UNIVERSITÀ DEGLI STUDI FIRENZE

Responsabilità giuridiche, GDPR e IA

Protezione dei dati, accountability, responsabilità del Comune nell'uso di sistemi digitali e algoritmi

Massa, 11/04/2026

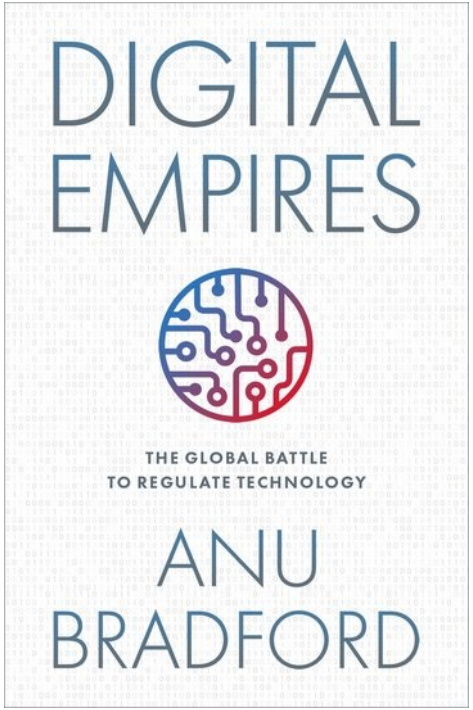
Matteo Giannelli

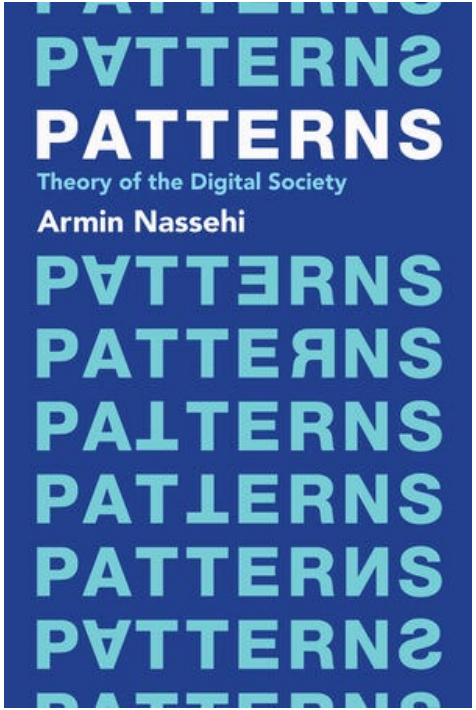
Università degli Studi di Firenze, Centro CybeRights

Il contesto geopolitico

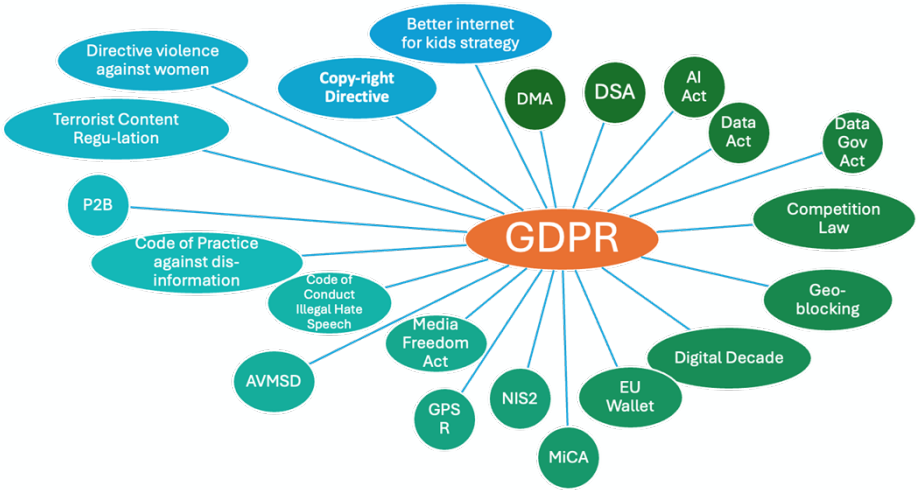
- Race to AI Regulation
- Regulatory Competition
- Brussel's Effect
- Grandi poteri privati

Due letture per capire (il governo e le opportunità)





In principio era il GDPR...

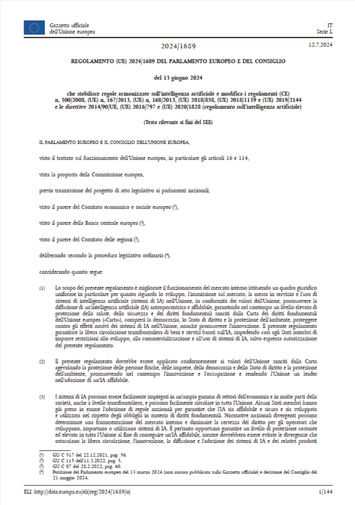


Contesto normativo sull’IA

UNIVERSITÀ DEGLI STUDI FIRENZE | CYBERIGHTS

livello europeo

Regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act)


Gazzetta ufficiale dell'Unione europea — IT Serie L

2024/1689 — 12.7.2024

REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 13 giugno 2024

che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)

(Testo rilevante ai fini del SEE)

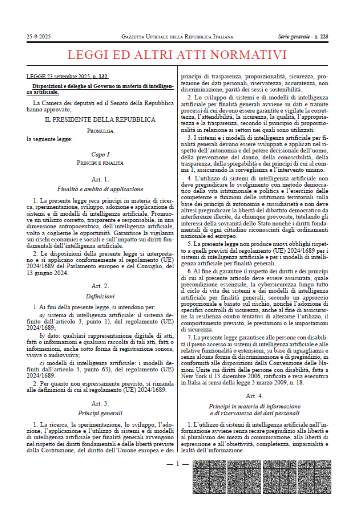
IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare gli articoli 16 e 114,

vista la proposta della Commissione europea,

livello nazionale

Legge 132/2025 – Disposizioni e deleghe al Governo in materia di intelligenza artificiale


25-9-2025 — GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA — *Serie generale* - n. 223

LEGGI ED ALTRI ATTI NORMATIVI

LEGGE 23 settembre 2025, n. 132.

Disposizioni e deleghe al Governo in materia di intelligenza artificiale.

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

PROMULGA

la seguente legge:

Capo I

PRINCIPI E FINALITÀ

Art. 1.

Finalità e ambito di applicazione

principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.

2. Lo sviluppo di sistemi e di modelli di intelligenza artificiale per finalità generali avviene su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l’attendibilità, la sicurezza, la qualità, l’appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati.

3. I sistemi e i modelli di intelligenza artificiale per finalità generali devono essere sviluppati e applicati nel rispetto dell’autonomia e del potere decisionale dell’uomo, della prevenzione del danno, della conoscibilità, della trasparenza, della spiegabilità e dei principi di cui al comma 1, assicurando la sorveglianza e l’intervento umano.

4. L’utilizzo di sistemi di intelligenza artificiale non deve pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica e l’esercizio delle

livello regionale

Legge regionale 57/2024 – Disciplina dell’innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale

Informatica e Reti telematiche — l.r. 57/2024 — 1

Legge regionale 9 dicembre 2024, n. 57

Disciplina dell’innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla l.r. 54/2009.

(Bollettino Ufficiale n. 70, parte prima, del 18.12.2024)

Proposta di legge n.52 del 16-02-2026 – Uso responsabile e consapevole dell’Intelligenza artificiale

Proposta di legge

Uso responsabile e consapevole dell’Intelligenza artificiale

Contesto normativo sulla (cyber)sicurezza

Quadro giuridico italiano sulla cybersicurezza

- **D.lgs. n. 65/2018**, recepimento Direttiva NIS
- **D.l. n. 105/2019**, convertito in legge n. 133/2019, istituzione del Perimetro di sicurezza nazionale cibernetica
- **D.l. n. 82/2021**, convertito in legge n. 109/2021
- **Legge n. 90/2024** (giugno 2024)
- **D.lgs. n. 138/2024** (settembre 2024), recepimento Direttiva NIS 2
- **D.lgs. n. 134/2024** (settembre 2024), recepimento Direttiva CER
- **D.lgs. n. 23/2025** (marzo 2025), adeguamento a Direttiva DORA e D. NIS 2

Le componenti della cybersecurity

1. Cyber-**intelligence**
2. Cyber-**warfare**
3. Cyber-**crime**
4. Cyber-**terrorism**
5. Cyber-**resilienza**

Regolazione del rischio per l'IA

Anche l'AI Act segue un approccio basato sul rischio *(c.d. risk-based)*.

Sistema di IA

- Rischio inaccettabile (pratiche vietate)
- Rischio elevato *(high risk)*
- Rischio di trasparenza
- Rischio minimo o nullo

Modello di IA

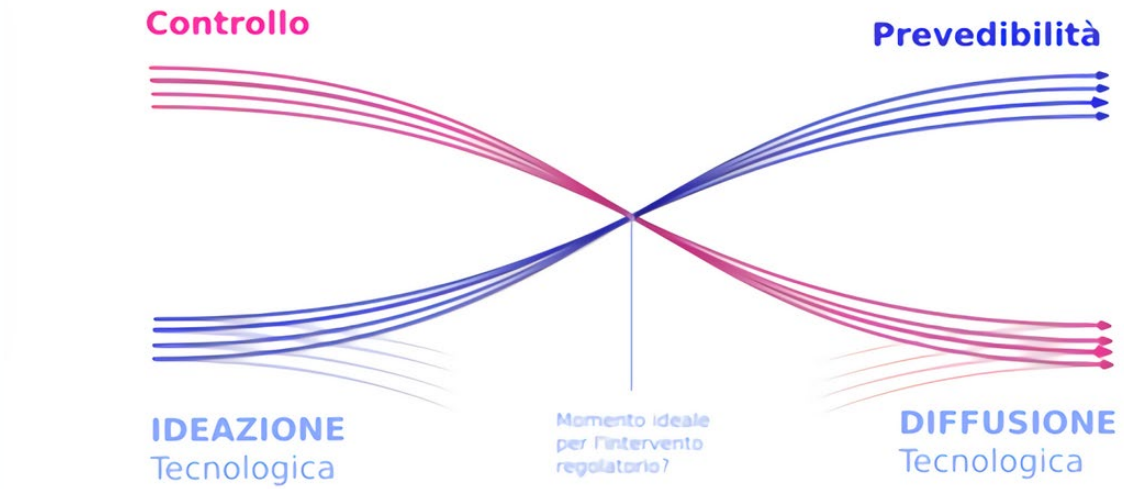
- Modello di IA per finalità generali
- Modello di IA per finalità generali con rischio sistemico

Per quanto riguarda i sistemi di IA, la classificazione del livello di rischio segue la **finalità prevista** e il **contesto di deployment**, non la specifica tecnologia.

Allo stesso modo, per i modelli, il rischio sistemico si basa sulla soglia delle **capacità di calcolo** e sul **possibile impatto** dello stesso.

Bilanciamento tra innovazione e regolazione

Il dilemma di Collingridge sul controllo sociale della tecnologia



Adapted Bestri F., Samprè F. (2018) Responsability driven design for the future self-driving society, Fondazione Giannino Bassetti

Asimmetria informativa tra sviluppatori e regolatori

Comprensione o fiducia limitate

Quadro giuridico complesso per la convalida della tecnologia

UNIVERSITÀ DEGLI STUDI FIRENZE

Casi studio applicativi in ambito AI e opportunità per i servizi pubblici

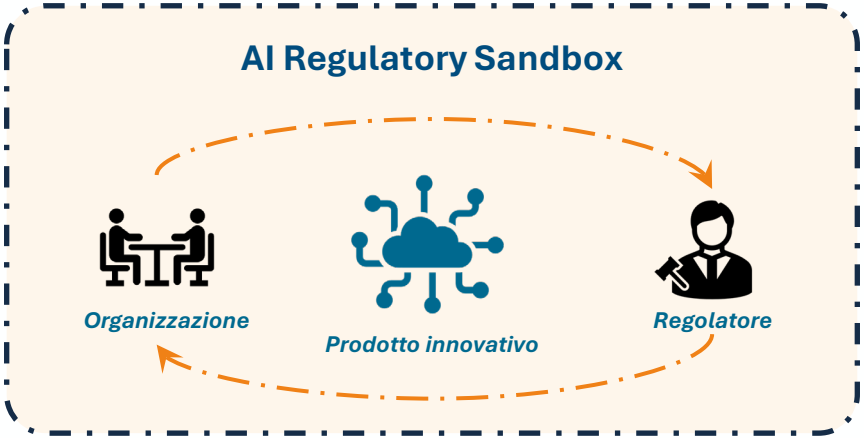
Massa, 11/04/2026

Matteo Giannelli

Università degli studi di Firenze, Centro CybeRights

Cos’è una regulatory sandbox per l’IA

L’Articolo 3(55) dell’AI Act definisce uno «spazio di sperimentazione normativa per l’IA» come «un **quadro controllato** istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di **sviluppare, addestrare, convalidare e provare [testing]**, se del caso in **condizioni reali**, un **sistema di IA innovativo**, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare».



Valore aggiunto dei quadri di sandbox

Sandbox come metodo abilitante dell'innovazione responsabile attraverso servizi dedicati a sviluppatori, deployer, PA ed enti di regolazione

- (A) Supporto nell'**interpretazione normativa** congiunta tra requisiti dell'AI Act e altre normative (locali, settoriali)
- (B) Accesso ad **ambienti virtuali di test** e supporto nella convalida tecnica dei sistemi
- (C) **Implementazioni reale su scala controllata** nella PA o in contesti di servizi nel territorio
- (D) Facilitazione dell'**accesso a dataset** aperti e/o sintetici
- (E) Condivisione e **trasferimento delle conoscenze** per le parti interessate e le organizzazioni coinvolte





La sperimentazione a livello europeo

EUSAiR è un **progetto biennale**, finanziato dal programma Europa digitale dell'Unione europea, che **supporta e contribuisce al coordinamento e all'implementazione** delle regulatory sandboxes sull'intelligenza artificiale secondo l'AI Act in tutta l'UE.

Risultati preliminari delle sandbox pilota EUSAiR per i servizi pubblici

a. L'**attenzione alla conformità** all'AI Act è in continua **crescita**.

b. **Omogeneità** tra le **tecnologie di AI/ML** utilizzata, **eterogeneità** degli specifici casi di **implementazione** → focus principale su finalità prevista, settore/ambito di deployment, classificazione del rischio, governance dei dati, sorveglianza umana

c. Principali servizi in ambito: **sanità**, **istruzione**, **servizi alla cittadinanza**, **monitoraggio infrastrutture**

d. Sandbox utile anche per la **definizione anticipata di feature** di prodotto (o nella fase di procurement)

UNIVERSITÀ DEGLI STUDI FIRENZE

Il ruolo dell'Università e di CybeRights nell'innovazione locale

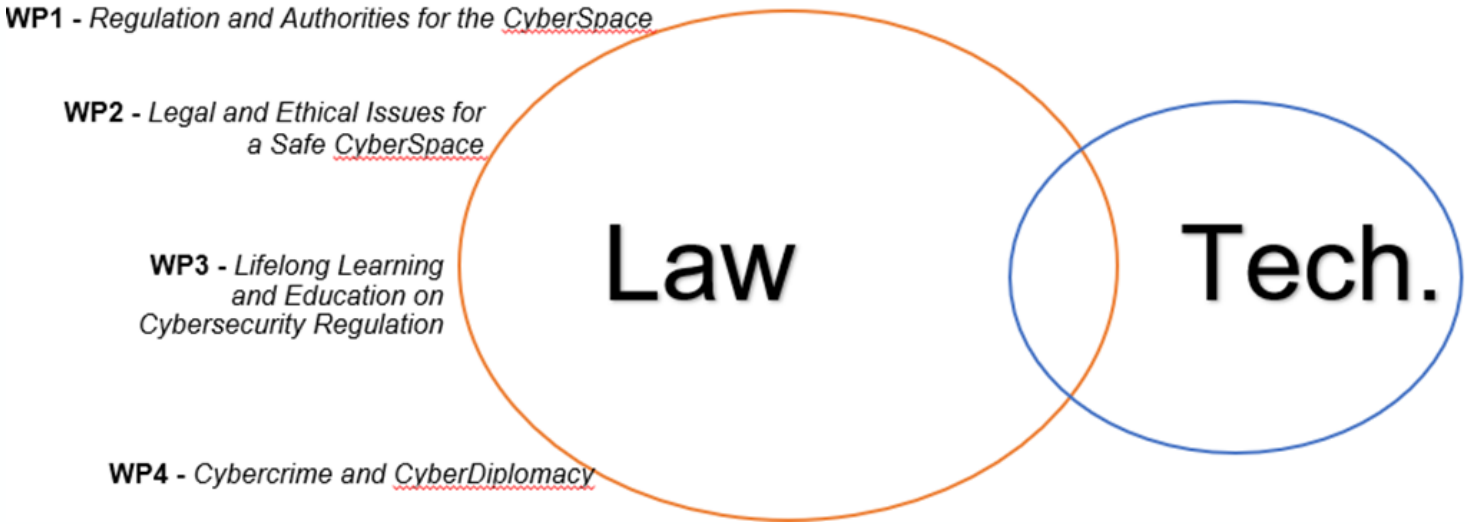
Massa, 11/04/2026

Matteo Giannelli

Università degli studi di Firenze, Centro CybeRights

Il Centro interuniversitario di ricerca CybeRights

CybeRights
Law and regulation for a better-safe Cyberspace



Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

SERICS
AREE TEMATICHE

SPOKE

SPOKE 1
Aspetti umani, sociali e legali
CNR

SPOKE 2
Disinformazione e fake news
UNISA

SPOKE 3
Attacchi e difese
UNICA

SPOKE 4
Sicurezza dei sistemi operativi e della visualizzazione
UNIGE

SPOKE 5
Crittografia e sicurezza dei sistemi distribuiti
UNICAL

SPOKE 6
Sicurezza del software e delle piattaforme
UNIVE

SPOKE 7
Sicurezza delle infrastrutture
POLITO

SPOKE 8
Gestione del rischio e governance
UNIBO

SPOKE 9
Mettere in sicurezza la trasformazione digitale
UNIROMA

SPOKE 10
Governance e protezione dei dati
UNIMI

CybeRights. La rete istituzionale

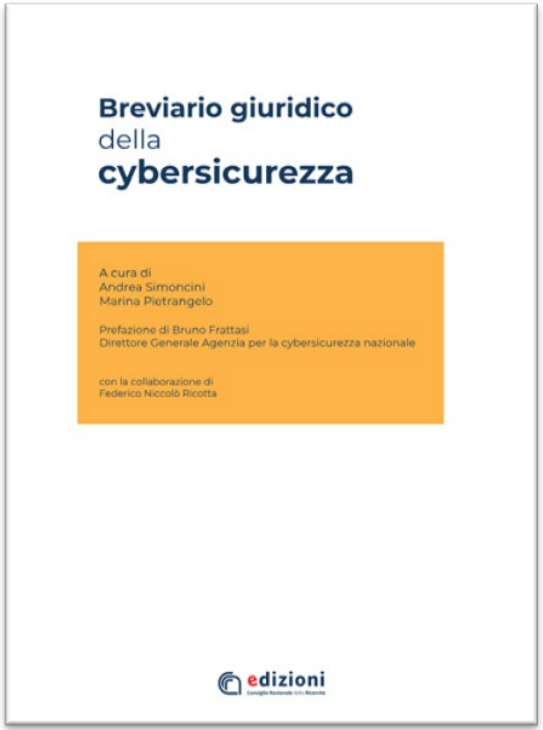
Collaborazioni con **Agenzie e Autorità nazionali**

- ACN (Cybersecurity - NIS2);
- GPDP (Privacy - GDPR e AI ACT);
- AGCOM (ICTs – DSA, FLODIR);

Cooperazione con **Regioni ed enti locali** (Toscana)

- CSIRT
- 5G
- Digital Governance

Oltre il PNRR (I): l'Osservatorio e il Breviario



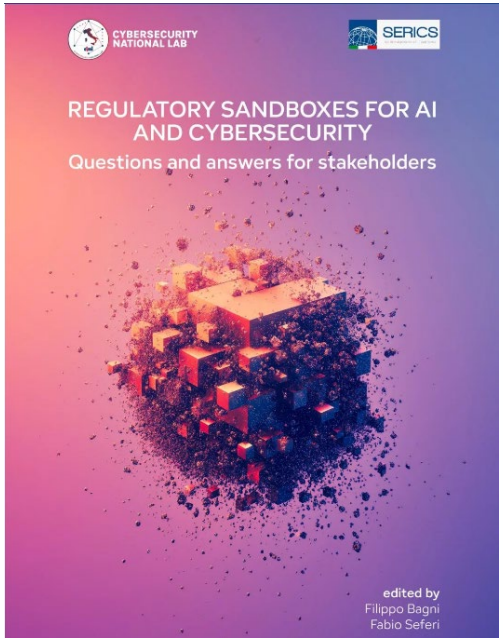
Oltre il PNRR (II): le Regulatory Sandboxes

CYBERSECURITY NATIONAL LAB

COMUNICATO STAMPA

Libro Bianco sulla *Regulatory Sandboxes*: una guida per l'innovazione e la conformità normativa in Europa in tema di IA e Cybersicurezza

EUSAiR
BRIDGING INNOVATION AND COMPLIANCE IN AI



CybeRights,
le aree tematiche di ricerca e trasferimento del Centro

- Law and Authority for Cyberspace (**DiLac**);
- Legal and Ethics Issues for a Secure Cyberspace (**DileSec**);
- Lifelong Learning and Legal Training on Cyber Security (**DilTec**);
- Cyber Crime and Cyber Diplomacy (**DiCrime**);
- Urban Technologies and Rights (**URbiTEC**);
- Resilience and Security in National Interest (**ReSiN**);
- Quantum computing and Cybersecurity (**QuaSec**);
- Cybersecurity in Space Operations (**CySOp**);

Per saperne di più: **cyberights.unifi.it** (in aggiornamento)

CybeRights, l'importanza di un ecosistema

- Ecosistema della ricerca in Cybersecurity
- L'evoluzione tecnologica e della minaccia richiedono un costante lavoro di aggiornamento degli strumenti (tecnologici e normativi)
- Ruolo delle sandbox regolatorie
- Importanza della collaborazione inter-istituzionale
    - aggiornamento e potenziamento della formazione post-laurea

CybeRights, la formazione

Nuova edizione

dal 26 maggio al 8 luglio 2026

Per informazioni cliccare qua

UNIVERSITÀ DEGLI STUDI FIRENZE

Grazie!

matteo.giannelli@unifi.it
cyberights@cyberights.unifi.it

Matteo Giannelli

Università degli studi di Firenze, Centro CybeRights