# AI Act:
# Luci ed ombre del nuovo modello di regolazione europea

18 giugno 2024

Prof. Maurizio Borghi
*Dipartimento di Giurisprudenza, Università di Torino*

Politecnico di Torino | Nexa Center for Internet & Society

Instagram

Accedi Iscriviti


[redacted] • Segui

[redacted] ULTIMA SERATA DELLA MASTERCLASS: PERCHÉ NON PUOI MANCARE?

Questa sera alle ore 21:30 finalmente ti rivelerò il mio nuovo Metodo Copia Incolla per scrivere un Libretto in meno di 1 Ora con ChatGPT!

Grazie a quello di cui ti parlerò questa sera tu potrai abbattere quasi del tutto i tempi di attesa per scrivere un libretto profittevole

Attenzione: questa è un'opportunità che potrebbe farti cambiare vita dall'oggi al domani

Non partecipare a questa diretta significa letteralmente bruciare i guadagni che faresti applicando

Piace a 30 persone

22 AGOSTO

Accedi per mettere "Mi piace" o commentare.

# Mushroom pickers urged to avoid foraging books on Amazon that appear to be written by AI

The Guardian

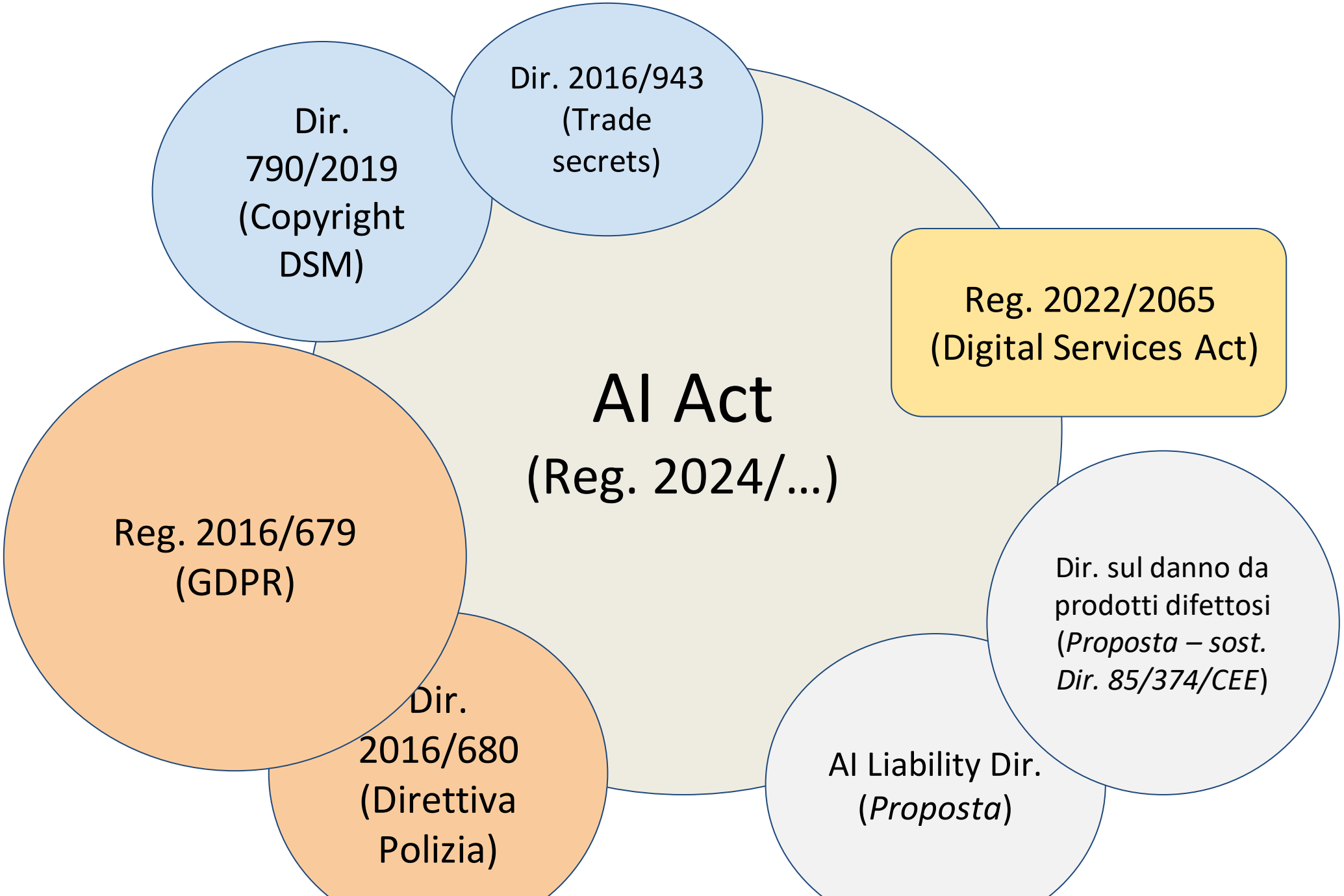
**Sample of books scored 100% on AI detection test as experts warn they contain dangerous advice**

Some of the books refer to smell and taste as ways to identify mushrooms, which experts say 'should absolutely not be the case'. Photograph: Justin Long/Alamy

Amateur mushroom pickers have been urged to avoid foraging books sold on Amazon that appear to have been written by artificial intelligence chatbots.

Amazon has become a marketplace for AI-produced tomes that are being

https://www.theguardian.com/technology/2023/sep/01/mushroom-pickers-urged-to-avoid-foraging-books-on-amazon-that-appear-to-be-written-by-ai


Dir. 790/2019 (Copyright DSM)
Dir. 2016/943 (Trade secrets)
Reg. 2022/2065 (Digital Services Act)
AI Act (Reg. 2024/…)
Reg. 2016/679 (GDPR)
Dir. 2016/680 (Direttiva Polizia)
Dir. sul danno da prodotti difettosi (*Proposta – sost. Dir. 85/374/CEE*)
AI Liability Dir. (*Proposta*)

# Ambito di applicazione - art. 2

- **Fornitori** di sistemi di AI o modelli di IA per finalità generali (situati in UE o in paesi terzi)
- ***Deployer*** di sistemi di IA (situati in UE o in paesi terzi se l'output è usato in UE)
- Importatori, distributori, fabbricanti di prodotti che incorporano AI, …

*Non si applica a:*

- Usi non professionali puramente **personali**
- Usi unicamente per **ricerca scientifica**
- Sistemi di IA per scopi **militari**, di difesa o di **sicurezza nazionale**
- Sistemi di IA con licenza **open source** (*ma con eccezioni*)

# Definizioni - art. 3

(3) "**fornitore**": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che **sviluppa** un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e **immette tale sistema o modello sul mercato** o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito;

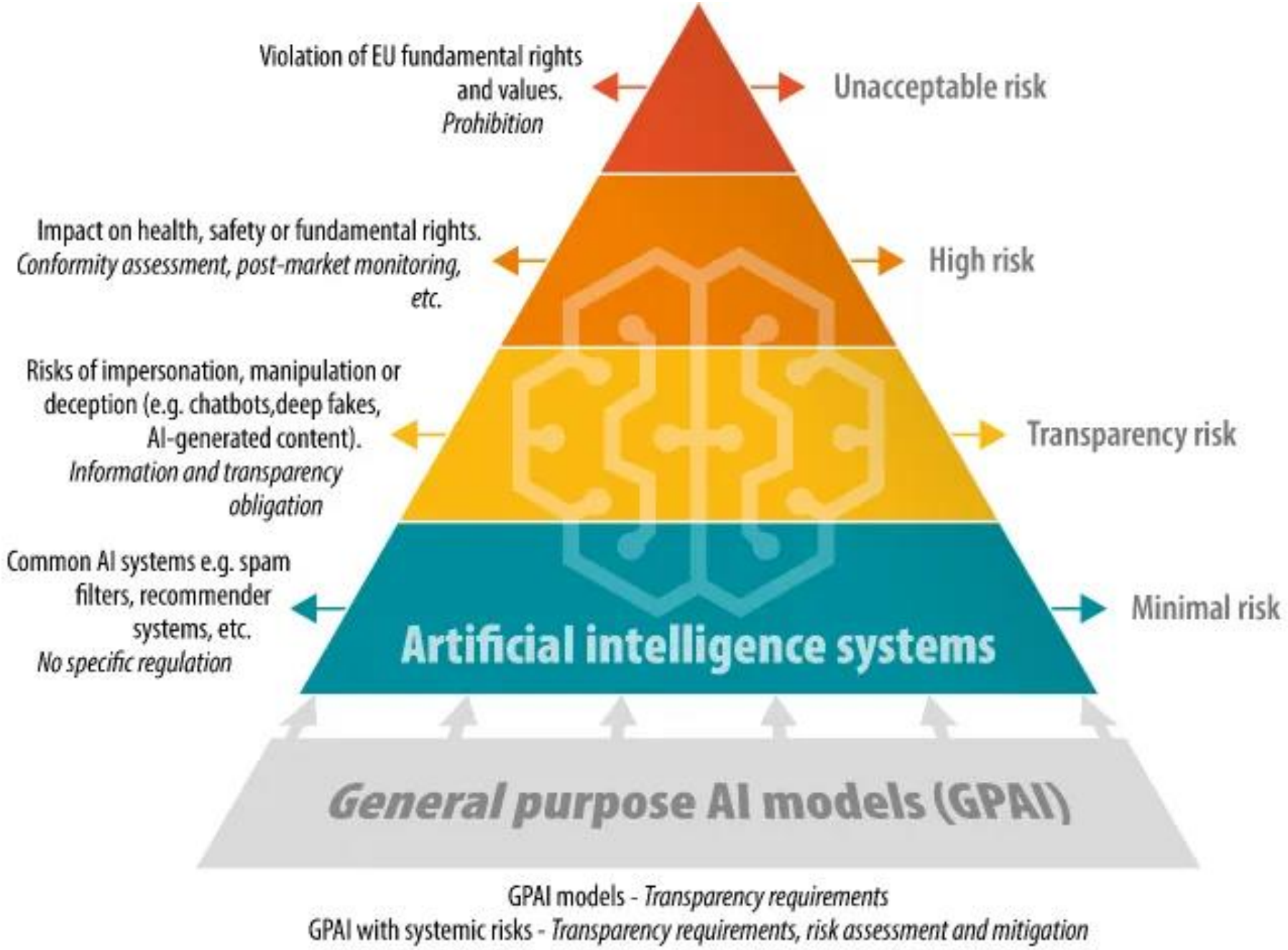
(4) "***deployer***": persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che **utilizza un sistema di IA sotto la propria autorità**, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale;

# Definizioni - art. 3

(1) "**sistema di IA**": un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

(43) "**modello di IA per finalità generali**": un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato;

UNIVERSITÀ DI TORINO




Data source: European Commission

# Pratiche di IA vietate – art. 5

*Il divieto (non assoluto) si applica a 8 tipologie di pratiche*:

a) Uso di tecniche **subliminali** di persuasione

b) Sfruttamento di **vulnerabilità** di soggetti fragili

c) Valutazione di persone in base al loro comportamento (‘***social scoring***’)

d) Valutazione del **rischio di recidiva** da parte di persone fisiche

e) Creazione di banche dati per **riconoscimento facciale** mediante scraping

f) Uso per **inferire emozioni** di persone fisiche in luoghi di lavoro

**g) Categorizzazione biometrica** per trarre deduzioni su razza, opinioni politiche, orientamento sessuale ecc.

h) Identificazione **biometrica remota in tempo reale**

# Sistemi di IA ad alto rischio – art. 6

*Un sistema di IA è classificato 'ad alto rischio' se*:

1) è un componente di sicurezza o un **prodotto disciplinato** da normativa UE in elenco (All. I) ed è soggetto a **valutazione di conformità** da parte di terzi (giocattoli, applicazioni mediche, ascensori, veicoli, impianti a fune, …) – *oppure:*

2) Il sistema è usato per una **finalità specifica** elencata in All. *L'elenco include:*

- Uso in infrastrutture critiche (viabilità, acqua, gas, elettricità…)
- Educazione, lavoro, servizi pubblici (sanità) o privati essenziali (assicurazioni)
- Uso da parte di forze dell'ordine, immigrazione, amministrazione della giustizia
- Processo democratico (elezioni)
- Categorizzazione biometrica non vietata, riconoscimento di stati emotivi, profilazione

# Sistemi di IA ad alto rischio – art. 6

***Eccezioni**: quando il sistema AI è destinato a*

- Eseguire un compito procedurale limitato
- Migliorare il risultato di un'attività umana precedentemente completata
- Rilevare schemi decisionali precedenti senza sostituire o influenzare la valutazione umana
- Eseguire un compito preparatorio per una valutazione

(*Sono attese linee guida della Commissione sull'interpretazione delle deroghe all'art. 6.2*)

# Requisiti – art. 8-15

Il Regolamento prevede requisiti stringenti per i sistemi IA classificati ‘ad alto rischio’, che riguardano in particolare:

- **Dati e governance dei dati** (art. 10): *i dataset di addestramento devono essere rilevanti, sufficientemente rappresentativi e, nei limiti del possibile, corretti*
- **Sorveglianza umana** (art. 14): *i sistemi devono essere progettati in modo da includere sostanziali misure di sorveglianza*
- **Accuratezza, robustezza e cibersicurezza** (art. 15): *i sistemi che continuano l’apprenidimento una volta immessi sul mercato devono prevenire o ridurre il rischio di output potenzialmente distorti*

# Obblighi di fornitori e *deployer* – art. 16-30

Chi è considerato **fornitore** di un sistema IA ad alto rischio (IAar)?

Art. 25(1): Ogni distributore, importatore o *deployer* che:

- Appone il proprio **nome o marchio** su un sistema IAar
- Apporta una **modifica sostanziale** a un sistema IAar
- Modifica la **finalità** prevista di un sistema IA in modo tale che diventi IAar

«Modifica sostanziale»: modifica di un sistema di IA a seguito della sua immissione sul mercato o messa in servizio che **non è prevista o programmata nella valutazione iniziale della conformità** effettuata dal fornitore e che ha l'effetto di incidere sulla conformità del sistema di IA ai requisiti di cui al capo II, sezione 2, o comporta una modifica della finalità prevista per la quale il sistema di IA è stato valutato

# Obblighi di fornitori e *deployer* – art. 16-30

**Valutazione di conformità** – Art. 16(f)

*Prima dell'introduzione nel mercato, il fornitore deve condurre una valutazione che include:*

- Qualità e governance dei dati; Documentazione tecnica; Informativa agli utenti; Garanzia di supervisione umana; Misure per garantire accuratezza, robustezza e cibersicurezza

*Al prodotto viene apposta la marcatura CE*

*Il fornitore deve inoltre prevedere un **sistema di gestione della qualità** (Art. 17) e **misure correttive** (Art. 20)*

Per alcuni sistemi IAar è inoltre prevista la **Valutazione d'impatto sui diritti fondamentali** (Art. 27)

# Sistemi di IA soggetti (soltanto) a obblighi di trasparenza – art. 50

*Quattro categorie di sistemi di IA sono considerati 'a basso rischio':*

- Sistemi che interagiscono direttamente con persone fisiche (**Chatbots**)
  - → Obbligo di informare la persona
- Sistemi che **generano** contenuti audio, immagine, video o testi sintetici
  - → Obbligo di marchiatura (ove tecnicamente possibile)
- Sistemi di **riconoscimento delle emozioni** o **riconoscimento facciale**
  - → Obbligo di informare la persona
- Sistemi di generazione di '**deep fake**'
  - → Obbligo di indicare l'origine (a meno che vi sia un evidente intento satirico)

*Gli obblighi non si applicano per usi investigativi ecc. da parte di forze di polizia.*

# Modelli per finalità generali

Art. 3(43) "**modello di IA per finalità generali**": un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando **l'autosupervisione su larga scala**, che sia caratterizzato una **generalità significativa** e sia in grado di svolgere con competenza **un'ampia gamma di compiti distinti**, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato;

# Classificazione dei MIAFG – art. 51

Un MIAFG è considerato **a rischio sistemico** se

a) presenta **capacità di impatto elevato** valutate sulla base di strumenti tecnici e metodologie adeguati

b) sulla base di una decisione della Commissione**, ex officio** o a seguito di una segnalazione qualificata del gruppo di esperti scientifici, presenta capacità o un impatto equivalenti a quelli di cui alla lettera a)

(Il rischio sistemico è presunto se FLOP > 10^25)

Comprende un ampio spettro di '**possibili effetti negativi ragionevolmente prevedibili**' – dalla catastrofe nucleare alla divulgazione di fake news… (Cons. 110)

# Obblighi dei fornitori di MIAFG – art. 53

*Sono tenuti a fornire:*

- **Documentazione tecnica** sul funzionamento del modello (incl. addestramento, datasets, consumo energetico…)
- Informazioni **per i fornitori di sistemi di IA** che integrano il MIAFG (fatti salvi i segreti commerciali)
- **Politica sul copyright** – in particolare sul rispetto della 'riserva' ex art. 4 Dir. 790/2019
- 'Sintesi sufficientemente dettagliata dei **contenuti utilizzati** per l'addestramento'

# Obblighi dei fornitori di MIAFG – art. 53

*Ancora sulla copyright policy:*

Cons. 106: i fornitori di MIAFG dovrebbero mettere in atto una politica volta a rispettare la normativa dell'Unione in materia di diritto d'autore e diritti connessi, in particolare per individuare e rispettare le riserve dei diritti espresse dai titolari dei diritti a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790. Qualsiasi fornitore che immetta sul mercato dell'Unione un MIAFG dovrebbe rispettare tale obbligo, **indipendentemente dalla giurisdizione in cui hanno luogo gli atti** pertinenti in materia di diritto d'autore alla base dell'addestramento di tali MIAFG. Ciò è necessario per garantire condizioni di parità tra i fornitori di modelli di IA per finalità generali, dato che nessun fornitore dovrebbe essere in grado di ottenere un vantaggio competitivo nel mercato dell'Unione applicando norme in materia di diritto d'autore **meno rigorose** di quelle previste nell'Unione.

UNIVERSITÀ DI TORINO

# Le esenzioni per modelli open-source

I fornitori di MIAFG open source sono **esentati** dagli obblighi di i) Documentazione tecnica e ii) Informazioni a fornitori di sistemi IA (ma non dagli obblighi relativi al copyright!)

*…a meno che non siano classificati come modelli 'a rischio sistemico'*

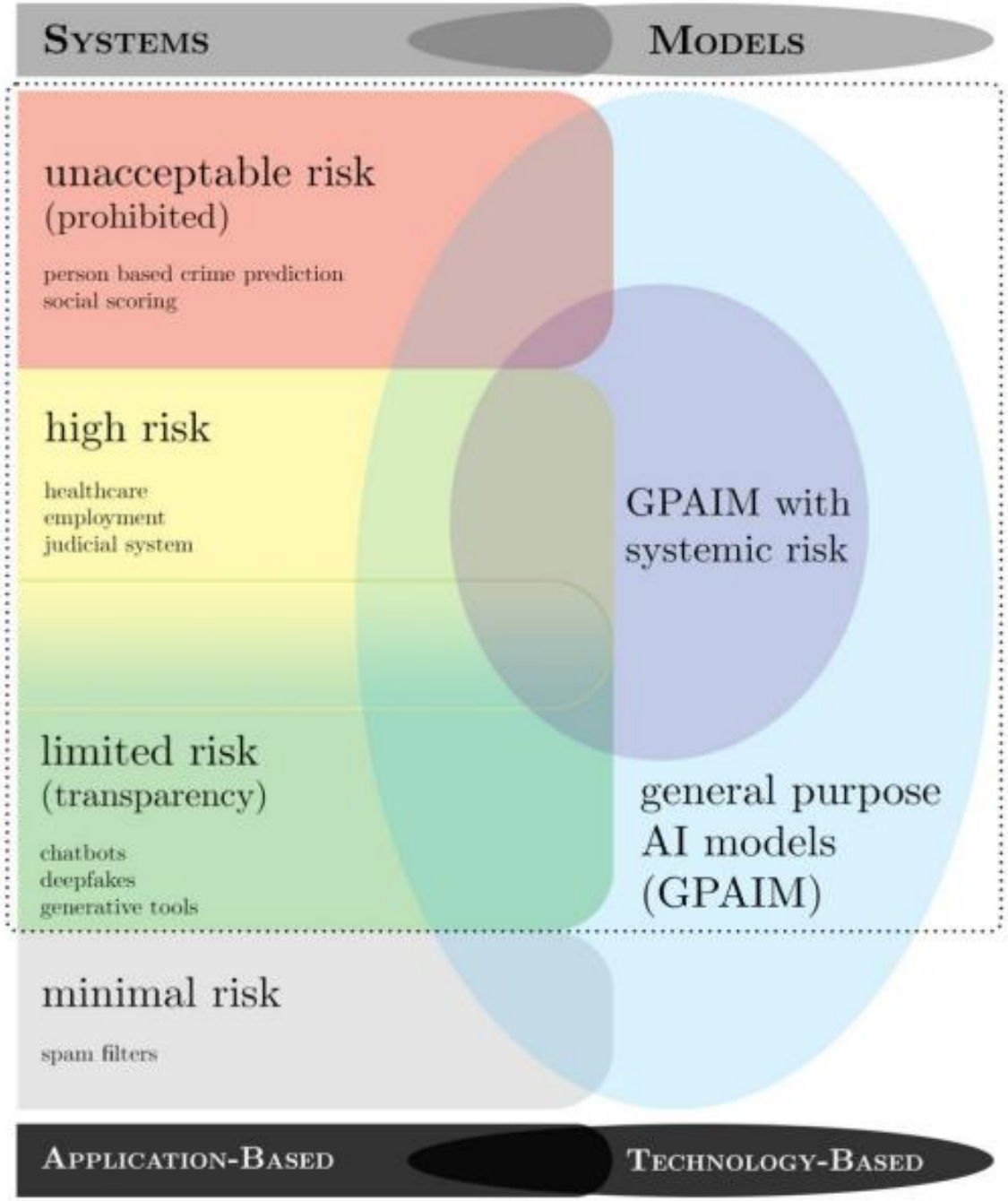
*…e a condizione che siano distribuiti* ***interamente a titolo gratuito***

(nemmeno supporto tecnico a pagamento)

# Obblighi per fornitori di MIAFG con rischio sistemico – art. 55

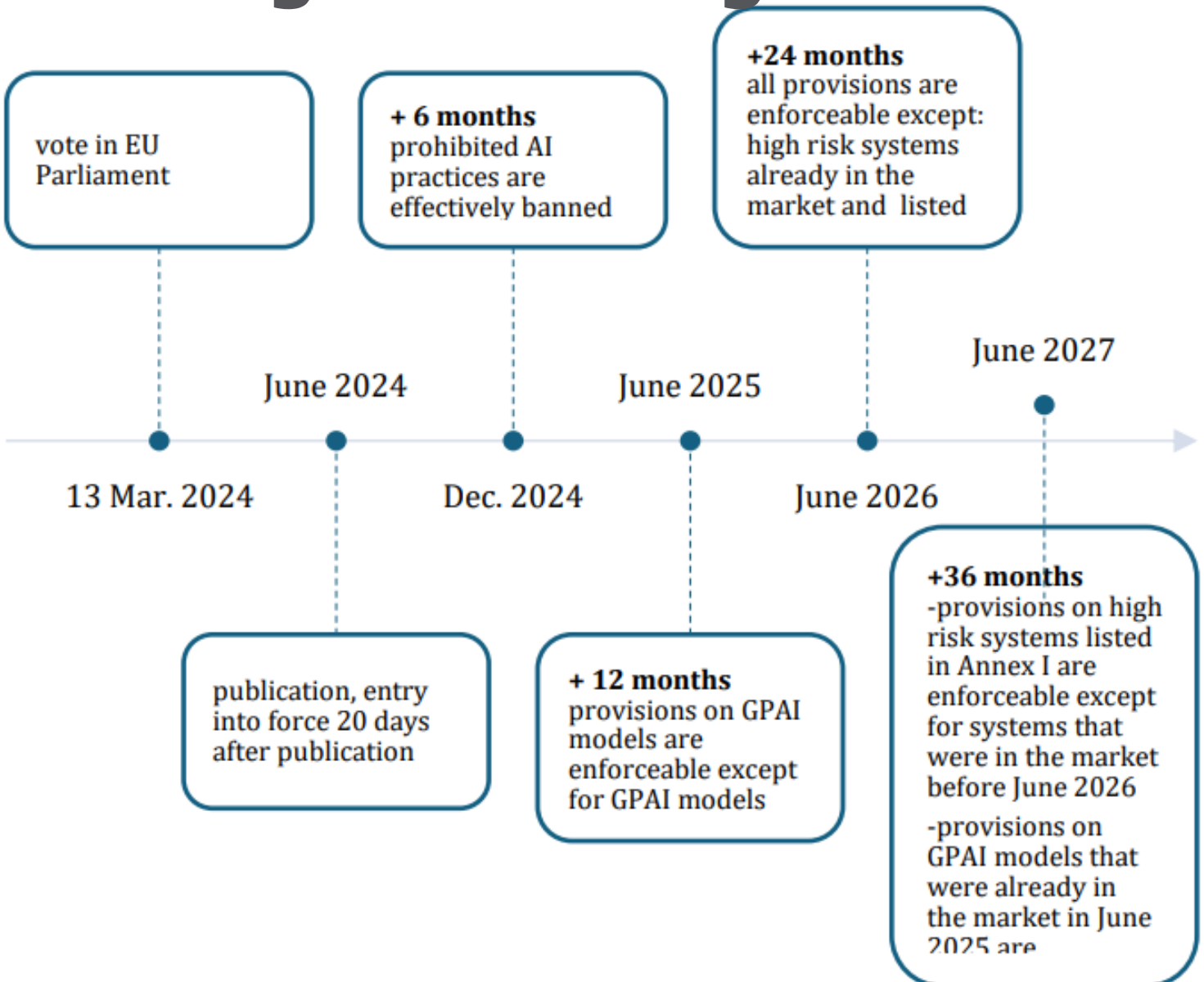
*I fornitori di MIAFG classificati 'a rischio sistemico' sono soggetti ad obblighi aggiuntivi (cf. DSA art. 34)*

- Valutazione dei modelli in conformità a protocolli e strumenti 'state-of-the-art'
- Valutazione di rischi e misure per mitigarli
- Record-keeping di incidenti ecc..
- Livello adeguato di cibersicurezza
- Documentazione aggiuntiva su architettura del sistema, procedure interne, ecc. ecc.




*Fonte:* G'sell, Florence, *An Overview of the European Union Framework Governing Generative AI Models and Systems* (May 20, 2024). Available at SSRN: https://ssrn.com/abstract=4762804

# Entrata in vigore e deroghe – art. 111-113



# Sanzioni – art. 99

| | |
|---|---|
| Non conformità al divieto di pratiche IA vietate | € 35M o 7% fatturato |
| Non conformità a obblighi di trasparenza | € 15M o 3% fatturato |
| Fornitura di informazioni inesatte, incomplete o fuorvianti | € 7.5M o 1% fatturato |