

AI Legal 2026

Privacy, Protezione dei Dati e Confidenzialità nel diritto digitale

La regolamentazione europea del mercato digitale: i sistemi di intelligenza artificiale tra circolazione dei dati e tutela dei diritti fondamentali

Prof. Valentina Di Gregorio



Martedì, 24 Febbraio 2026



1. La transizione digitale.

Protezione dei dati vs circolazione dei dati

Sviluppo del
mercato



Innovazione

Circolazione dei dati

L'intelligenza artificiale e l'innovazione tecnologica stanno ridefinendo l'economia digitale dell'UE

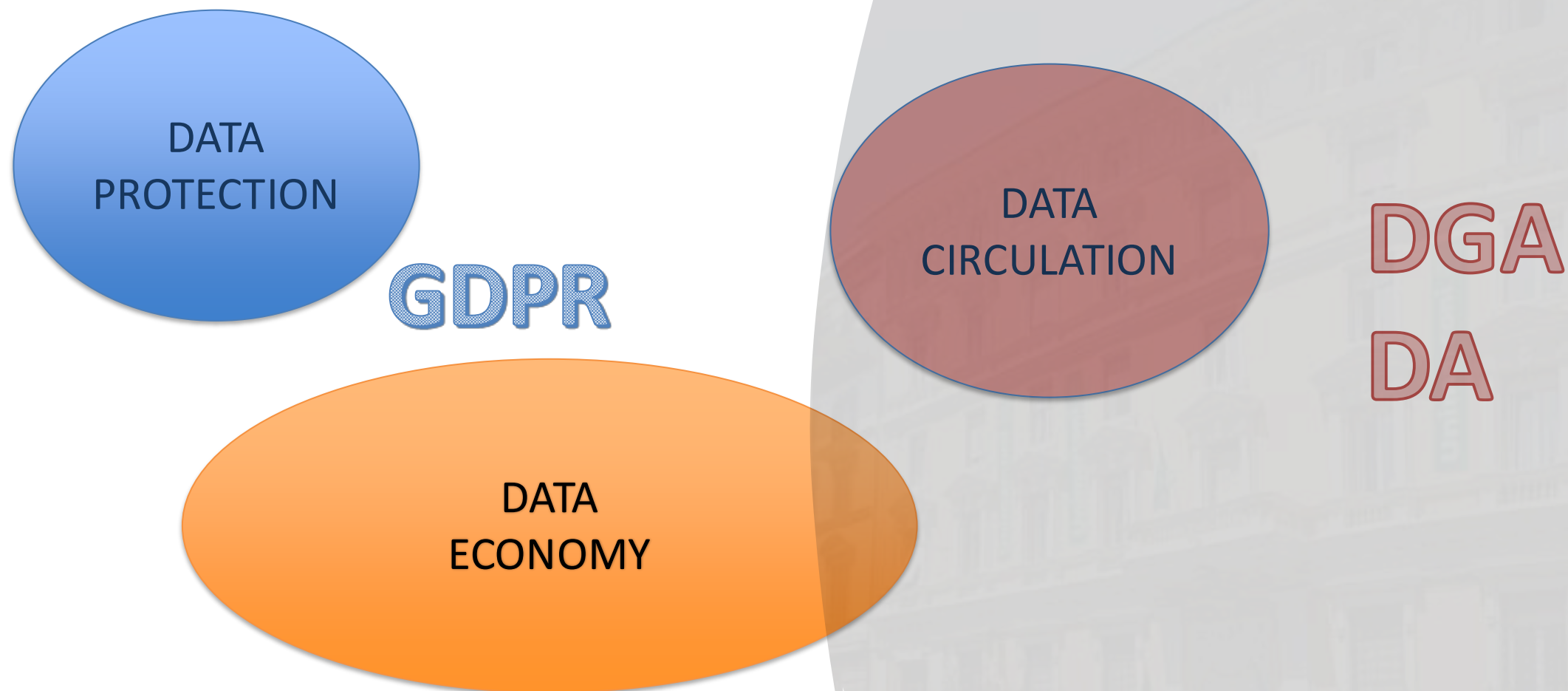
L'Intelligenza Artificiale si basa sui dati

Strategia dell'Ue: promuovere l'innovazione sbloccando i dati e garantendo al contempo:
protezione di salute, sicurezza, diritti fondamentali sanciti dalla Carta UE, compresi democrazia, stato
di diritto, protezione ambiente

2. Normativa europea essenziale

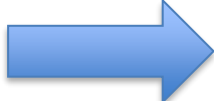
- GDPR (679/2016): Focus sulla protezione dei dati personali
- Data Governance Act (2022): Accesso equo ai dati
- Data Act (2023): Miglioramento dell'accesso ai dati e dell'interoperabilità soprattutto per servizi IoT
- AI Act (1689/2024): Quadro normativo basato sul rischio per la regolamentazione dell'AI
- Direttiva sulla responsabilità del produttore (2024): modifica il quadro precedente includendo il software nella definizione di prodotto
- Digital Services Package (2022): spazio digitale più sicuro per i clienti dei servizi e le piattaforme composto da *Digital services Act* (riguarda i servizi digitali che svolgono funzione di intermediari tra utenti e contenuti, beni o servizi come social network e piattaforme di condivisione) e *Digital markets Act* (impone regole severe ai "gatekeeper" e mira a garantire un mercato digitale più equo, trasparenti e concorrenziali).
- Regolamento Spazio europeo dati sanitari EHDS (2025)
- Proposta di regolamento "Digital Omnibus" (2025) n. 836 (per l'AI Act) e n.837 (per GDPR, e privacy, direttiva NIS 2, Data act) che propongono emendamenti

3. Quadro normative dell'UE. La sovranità tecnologica dell'UE



Dato come risorsa economica

4. I dati alimentano l'intelligenza artificiale: l'intervento del legislatore UE con L'AI act (reg. 2024/1689)

Dati in circolazione:  motore per l'economia

Rapidità dell'innovazione tecnologica e sviluppo esponenziale dell'AI



necessità di una struttura regolatoria per controllo della sicurezza e dell'affidabilità dei sistemi di AI, potenziamento competitività delle imprese europee e cooperazione tra gli Stati membri.

5. L'AI Act e la valutazione dell'impatto sui diritti fondamentali

- AI antropocentrica e affidabile
- Valutazione della conformità e supervisione

Valutazione d'impatto: valutazione *ex ante* dell'impatto delle politiche, delle attività commerciali, dei sistemi di IA, ecc.

- Valutazione d'impatto sulla protezione dei dati (**DPIA**) (art. 35)
- Valutazione d'impatto sui diritti fondamentali (**FRIA**) (art. 27)

6. Il paradigma del legislatore europeo incentrato sul rischio

L'AI Act definisce l'intelligenza artificiale e opta per il **risk-based approach**

Uso dell'IA nell'UE **sicuro ed etico**

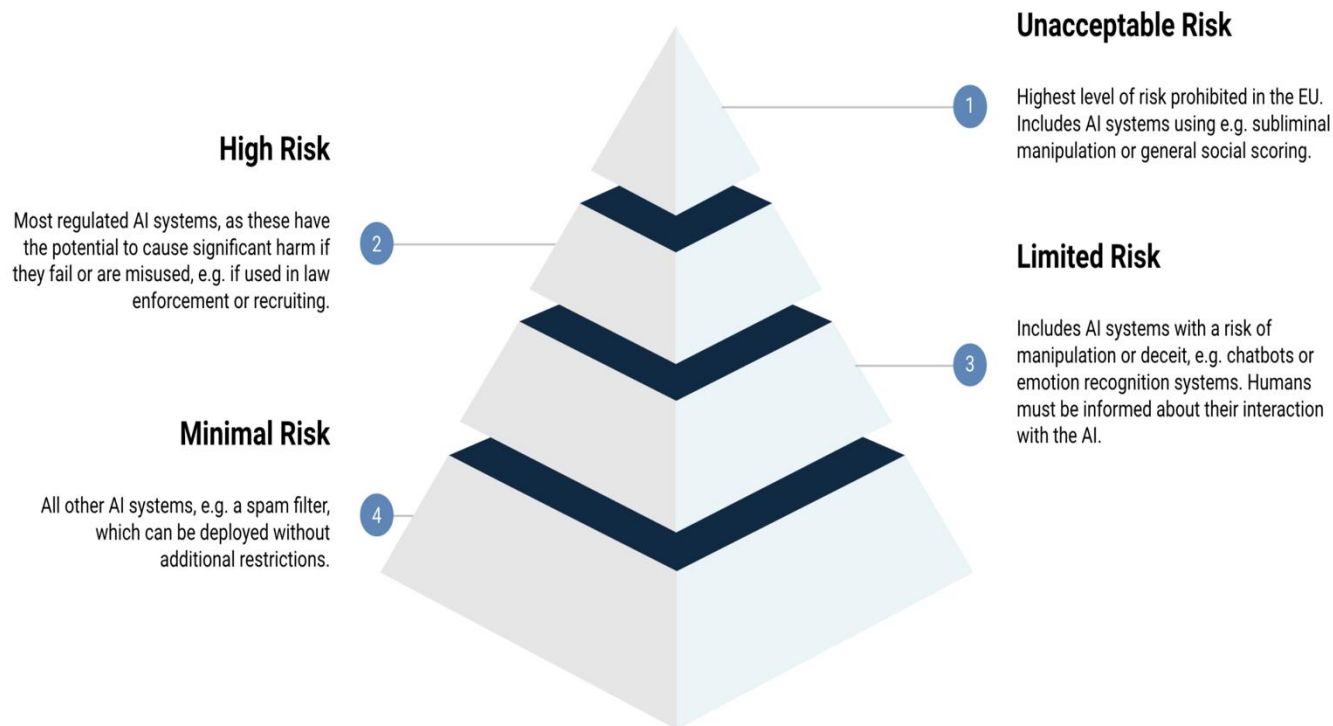
con obblighi alle imprese:

- conformità alle prescrizioni normative del regolamento e in altre norme armonizzate
- trasparenza
- non discriminazione
- protezione dei dati personali

Garanzia di un livello elevato di **tutela dei diritti fondamentali delle persone**



7. Risk-based approach



Unacceptable risk: applicazioni vietate perché che creano un rischio inaccettabile per la sicurezza, la salute o i diritti fondamentali delle persone.

High risk: sistemi AI che presentano un alto grado di potenziale danno per la salute, la sicurezza o i diritti fondamentali delle persone. Sono soggetti a una maggiore supervisione e valutazione.

Limited risk: rischi associati alla mancanza di trasparenza nell'uso dell'IA. Specifici obblighi di trasparenza per garantire un'adeguata informazione, promuovendo la fiducia delle persone nell'AI

Minimal risk: non soggette a restrizioni specifiche. Applicazioni che pongono un rischio minimo o nullo per la sicurezza, la salute o i diritti fondamentali delle persone.

8. AI Act: la regolamentazione basata sul rischio e questioni di responsabilità

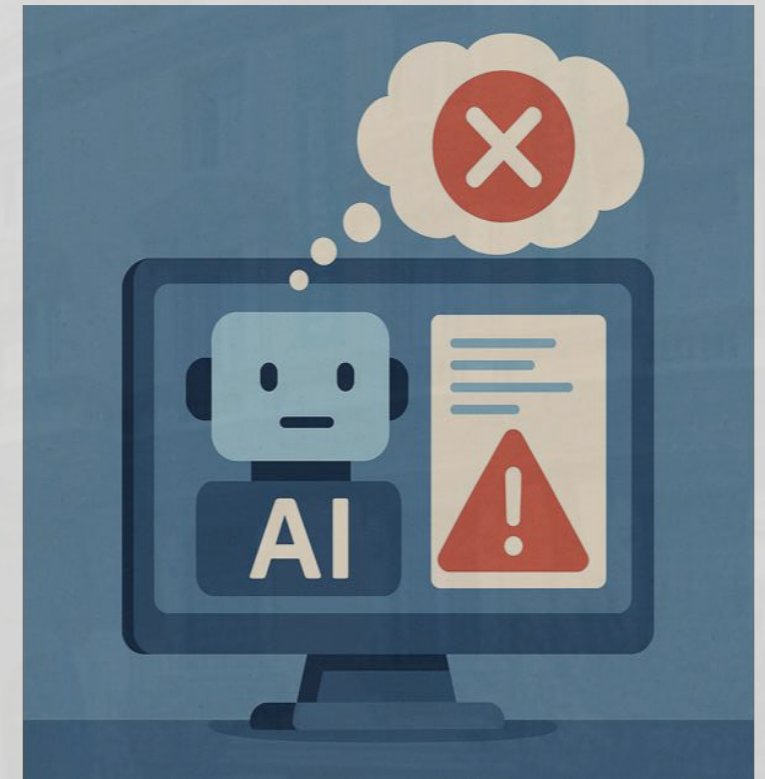
Nessun quadro armonizzato a livello UE in materia di responsabilità civile per l'IA.

In Italia: articoli 2050 e 2051 del codice civile, **Direttiva sulla responsabilità del produttore (UE) 2024/2853**

Problemi per i casi esclusi:

- *distruzione o corruzione dei dati*
- *danni quali perdite economiche pure, violazioni della privacy o discriminazione*

In Italia In Italia, l. delega n.132/2025 (art. 24, 5° comma, lett. c) d)



9. Approccio basato sul rischio e responsabilità dei sistemi di IA

AI Act prevede una
classificazione dei sistemi
di IA basata sul rischio.

Raccomandato un regime
di responsabilità
differenziato, in base sia al
livello di rischio che al
settore di applicazione.

10. Proposta Digital Omnibus UE 2025

Proposte nn. n. 836 (per AI Act e reg. 2018/1139) e n.837 (per GDPR, dir. e-privacy, dir. NIS 2, Data act).

Obiettivi:

- ❖ **Armonizzazione** del quadro normativo digitale (privacy, dati, IA, cybersecurity) per eliminare incoerenze tra norme (GDPR, AI Act, Data Governance) e collegamento del calendario di attuazione delle norme in tema di alto rischio con la disponibilità di standard di supporto.
- ❖ **Riduzione** della frammentazione regolatoria, anche accorpando nel Data Act la normativa su governance dei dati, libera circolazione dei dati non personali
- ❖ **Semplificazione** oneri amministrativi per imprese, per le PMI e le piccole imprese a media capitalizzazione (small Mid-cap Enterprises, SMCs e per enti pubblici
- ❖ **Single-Entry point:** portale che centralizzerà le notifiche richieste dal GDPR, dal NIS2, dal DORA, dall'eIDAS e dalla direttiva CER.

11. Digital Omnibus e dati personali: GDPR Reg. EU 679/2016

Obiettivi:

Art. 1 Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

Protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

La proposta di regolamento Digital Omnibus COM(2025)837, 19/11/2025 incide su (tra gli altri articoli del GDPR)

Art. 4, 1) definizione di dato personale

Art. 6 condizioni di liceità del trattamento e inserimento art. 88 c

Art. 9 Trattamento di categoria particolari di dati personali

Art.22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

Art.33 Notifica violazione dei dati personali all'autorità di controllo

12. Digital Omnibus e AI Act

➤ Obiettivo

Promuovere politiche innovative e orientate al futuro che rafforzino la competitività dell'Unione europea (UE) e alleggeriscano gli oneri normativi che gravano sui cittadini, sulle imprese e sulle amministrazioni

- **Estensione agevolazioni PMI a Small Mid-Cap Enterprises (SMCs)**
- **Modifica definizione art. 3: inserimento *agenti***
- **Introduzione art. 4 bis:** trattamento di dati di categorie particolari a fini di eliminare le distorsioni, estendendo ai sistemi di AI non ad alto rischio la possibilità di utilizzare dati sensibili per migliorare l'equità algoritmica(v. art.10)
- **Introduzione nell'art. 5 (pratiche vietate)** *«L'immissione sul mercato, la messa in servizio o l'utilizzo di un sistema di IA in grado di generare o manipolare audio, immagini e video a carattere sessuale di individui, facilitando in tal modo la condivisione non consensuale di materiale intimo o manipolato, come definito nella direttiva (UE) 2024/1385»*
- **Modifiche Articolo 6 (nn. 3 e 4) - Sistemi ad alto rischio**
punto 4: Eliminazione obbligo di registrazione nel database centrale per sistemi che, pur ricadendo in ambiti ad alto rischio, sono valutate internamente come non ad alto rischio con documentazione della valutazione del rischio
- **Codici di buone pratiche e spazi di sperimentazione (Artt. 50 e 56)** Rafforzamento ricorso a codici di condotta per obblighi di trasparenza relativi a contenuto generato artificialmente.

Grazie

Prof. Valentina Di Gregorio

valentina.digregorio@unige.it

