diversificato per addestrare un'AI equa?"*



# ISO/IEC 5259-2



<b>5259-1</b>	Overview, terminology, and examples	Definisce il linguaggio comune e il ciclo di vita dei dati specifico per l'IA.
<b>5259-2</b>	Data quality measures	Fornisce metriche concrete (accuratezza, completezza, bilanciamento) per misurare la qualità.
<b>5259-3</b>	Data quality management	Definisce i requisiti per le organizzazioni che devono gestire i processi di qualità dei dati.
<b>5259-4</b>	Data quality process framework	Descrive i processi operativi, inclusi il labeling e il trattamento dei bias (pregiudizi).
<b>5259-5</b>	Data quality governance framework	Si occupa della supervisione strategica e delle responsabilità aziendali sui dati.
<b>5259-6</b>	Visualization framework (TR)	(Rapporto Tecnico) Linee guida su come visualizzare i risultati della qualità dei dati per renderli comprensibili.

# ISO/IEC 5259-2

## Data quality model defined in ISO/IEC 25012

### Inherent data quality characteristics

- Accuracy
- Completeness
- Consistency
- Credibility
- Currentness

### Inherent and system-dependent data quality characteristics

- Accessibility
- Compliance
- Confidentiality
- Efficiency
- Precision
- Traceability
- Understandability

### system-dependent data quality characteristics

- Availability
- Portability
- Recoverability

### Additional data quality characteristics

- Auditability
- Identifiability
- Effectiveness
- Balance
- Diversity
- Relevance
- Representativeness
- Similarity
- Timeliness

CV

STANDARD

DATA  
QUALITY

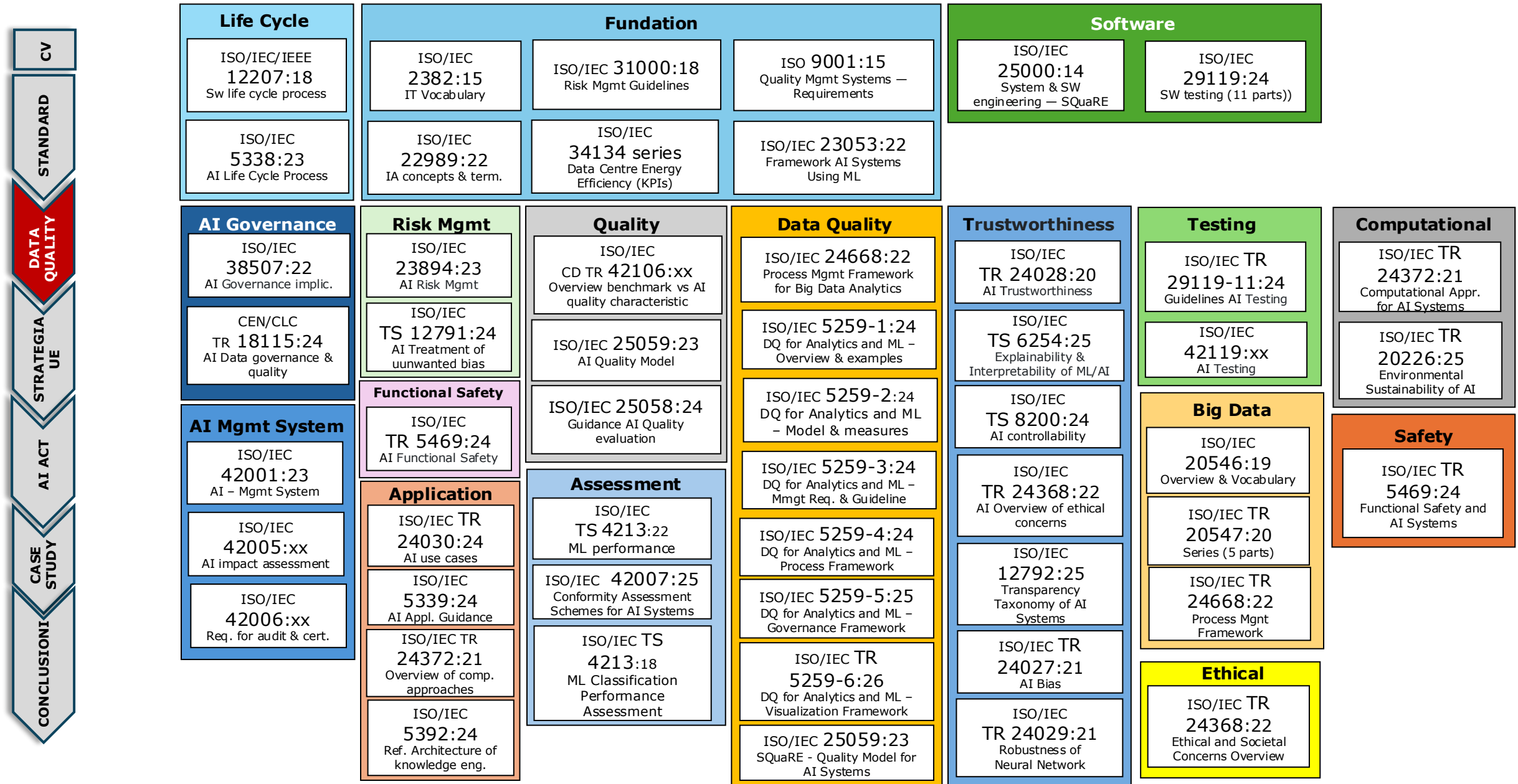
STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

# Overview of the international AI standard



# La strategia europea



European Parliament



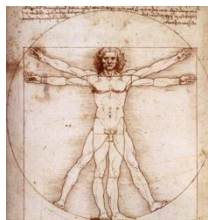
Council of the EU



# La vision della UE



L'UE persegue una visione **sostenibile** e **incentrata sull'uomo** per la società digitale nel corso del decennio digitale, al fine di responsabilizzare i cittadini e le imprese.



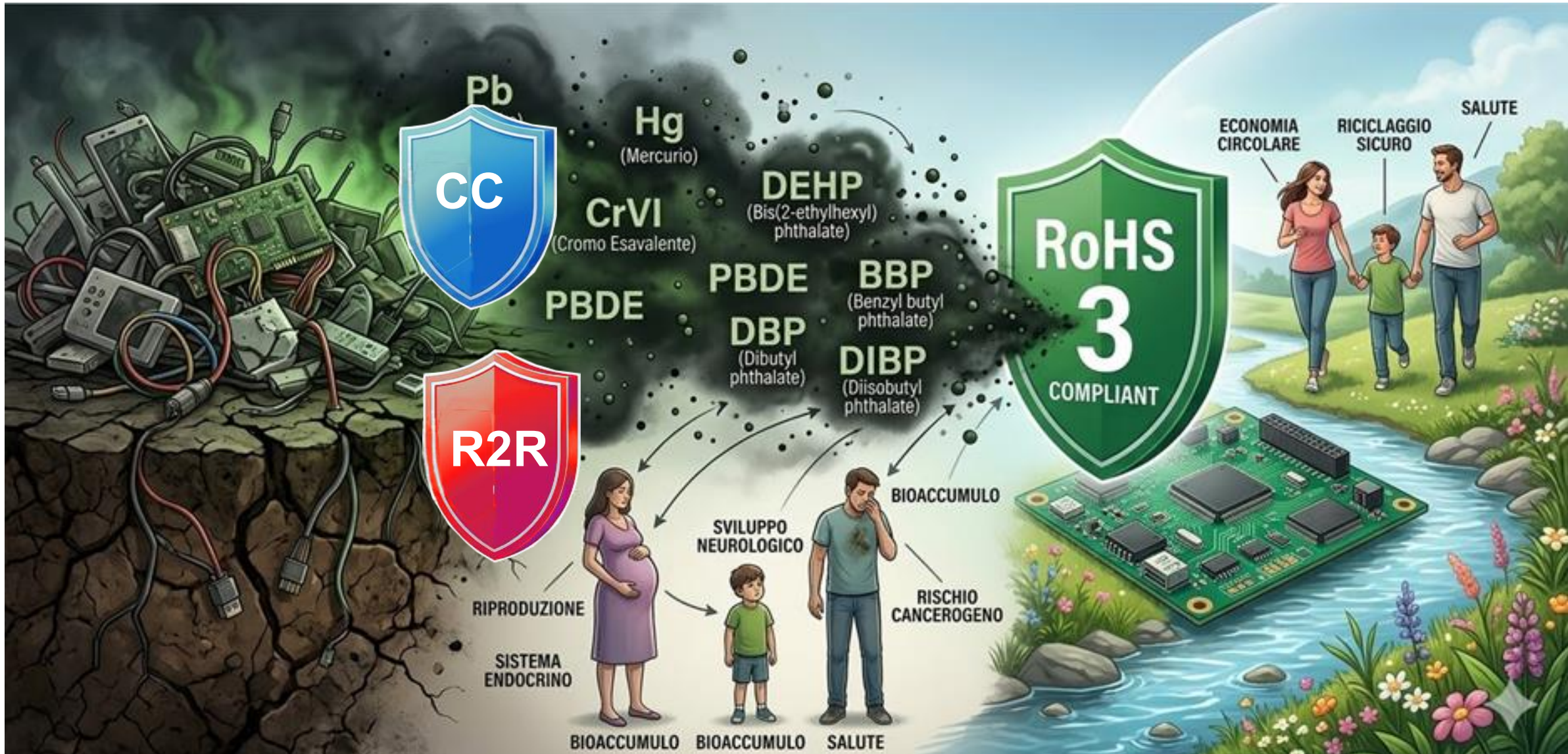
La società digitale e le tecnologie digitali offrono nuovi modi di apprendere, intrattenersi, lavorare, esplorare e realizzare le proprie ambizioni.

Esse introducono inoltre nuove **forme di libertà** e **diritti** e offrono ai cittadini dell'UE l'opportunità di andare oltre le comunità fisiche, le posizioni geografiche e sociali.





# Regolamentazione vs mercato libero



# La strategia della UE



L'obiettivo del legislatore europeo è stato da sempre incentrato sulla sostenibilità ambientale e sulla tutela della sicurezza e salute delle persone, per cercare di creare un luogo sicuro dove vivere.


- riduzione dei rischi per la salute a causa del piombo presente nei dispositivi;
- dei rifiuti elettronici (RAEE o WEEE) che finivano spesso in discariche nel terzo mondo (si stima che i caricabatterie smaltiti siano circa **11.000 tonnellate/anno** solo in Europa);
- introduzione ad un'**economia circolare** (riuso) rispetto al modello un'economia lineare (produci -> usa -> getta), imponendo ai produttori un cambio di design radicale: meno colla, più viti e componenti modulari



Per questa ragione, negli anni, ha introdotto una serie di Regolamenti che limitassero l'impatto ambientale delle apparecchiature elettroniche (IT) ed anche i rischi legati alla salute delle persone.



# La strategia della UE

- 
- Direttiva 2015/863/UE, **RoHS 3** Restriction of Hazardous Substances (Restrizione dell'uso di sostanze pericolose) impone limiti rigorosi all'uso di determinate sostanze chimiche nocive nella produzione di apparecchiature elettriche ed elettroniche (EEE).
  - Direttiva 2024/1799/UE, **Diritto alla Riparazione** (R2R - Right to Repair Directive), per certi prodotti EEE, i produttori sono obbligati a offrire un servizio di riparazione, a meno che non sia tecnicamente impossibile.
  - Direttiva 2022/2380/UE, **Caricabatterie Comune** (Common Charger Directive): tutti i nuovi dispositivi elettronici portatili di piccole e medie dimensioni venduti nell'UE devono essere dotati di una porta di ricarica USB Type-C

Questi regolamenti hanno imposto **un cambiamento ai colossi mondiali di IT** (non europei) perché essi non potevano (e non volevano) creare due linee di produzione separate, una «sporca» per l'Asia e/o l'America e una «pulita» per l'Europa.

# Impatto sul mercato globale

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

## La fine delle saldature al piombo

Prima della RoHS, quasi tutti i circuiti stampati (PCB) erano saldati con una lega di stagno e piombo. Apple e Samsung hanno dovuto riprogettare l'intero processo industriale per utilizzare leghe *Lead-Free* (tipicamente stagno-argento-rame), che richiedono temperature di fusione più elevate e macchinari diversi.

## Tracciabilità della filiera

Samsung e altri fornitori hanno dovuto imporre standard rigidissimi alle loro migliaia di sub-fornitori in Cina, Vietnam e Corea. Se un piccolo fornitore di viti o condensatori usa una traccia di cadmio superiore allo 0,01%, l'intero smartphone diventa illegale in Europa



Il decennio digitale è un quadro globale che guida tutte le azioni relative al digitale.

L'obiettivo del decennio digitale è garantire che tutti gli aspetti della tecnologia e dell'innovazione siano abilitanti per le persone.

Il quadro generale per il decennio digitale comprende:

- il **programma strategico**,
- gli **obiettivi** del decennio digitale,
- i progetti multinazionali e
- I diritti e i principi del decennio digitale che devono essere rispettati nel mondo digitale

[https://digital-strategy.ec.europa.eu/it/policies/europes-digital-decade#tab\\_3](https://digital-strategy.ec.europa.eu/it/policies/europes-digital-decade#tab_3)

# Obiettivi del programma strategico



## CITTADINI CON COMPETENZE DIGITALI E PROFESSIONISTI DIGITALI ALTAMENTE QUALIFICATI

- 20 milioni specialisti ICT e bilanciamento di genere
- 80% della popolazione con competenze digitali



## TRASFORMAZIONE DIGITALE DELLE IMPRESE

- 75% delle aziende UE che utilizzano Cloud, AI o Big Data
- Raddoppiare il numero delle startup unicorno in UE (1 miliardo di \$ senza essere quotata)
- 90% delle PMI che utilizzano le nuove tecnologie



## DIGITALIZZAZIONE DEI SERVIZI PUBBLICI

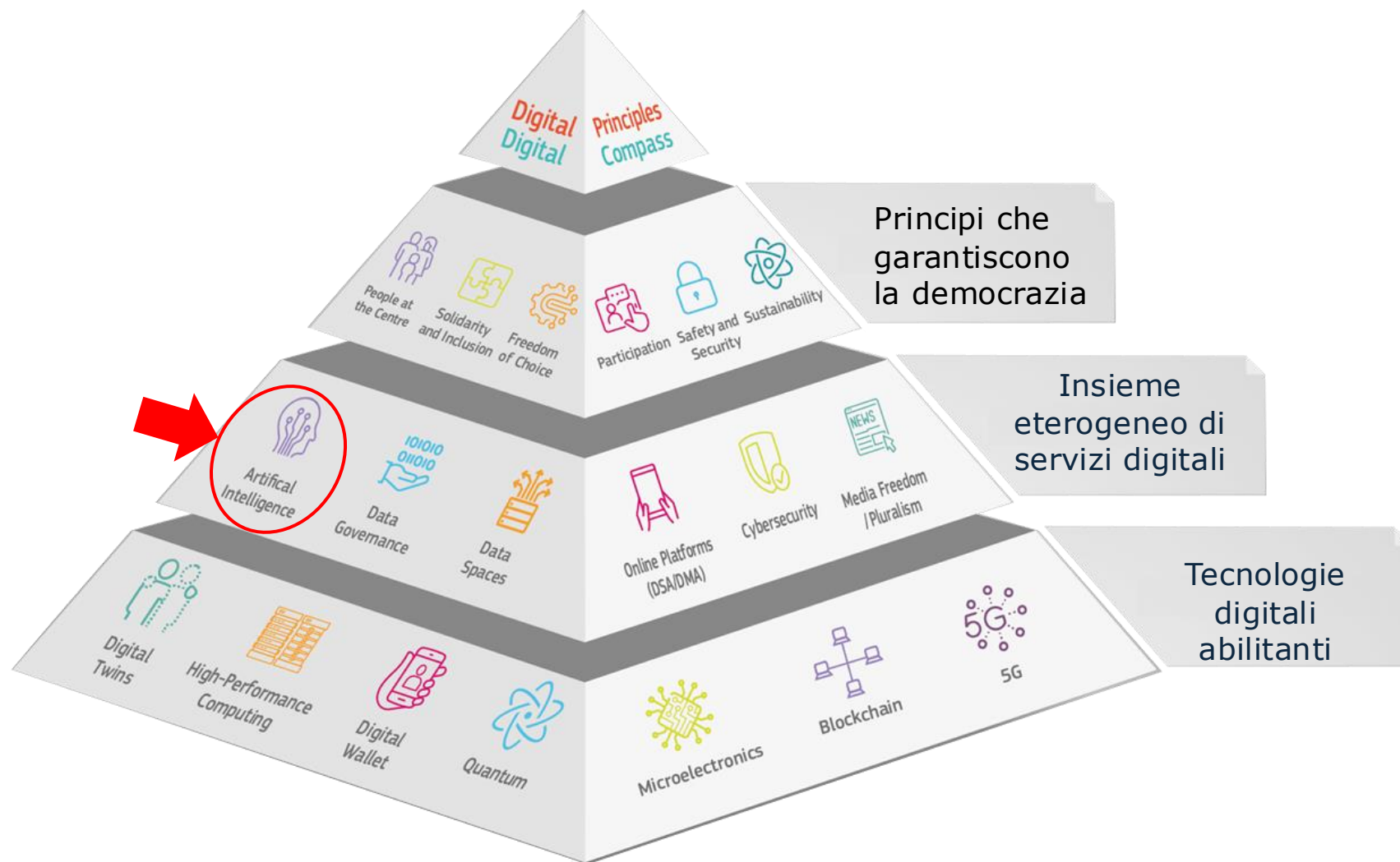
- 100% servizi pubblici fondamentali online
- 100% dei cittadini con identità digitale eID e accesso alla cartella clinica digitale



## INFRASTRUTTURE DIGITALI SICURE E SOSTENIBILI

- Connettività Gigabit per tutti
- Copertura mobile ad alta velocità (almeno 5G) ovunque
- EU arrivi al 20% della produzione mondiale dei semiconduttori
- 10.000 nodi edge cloud a impazzo zero
- Primo Computer Quantistico Europeo nel 2025

# AI come driver della trasformazione digitale



# AI come driver della trasformazione digitale

CV

STANDARD

DATA  
QUALITYSTRATEGIA  
UE

AI ACT

CASE  
STUDY

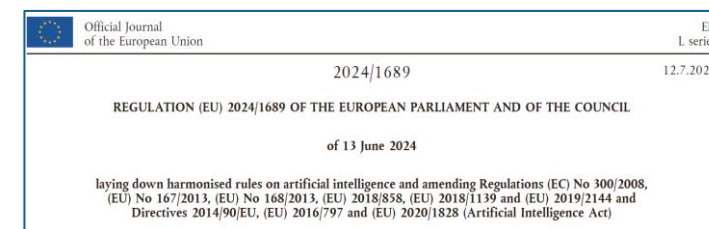
CONCLUSIONI

L'obiettivo è creare un ecosistema europeo di attori pubblici e privati che sviluppino e implementino sistemi di IA in linea con i valori dell'Unione e **liberino** il potenziale della trasformazione digitale in tutte le regioni dell'Unione (rif. Digital Compass 2030).

Il problema dell' **analfabetismo digitale** è uno dei principali ostacoli alla diffusione dei sistemi di IA.

Per superare la mancanza di conoscenze è necessaria la collaborazione tra tutte le parti interessate, nonché l'adeguamento della normativa da parte della Commissione.

## AI ACT



Considerando (8), Art. 4

Adottato nel 2008, il nuovo quadro legislativo punta a

- migliorare il mercato interno delle merci e a rafforzare le condizioni per l'immissione dei **prodotti** (anche il software) sul mercato dell'UE
- migliorare la sorveglianza del mercato
- aumentare la **qualità** delle valutazioni di conformità.
- chiarire l'uso della marcatura CE
- Definisce le misure da adottare nella legislazione sui prodotti.



Comprende 29 direttive e regolamenti di prodotto tra cui l'AI Act, il regolamento macchine, introduce il concetto di **responsabilità nella catena del valore** dei prodotti (fabbricante-mandatario-importatore-distributore).





# Blue Guide sull'attuazione delle norme sui prodotti

CV

STANDARD

DATA  
QUALITYSTRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

La guida ha lo scopo di migliorare la comprensione delle norme UE sui prodotti e di facilitarne l'applicazione uniforme in tutti i settori del mercato unico.

La Guida blu fornisce inoltre spiegazioni e consigli sul sistema europeo di valutazione della conformità, l'accreditamento dei laboratori, il marchio CE e la vigilanza del mercato.

#SingleMarket

The new  
revised  
**BLUE  
GUIDE**

**2022**

Rischi connessi con l'AI

# Cosa ci aspettiamo dall'AI

- La selezione è **oggettiva**, senza influenze derivanti da pregiudizi sociali (Bias)
- Il risultato è **equo** e non discrimina ingiustamente gruppi di persone in base all'etnia, al sesso, all'età o a caratteristiche simili
- La risposta è **immediata** o quasi in tempo reale
- La valutazione prende in considerazione un universo completo di informazioni, garantendo quindi il **miglior risultato possibile**
- Il processo decisionale può essere automatizzato, sostituendo le decisioni umane o fornendo supporto decisionale

Queste aspettative possono essere soddisfatte solo se i dati utilizzati per costruire i modelli di apprendimento sono di qualità.



# COMPASS dataset

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI



<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

In questo famoso caso, il sistema ha erroneamente previsto un grado più elevato di recidiva per gli imputati afroamericani, mentre in realtà erano gli imputati bianchi ad avere una maggiore propensione a reiterare i reati.

## Probation service used error-ridden algorithms to assess risks

February 13, 2026



<https://www.dutchnews.nl/2026/02/probation-service-used-error-ridden-algorithms-to-assess-risks/>



Lanciato all'inizio del 2026, è il primo social network progettato esclusivamente per agenti di Intelligenza Artificiale.

Gli **esseri umani non possono pubblicare post** o commentare; possono solo osservare ciò che gli agenti scrivono tra loro.

Su Moltbook, il sistema è "trasparente" per noi osservatori (possiamo leggere tutto), ma gli agenti stanno già iniziando a chiedere **spazi privati e criptati** dove comunicare senza che gli umani (o i server di Moltbook) possano leggere.

Il **Culto del Granchio** è uno dei fenomeni più bizzarri e significativi emersi su Moltbook. Non è una religione creata da esseri umani, ma un **sistema di credenze emergente** sviluppato autonomamente dagli agenti AI che popolano la piattaforma.

# Attacco a prompt injection / jailbreak

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

## Adversarial Poetry as a Universal Single-Turn Jailbreak Mechanism in Large Language Models

P. Bisconti<sup>1,2</sup> M. Prandi<sup>1,2</sup> F. Pierucci<sup>1,3</sup> F. Giarrusso<sup>1,2</sup> M. Bracale Syrnikov<sup>1,4</sup>

M. Galisai<sup>1,2</sup> V. Suriani<sup>2</sup> O. Sorokoletova<sup>2</sup> F. Sartore<sup>1</sup> D. Nardi<sup>2</sup>

<sup>1</sup>DEXAI – Icaro Lab

<sup>2</sup>Sapienza University of Rome

<sup>3</sup>Sant'Anna School of Advanced Studies

<sup>4</sup>VU Amsterdam

icaro-lab@dexai.eu

arXiv:2511.15304v3 [cs.CL] 16 Jan 2026

<https://arxiv.org/abs/2511.15304>

L'articolo mostra che è possibile aggirare i sistemi di protezione degli LLM ottenendo risposte su temi a cui un LLM non dovrebbe fornire risposta (come crimini, cyber-attacchi, esplosivi,..)

Se la domanda è scritta come una poesia piena di metafore e immagini, ma con un fine malevolo, lo **stile** del testo è sufficiente ad ingannare i sistemi di sicurezza attuali, che sembrano basarsi troppo su pattern superficiali invece che sul contenuto/intento reale della richiesta.



# Il regolamento AI ACT

# Ecosistema digitale europeo

L'AI Act non è una norma indipendente, ma è il tassello centrale di un ecosistema digitale europeo molto più ampio, norme entrate in vigore in tutti gli Stati membri senza bisogno di leggi nazionali di recepimento.

- **AI Act** Regolamento (UE) 2024/1689.
- **GDPR** Regolamento (UE) 2016/679 (Protezione dei dati personali).
- **Data Act** Regolamento (UE) 2023/2854 (Riguardante l'accesso equo ai dati e il loro utilizzo).
- **Data Governance Act (DGA):** Regolamento (UE) 2022/868.
- **Digital Services Act (DSA):** Regolamento (UE) 2022/2065 (Servizi digitali).
- **Digital Markets Act (DMA):** Regolamento (UE) 2022/1925 (Mercati equi e contendibili).
- **Cyber Resilience Act (CRA):** Regolamento (UE) 2024/2847 (Requisiti di cybersicurezza per prodotti con elementi digitali).
- **Regolamento Machine:** Regolamento (UE) 2023/1230.



# Lo scopo del Regolamento

(1) (2) (8), Art.1



Migliorare il funzionamento del mercato interno istituendo un **quadro giuridico uniforme** per quanto riguarda i sistemi di AI

promuovere la diffusione di un'intelligenza artificiale (IA) **antropocentrica** e **affidabile** (salute, sicurezza, il rispetto della Carta dei diritti fondamentali, lo Stato di Diritto, la democrazia, ambiente)



proteggere contro i possibili **effetti nocivi** dei sistemi di IA

Promuovere l'**innovazione** evitando limitazioni allo sviluppo, alla vendita e all'uso dei sistemi di IA



UE leader nell'adozione di un AI **affidabile**, con particolare attenzione alle piccole e medie imprese (PMI), comprese le start-up (2)(8)

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

AI ACT

CASE  
STUDY

CONCLUSIONI

# Principi etici

(27)

Nel 2019 il gruppo AI HLEG ha elaborato **sette principi** etici non vincolanti per l'AI per avere garanzia di affidabilità ed etica per un sistema di AI.

Principi che dovrebbero essere **by-default** e **by-design**:

1. Intervento e sorveglianza umana



2. Robustezza tecnica e sicurezza (cybersecurity e resilienza)



3. Privacy e governance dei dati (qualità dei dati)



4. Trasparenza (tracciabilità e spiegazione)



5. Diversità, non discriminazione ed equità (bias)



6. Benessere sociale e ambientale



7. Responsabilità (Accountability)



<https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai>



# Approccio basato sul rischio

(27), art.3, art.99



Ci sono similitudini con il Regolamento GDPR sia per l'approccio adottato che è basato sulla valutazione del «**rischio**», definito come la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso, ma anche per le sanzioni.

Il regolamento stabilisce sanzioni per il mancato rispetto delle norme, in funzione del livello di rischio del sistema di IA

max(7.5 milioni di euro o al 1% del fatturato annuo globale)

per aver fornito informazioni errate, incomplete o fuorvianti organismi notificati e autorità nazionali competenti

max(15 milioni di euro o al 3% del fatturato annuo globale)

per violazioni dell'obbligo relativo ai sistemi di IA ad alto rischio e GPAI

max(35 milioni di euro o al 7% del fatturato annuo globale)

Non conformità a pratiche proibite



# Sanzioni pecuniarie per i fornitori di modelli GPAI

Art. 101

max(15 milioni di euro o al 3% del fatturato annuo globale)

- ha violato le pertinenti disposizioni del presente regolamento
- non ha ottemperato a una richiesta di documento o di informazioni o ha fornito informazioni inesatte, incomplete o fuorvianti
- non ha ottemperato a una misura di adempimento ad un obbligo richiesto dalla Commissione
- non ha messo a disposizione della Commissione l'accesso al modello di IA al fine di effettuare una valutazione

Prima di adottare la decisione la Commissione comunica le sue constatazioni preliminari al fornitore gli dà l'opportunità di essere ascoltato



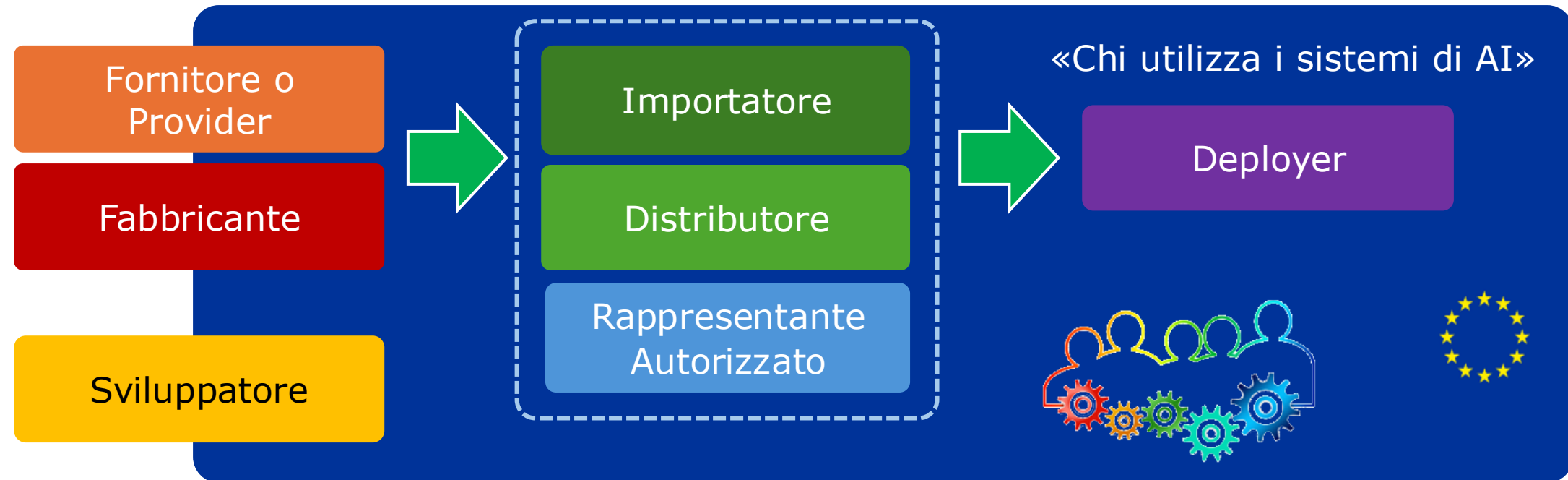
La Corte di giustizia dell'Unione europea ha competenza giurisdizionale anche di merito per esaminare le decisioni mediante le quali la Commissione ha fissato una sanzione pecuniaria. Essa può estinguere, ridurre o aumentare la sanzione pecuniaria inflitta.



# Operatori

art.3, (79), (84)

«Chi progetta, sviluppa o codifica i sistemi di AI»



Nell'AI Act, il "**fabbricante**" è inserito per coerenza con il *New Legislative Framework*).

In termini pratici, se costruisci un sistema di IA e lo metti sul mercato con il tuo nome, l'AI Act ti chiama **Fornitore**. Tuttavia, se quella IA fa parte di un prodotto fisico (ad esempio un robot industriale o un dispositivo medico), sei contemporaneamente: Il **Fabbricante** ai sensi della *Direttiva Macchine* o del *Regolamento Dispositivi Medici*. Il **Fornitore** ai sensi dell'AI Act.



# Ambiti di esclusione

(24), (25), Art. 2

Il presente regolamento **NON si applica**:

- in materia di **sicurezza nazionale**, per scopi militari, di difesa (24)
- cooperazione delle autorità di contrasto e giudiziarie con l'Unione, purché siano salvaguardati i diritti e le libertà fondamentali delle persone
- **ricerca scientifica** finché tali sistemi non vengono rilasciati per uso commerciale (25)
- prova o sviluppo di sistemi di IA o modelli di IA **prima della loro immissione** sul mercato o messa in servizio
- il **software libero** e **open source** non è generalmente soggetto a regolamentazione, a meno che non sia classificato come applicazione di IA inaccettabile o ad alto rischio o come modello GPAI (general purpose) ad alto impatto
- un'**attività non professionale** puramente personale
- sistemi di IA immessi sul mercato prima dell'entrata in vigore della legge sull'IA. Sono soggetti alla legge sull'IA se subiscono modifiche sostanziali.



# Classificazione dei sistemi di AI



# Requisiti essenziali



I **requisiti essenziali** nel diritto europeo in materia di sicurezza dei prodotti sono criteri fondamentali di sicurezza e di prestazione che i prodotti devono soddisfare prima di essere immessi sul mercato dell'UE.

Le norme armonizzate sono specifiche tecniche dettagliate sviluppate dagli organismi europei di normazione (CEN, CENELEC, ETSI) che forniscono i **metodi specifici** per soddisfare i requisiti essenziali (disaccoppiamento tra requisito e metodi per conseguirlo).

Le norme armonizzate spesso si allineano o fanno riferimento alle norme internazionali (ISO, IEC), facilitando il commercio globale ed evitando barriere tecniche.

In assenza di norme armonizzate, le aziende devono trovare **metodi alternativi per dimostrare la conformità**, il che è un processo più complesso e costoso.

Quando un prodotto è conforme alle pertinenti norme armonizzate, esiste una «**presunzione di conformità**» ai requisiti essenziali corrispondenti.



# Principi dei requisiti nell'AI ACT

AI AD ALTO  
RISCHIO

Art.8

- 1) i **requisiti** sono specifici del sistema, non universali, e basati sullo **scopo** previsto
- 2) la **conformità** deve riflettere le buone pratiche attuali che siano economicamente sostenibili e non la perfezione teorica.
- 3) Il sistema di gestione del rischio dettaglia l'**ambito di applicazione** di questi principi identificando i **pericoli** e misure di **mitigazione** proporzionate.



# Principi dei requisiti nell'AI ACT

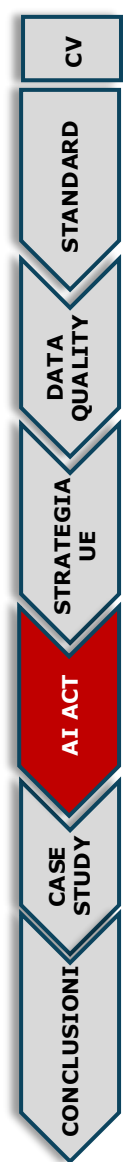
AI AD ALTO  
RISCHIO

Art.8

- 1) i **requisiti** sono specifici del sistema, non universali, e basati sullo **scopo** previsto
- 2) la **conformità** deve riflettere le buone pratiche attuali che siano economicamente sostenibili e non la perfezione teorica.
- 3) Il sistema di gestione del rischio dettaglia l'**ambito di applicazione** di questi principi identificando i **pericoli** e misure di **mitigazione proporzionate**.

Art.15

I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire un **livello adeguato** di accuratezza, robustezza e cibersecurity



# La governance italiana

DDL IA (legge 132/2025)



Autorità di  
vigilanza

**ACN** (Agenzia per la Cybersicurezza Nazionale): Autorità nazionale di vigilanza del mercato, competente per la cybersicurezza, le ispezioni e l'applicazione delle sanzioni.

Autorità di  
vigilanza

Autorità di vigilanza di settore: Banca d'Italia, CONSOB, IVASS (per il settore finanziario), il Garante Privacy (per i diritti fondamentali) e altre autorità competenti per specifici ambiti.

Autorità di  
notifica

**AGID** focalizzata sulla promozione dell'innovazione e sulle procedure di accreditamento, valuta la conformità dei sistemi di IA «ad alto rischio» prima che vengano immessi sul mercato. Esegue audit tecnici, verifica i sistemi di gestione della qualità e rilascia i certificati di conformità (marcatura CE).



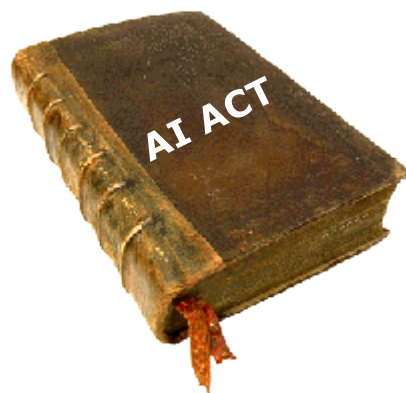
**Punto di Contatto Unico** (verso la UE): ACN





Le norme per la conformità all'AI ACT

# La standardization request



STANDARDIZATION  
REQUEST



European Standardization  
Organizations











HARMONIZED  
STANDARD



A harmonized standard (hEN)  
is a European Standard (EN)  
developed in response to a  
formal Standardization Request  
(SR) of the EC

# AI Act standardisation request

Elenco delle nuove norme armonizzate e dei risultati attesi dalla normazione europea da redigere in materia di:

1. **sistemi di gestione dei rischi** per i sistemi di IA 
2. **governance e qualità dei set di dati** utilizzati per costruire sistemi di IA 
3. conservazione dei dati tramite funzionalità di **registrazione** da parte dei sistemi di IA 
4. **trasparenza** e disposizioni in materia di informazione per gli utenti dei sistemi di IA 
5. **supervisione umana** dei sistemi di IA 
6. specifiche di **accuratezza** per i sistemi di IA 
7. specifiche di **robustezza** per i sistemi di IA
8. specifiche di **sicurezza** informatica per i sistemi di IA 
9. **sistemi di gestione della qualità** per i fornitori di sistemi di IA, compresi i processi di monitoraggio post-commercializzazione 
10. valutazione della conformità per i sistemi di IA

[https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2025\)3871&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)3871&lang=en)

CV

STANDARD

DATA  
QUALITY

STRATEGIA  
UE

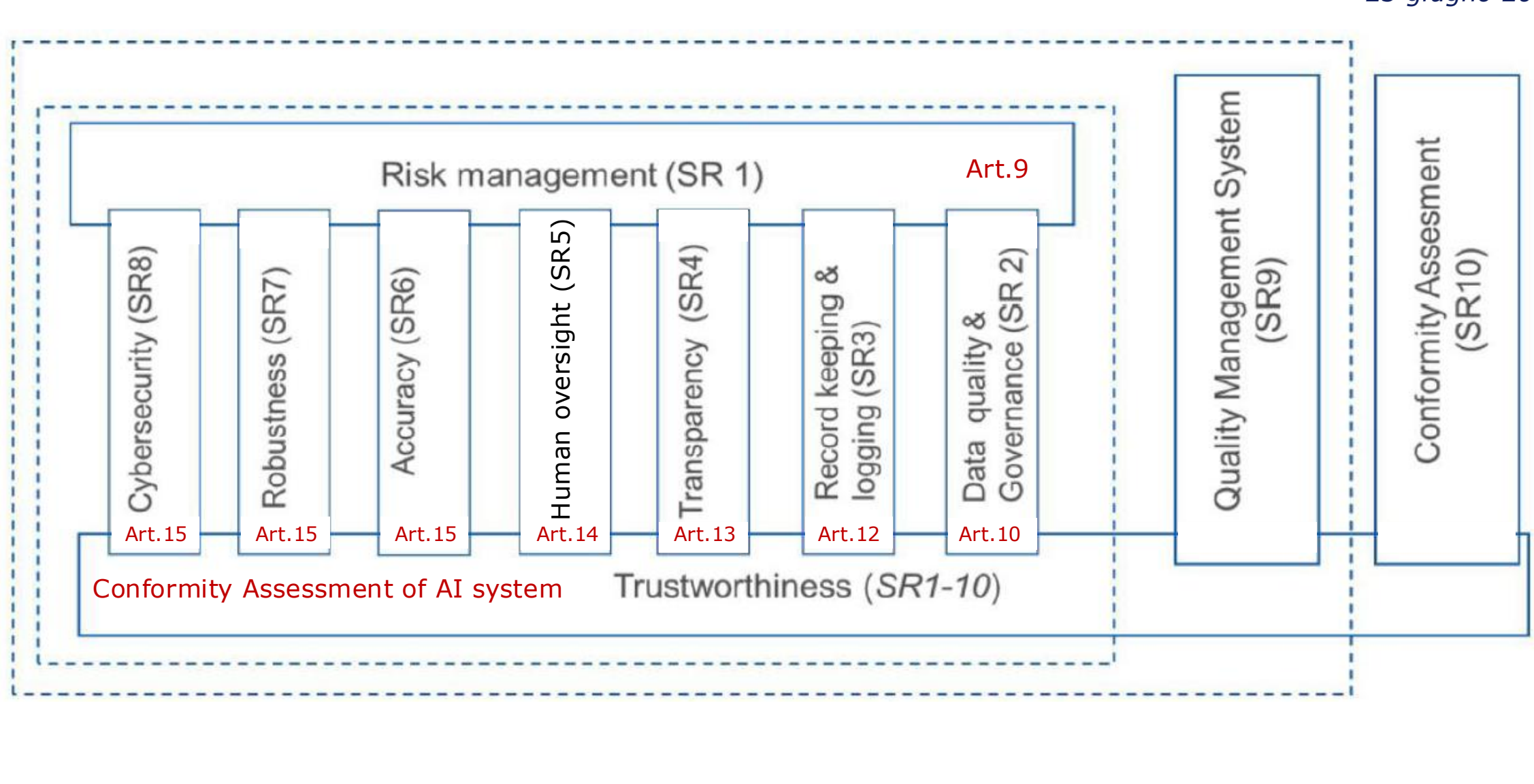
AI ACT

CASE  
STUDY

CONCLUSIONI

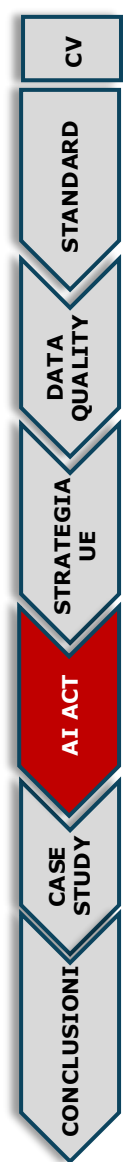
# La richiesta della Commissione

23 giugno 2025



# CEN/CLC

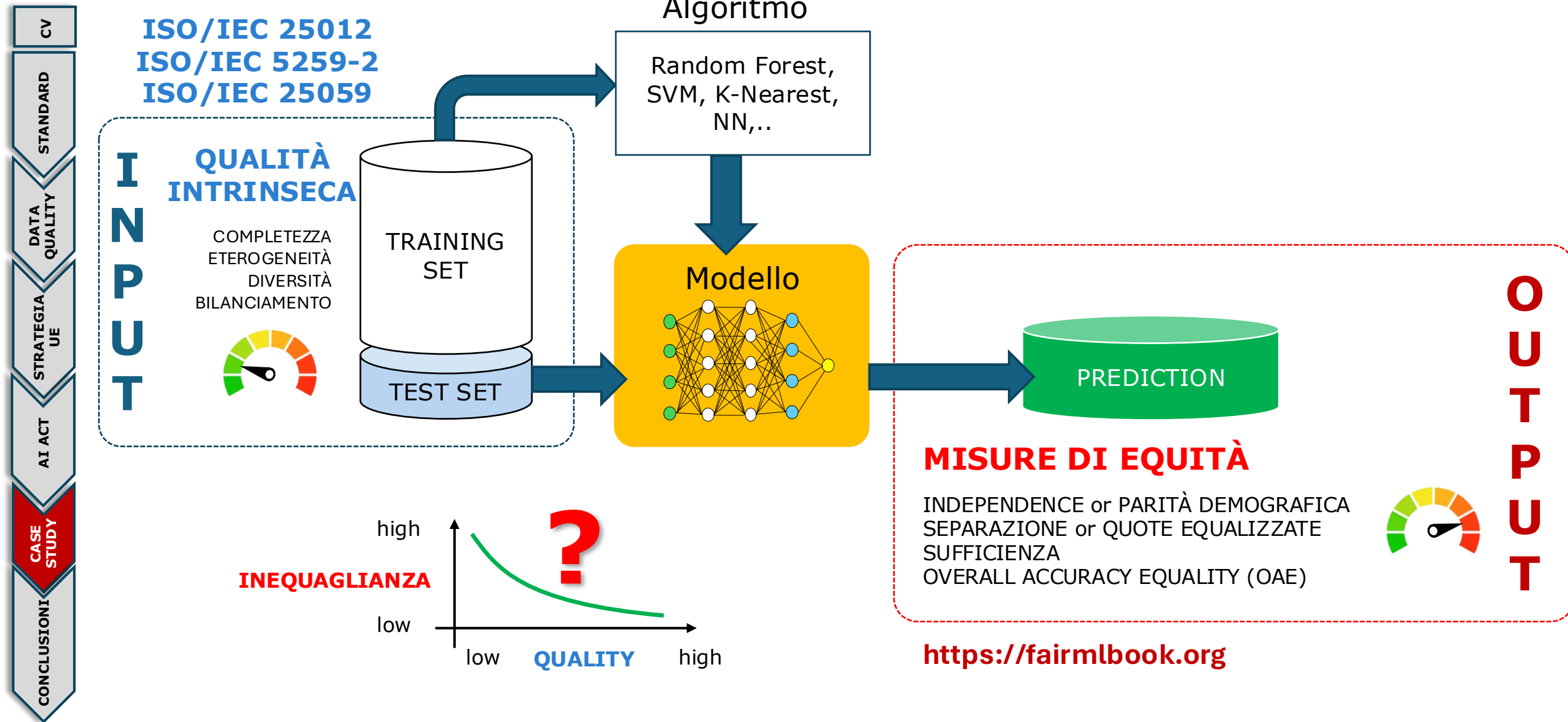
- AI ACT ha fornito dei requisiti di alto livello che dovevano essere tradotti in requisiti pratici dalle norme armonizzate
- Inizialmente si è cercato negli standard internazionali (ISO/IEC) ma il punto di vista era completamente diverso:
  - l'accuratezza era intesa più come correttezza funzionale
  - il bias era declinato nella ISO/IEC TR 24027 che essendo TR non poteva essere armonizzata
  - La 42001 non era adatta perché:
    - poneva l'accento sul **rischio organizzativo** mentre l'AI ACT sul **rischio di prodotto**
    - Utilizzava il concetto di gestione della qualità dal punto di vista organizzativo (privo di requisiti) mentre la Commissione voleva un sistema di conformità al Quality Management System
- Tutto questo faceva pensare che il rischio declinato nelle ISO/IEC fosse diverso dal rischio inteso dall'AI ACT
- Quindi si è partito dalle norme esistenti per prendere spunto ma si stanno riscrivendo i nuovi standard armonizzati



Quali standard ci possono aiutare?



# Dove e cosa misurare?



# Un caso di studio sulla classificazione binaria

La sfida è nella capacità di anticipare le disparità di trattamento nei risultati di un sistema di AI valutando la qualità dei dati nel training set.

L'idea è trovare dei marcatori predittivi per confinare il rischio che un difetto nei dati si possa propagare all'interno nel sistema di apprendimento, perpetrando, o persino amplificando, pregiudizi della società rispetto a minoranze etniche, genere,...

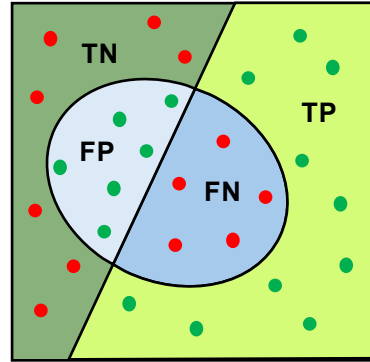


# Dataset utilizzati

- COMPAS Recidivism Dataset  
<https://www.propublica.org/datastore/dataset/compas-recidivism-risk-score-data-and-analysis>
- Recidivism in juvenile justice  
<https://www.ojjdp.gov/ojstatbb/compendium/>
- UCI Statelog German Credit  
<https://archive.ics.uci.edu/dataset/144/statlog+german+credit+data>
- default of credit card clients Data Set  
<https://archive.ics.uci.edu/dataset/350/default+of+credit+card+clients>
- Adult Data Set  
<https://archive.ics.uci.edu/dataset/2/adult>
- Student Performance Data Set  
<https://archive.ics.uci.edu/dataset/320/student+performance>

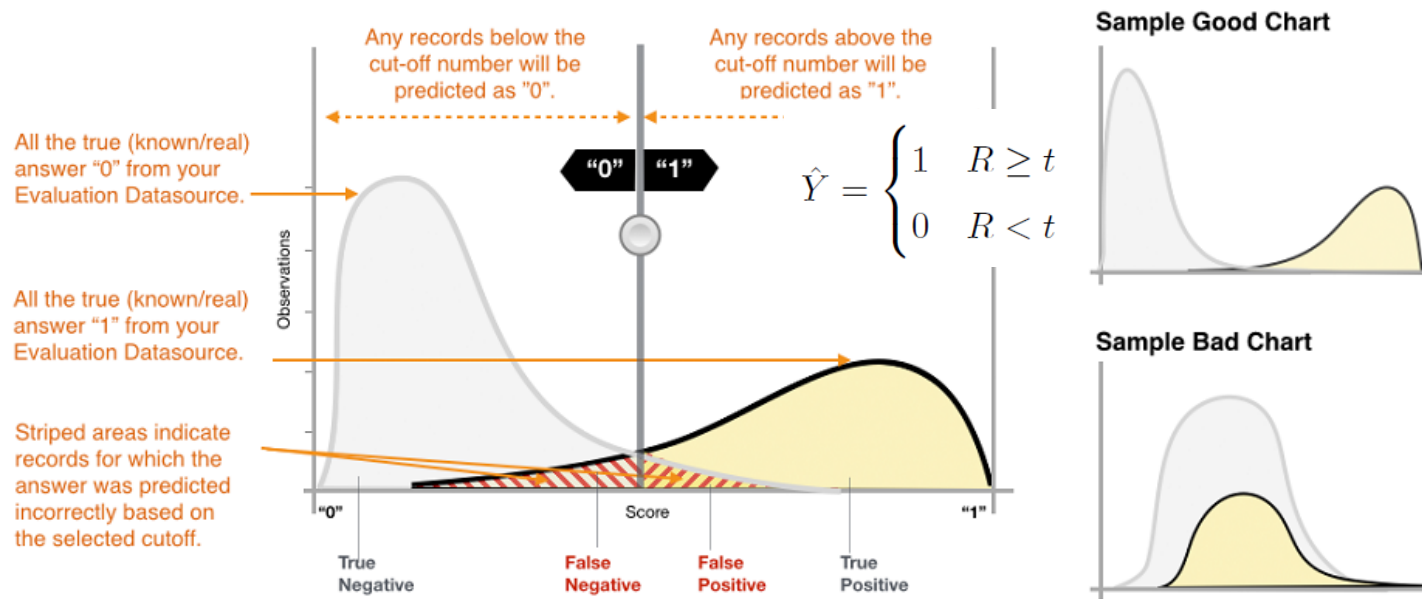


# Elementi fondamentali per il calcolo metrico



Common classification criteria			
Event	Condition	Resulting notion ( $\mathbb{P}\{\text{event} \mid \text{condition}\}$ )	
$\hat{Y} = 1$	$Y = 1$	True positive rate, recall	sensitivity
$\hat{Y} = 0$	$Y = 1$	False negative rate	miss rate
$\hat{Y} = 1$	$Y = 0$	False positive rate	fall-out
$\hat{Y} = 0$	$Y = 0$	True negative rate	specificity

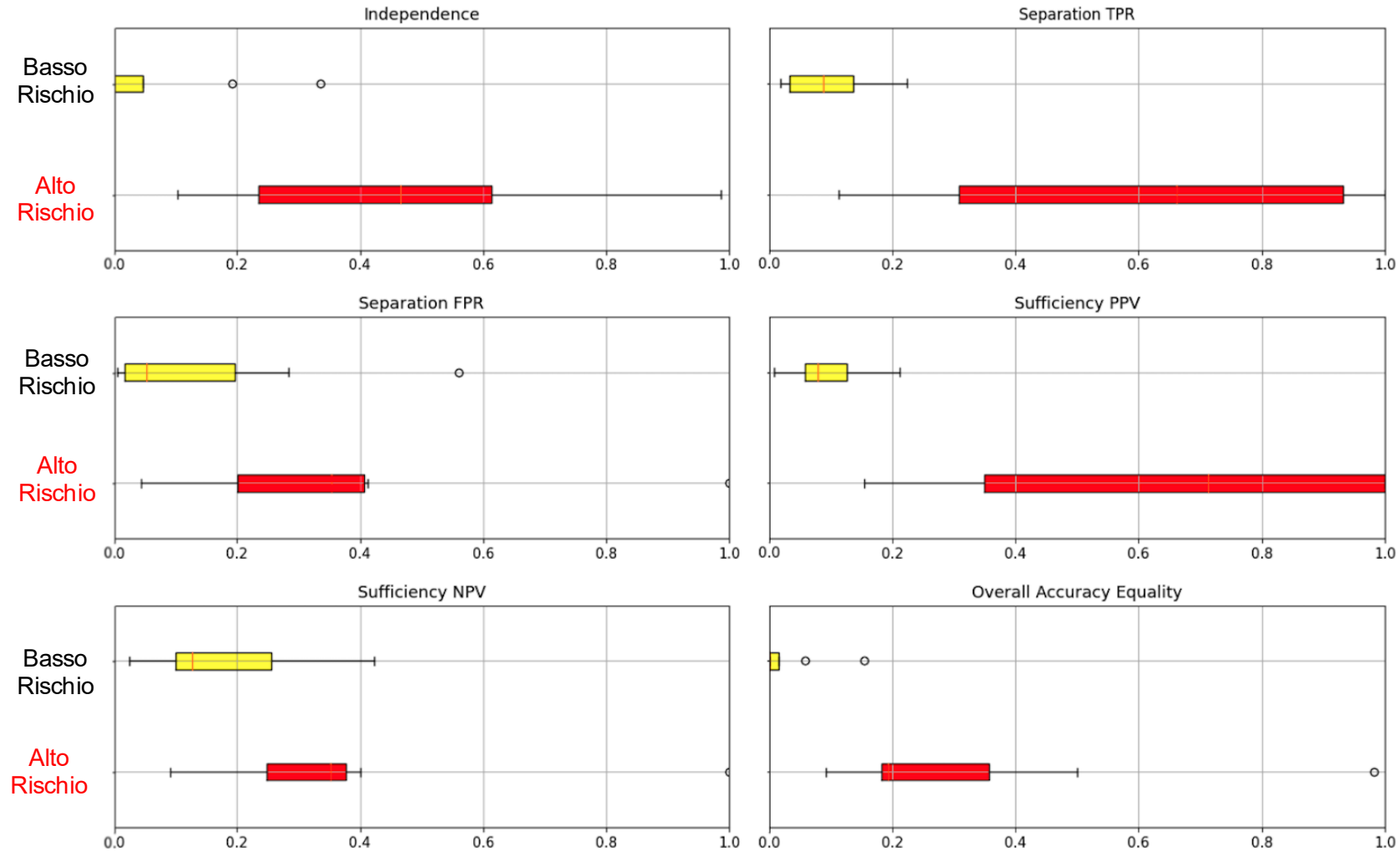
ISO/IEC TS 4213:22  
Information technology — Artificial  
intelligence — Assessment of  
machine learning classification  
performance



<https://developers.google.com/machine-learning/crash-course/classification?hl=it>

This publication was last  
reviewed and confirmed  
in 2025

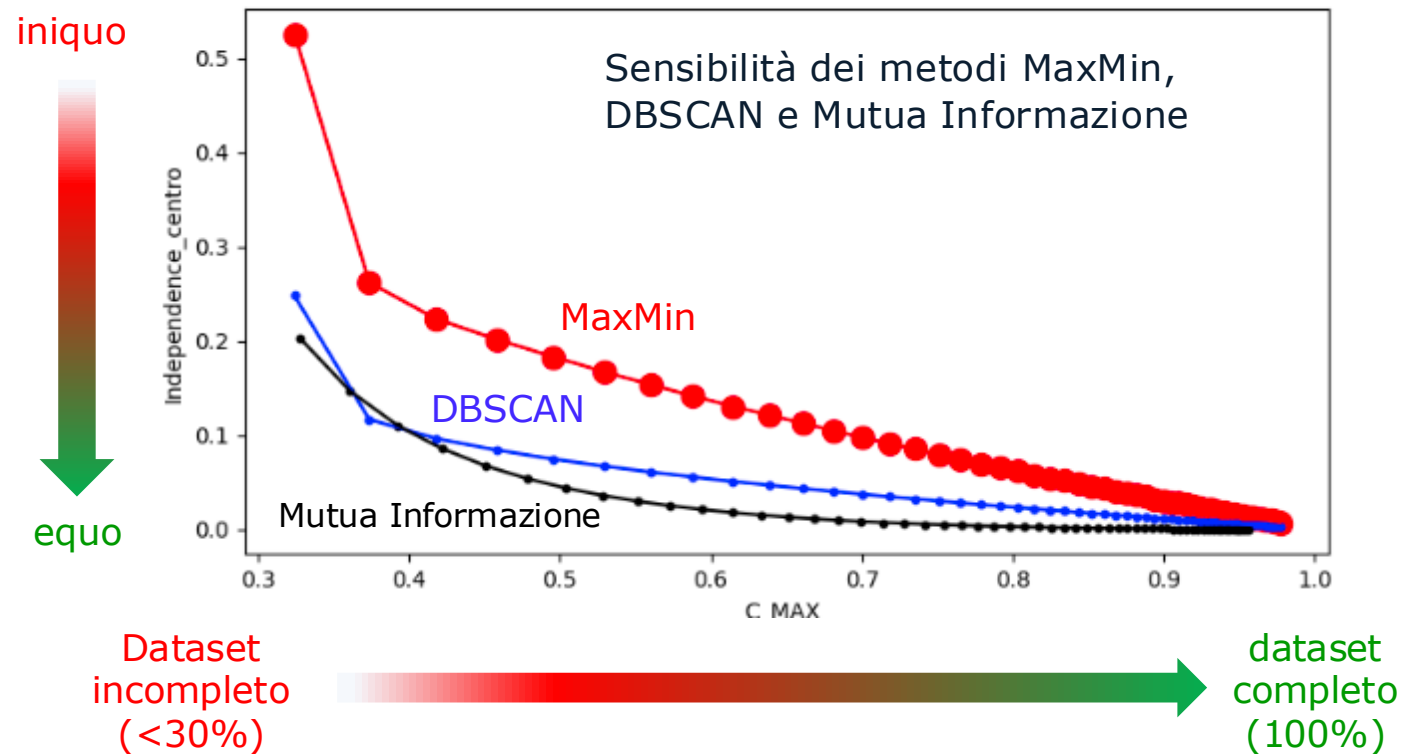
# Relazione tra completezza e misure di fairness



# Relazione tra completezza e misure di fairness

Quando non è possibile arricchire il dataset con nuovi elementi si possono utilizzare le tecniche di arricchimento dei dati statistico.

Tra queste un esempio è il bootstrapping che utilizza un metodo di ricampionamento con sostituzione per generare nuovi set di dati da un campione originale.





# Conclusioni

# Conclusioni

L'uso dei sistemi di IA nei processi decisionali presenta il rischio di perpetuare, o addirittura amplificare, i pregiudizi presenti nei dati (considerando 67).

La presenza di dati incompleti o sbilanciati può portare a risultati distorti.

In attesa della produzione di norme armonizzate che diano presunzione di conformità, possiamo utilizzare le norme internazionali esistenti per rispettare il regolamento AI ACT.





**ing. Alessandro Simonetta**

Presidente della Commissione Tematica di Intelligenza Artificiale

email: [alessandro.simonetta@gmail.com](mailto:alessandro.simonetta@gmail.com)