ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

Privacy & dintorni: evoluzione GDPR e relazioni con altre normative

Cesare De Santis

Roma 26/9/2025

Agenda

- Presentazione relatore
- Privacy e dintorni: evoluzione GDPR e relazioni con altre normative
- Bibliografia & sitografia
- Q&A

Agenda

- **Presentazione relatore**
- Privacy e dintorni: evoluzione GDPR e relazioni con altre normative
- Bibliografia & sitografia
- Q&A

Presentazione relatore

Cesare De Santis

Ho lavorato a lungo per Enti della P.A. (Difesa/Aeronautica) ed aziende private (banca e alcune società di consulenza di emanazione bancaria) prima di intraprendere, nel 2008, un autonomo percorso professionale.

Attualmente sono amministratore unico di PRIMAe srl a socio unico, che opera principalmente sui temi della conformità normativa e della protezione dei dati personali. Tra i clienti di PRIMAe srl a socio unico si annoverano banche, società finanziarie ed operanti nel campo assicurativo, altre società di consulenza. Assicuriamo il servizio DPO ad alcune banche, a società facenti parte di gruppo bancario e ad un fondo sanitario di emanazione bancaria..

Titoli/certificazioni/attestati

Laureato in Scienze statistiche ed attuariali, abilitato alla professione di attuario, CISM

Agenda

- Presentazione relatore
- **Privacy e dintorni: evoluzione GDPR e relazioni con altre normative**
- Bibliografia & sitografia
- Q&A

Evoluzione GDPR: contesto

La Commissione UE ha pubblicato il 21 maggio 2025 la proposta per l'adozione di un Regolamento per modificare alcune normative esistenti tra cui il GDPR.

La proposta fa parte di un processo di semplificazione normativa stimolato dal Rapporto Draghi secondo il quale la regolamentazione dell'UE impone un ***onere proporzionalmente maggiore*** *alle PMI e alle small mid-cap enterprises (SMC), imprese che hanno superato le soglie delle PMI, e che vengono individuate nelle*

> companies which, according to their last annual or consolidated accounts, meet at least two of the following three criteria: an average number of employees during the financial year of less than 750, a total balance sheet not exceeding EUR 129 000 000 and an annual net turnover not exceeding EUR 150 000 000;

rispetto alle imprese di maggiori dimensioni.

Evoluzione GDPR: contenuto

Per quanto riguarda il GDPR la proposta contiene l'inserimento all'interno dell'art. 4 del GDPR delle definizioni di "microimprese, piccole e medie imprese" e "imprese a media capitalizzazione di piccole dimensioni" e l'aggiunta del riferimento a queste ultime nell'art. 40 c. 1 (Codici di condotta) e nell'art. 42 c. 1 (Certificazioni) nonché ***una modifica all'esenzione dell'obbligo di tenuta del registro dei trattamenti, elevando il limite da 250 a 750 dipendenti (corrispondente al valore soglia delle imprese a media capitalizzazione) con esclusione dei trattamenti a rischio elevato****:*

«Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 750 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio elevato per i diritti e le libertà dell'interessato ai sensi dell'articolo 35.».

Evoluzione GDPR: chiarimenti e pareri

Sarà chiarito con un considerando che non saranno ritenuti di rischio elevato ai fini della tenuta del Registro i trattamenti di dati personali appartenenti a particolari categorie relativi all'art. 9 c. 2 lett. b) del GDPR (trattamento necessario per assolvere obblighi o esercitare diritti in materia di diritto del lavoro, della sicurezza sociale e protezione sociale ove autorizzati da una norma o da un contratto collettivo in presenza di garanzie appropriate).

Su tale proposta EDPB ed EDPS hanno rilasciato il proprio parere : " … Based on the information available, and subject to a full analysis of the specific proposal, the ***EDPB and EDPS can express preliminary support to this targeted simplification initiative****, bearing in mind that this would not affect the obligation of controllers and processors to comply with other GDPR obligations. …"*

Evoluzione Codice privacy: data breach

Il 4 agosto 2025 il Consiglio dei Ministri ha approvato un disegno di legge di semplificazione (Comunicato stampa del Consiglio dei Ministri n.138 | www.governo.it) che all'art. 19 riporta una semplificazione per le aziende con ***meno di cinque dipendenti relativamente alla comunicazioni di data breach:***

ART. 19

(Disposizioni in materia di microimprese)

1. Al decreto legislativo 30 giugno 2003, n. 196, dopo l'articolo 2-*quaterdecies* è inserito il seguente:

«*Articolo 2-quaterdecies.1*

(Procedura di notifica delle violazioni di dati personali da parte di microimprese)

1. Le imprese con meno di cinque dipendenti si avvalgono, per l'adempimento dell'obbligo di cui all'articolo 33 del Regolamento, di una specifica procedura di notifica.

2. La procedura di cui al comma 1 è disciplinata dal Garante con proprio provvedimento, prevedendo il ricorso a strumenti di autovalutazione guidata e un canale di assistenza semplificata che forniscano supporto ai soggetti tenuti alla notifica.».

2. Dall'attuazione della disposizione di cui al comma **1** non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. L'amministrazione competente provvede agli adempimenti previsti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Relazioni con altre normative (1): AI Act

- ✓ *L'intelligenza artificiale (IA) è una disciplina che studia sistemi capaci di imitare l'intelligenza umana. Nasce negli anni '50, ma si sviluppa fortemente con l'avvento dei computer moderni. Grazie ai big data e al machine learning, l'IA ha fatto grandi progressi. Le reti neurali permettono alle macchine di apprendere da esempi. Oggi l'IA è usata in medicina, finanza, trasporti e molti altri settori. È fondamentale nell'elaborazione del linguaggio e nella visione artificiale. Queste tecnologie rendono più naturale l'interazione uomo-macchina. L'IA solleva anche questioni etiche e sociali importanti. Cresce il dibattito sulla regolamentazione e sull'uso responsabile di essa. Il suo sviluppo promette cambiamenti profondi nella nostra società.*
- ✓ *(il testo che precede è stato prodotto istantaneamente da ChatGPT rispondendo alla richiesta «descrivi in 10 righe il fenomeno di sviluppo dell'intelligenza artificiale»)*
- ✓ *«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. [art. 3 c. 1 Regolamento UE 2024/1689 (AI Act)]*

AI: tipologie di sistemi AI per le banche

Chatbot bancari
Assistenti virtuali che gestiscono le richieste dei clienti 24/7 (es. saldo, bonifici, info su prodotti), riducendo i tempi di attesa e migliorando l'assistenza.
Sistemi di rilevamento frodi
Analizzano in tempo reale le transazioni per individuare comportamenti anomali e potenzialmente fraudolenti, bloccando attività sospette in automatico.
Sistemi di credit scoring intelligenti
Valutano l'affidabilità creditizia di un cliente usando molti dati (anche alternativi), permettendo decisioni di prestito più accurate e personalizzate.
Consulenti finanziari virtuali (robo-advisor)
Offrono consigli automatici su investimenti, piani di risparmio e gestione del portafoglio, in base al profilo e agli obiettivi dell'utente.
IA per la gestione dei rischi
Analizza grandi quantità di dati economici e finanziari per prevedere rischi di mercato, creditizi o operativi, supportando le decisioni strategiche.
Automazione dei processi (RPA + IA)
Automatizza attività ripetitive come l'apertura conti, verifica documenti o gestione reclami, migliorando efficienza e riducendo errori umani.
Analisi predittiva per il marketing
Prevede i bisogni dei clienti (es. mutui, carte di credito) e propone offerte mirate, aumentando la personalizzazione e il tasso di conversione.
Riconoscimento biometrico intelligente
Utilizza l'IA per riconoscere il volto, la voce o l'impronta digitale dei clienti, rendendo l'autenticazione più sicura e veloce.

AI: normativa di riferimento

Europea

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) Pubblicato in G.U. UE il 12 luglio 2024*

Italiana

Senato della Repubblica

Intelligenza artificiale

E' prevista in Aula oggi, 17 settembre, la discussione del ddl recante disposizioni e delega al Governo in materia di intelligenza artificiale (A.S. 1146-B), approvato dal Senato e modificato dalla Camera e collegato alla manovra. L'esame del ddl nelle Commissioni riunite 8a e 10a si è concluso nella seduta del 30 luglio con mandato ai relatori, sen. Rosa e Minasi, a riferirne all'Assemblea.

Dossier di documentazione

Art. 4 c. 2 L'utilizzo di sistemi di intelligenza artificiale garantisce il trattamento lecito, corretto e trasparente dei dati personali e la compatibilità con le finalità per le quali sono stati raccolti, in conformità al diritto dell'Unione europea in materia di dati personali e di tutela della riservatezza.

Art. 11 c. 2 L'utilizzo dell'intelligenza artificiale in ambito lavorativo deve essere sicuro, affidabile, trasparente e non può svolgersi in contrasto con la dignità umana né violare la riservatezza dei dati personali. Il datore di lavoro o il committente è tenuto a informare il lavoratore dell'utilizzo dell'intelligenza artificiale nei casi e con le modalità di cui all'articolo 1-bis del decreto legislativo 26 maggio 1997, n. 152.

AI Act: obiettivi

Il regolamento (UE) 2024/1689 mira a incoraggiare lo sviluppo e l'adozione di sistemi di intelligenza artificiale (IA) **sicuri** e **affidabili** in tutto il mercato unico dell'Unione europea (Unione) sia nel settore pubblico che in quello privato, garantendo al contempo la salute e la sicurezza dei cittadini dell'Unione e il rispetto dei **diritti fondamentali**. Il regolamento stabilisce norme basate sul rischio per quanto riguarda:

- l'immissione sul mercato, la messa in servizio e l'utilizzo di taluni sistemi IA;
- il divieto di determinate pratiche di IA;
- i requisiti e gli obblighi relativi ai sistemi di IA ad alto rischio;
- la trasparenza per taluni sistemi di IA;
- la trasparenza e la gestione dei rischi per i modelli di IA per finalità generali (modelli IA potenti che supportano i sistemi IA in grado di svolgere una vasta gamma di compiti);
- il monitoraggio del mercato, la vigilanza del mercato, la governance e l'esecuzione;
- il sostegno all'innovazione, concentrandosi sulle piccole e medie imprese (PMI) e sulle start-up.

Sono previste alcune esenzioni, come ad esempio per i sistemi utilizzati esclusivamente a fini **militari e di difesa** o a fini di **ricerca**.

*Tratto dal documento UE «*Regole per un'intelligenza artificiale affidabile nell'Unione europea»
(https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=LEGISSUM:4762484)

AI Act: quando si applicherà

La legge sull'IA si applicherà il **2 agosto 2026**, due anni dopo l'entrata in vigore, ad eccezione che per le seguenti disposizioni specifiche:

- ✓ **i divieti, le definizioni e le disposizioni relativi all'alfabetizzazione** in materia di IA (Capi I e II AI) si applicano 6 mesi dopo l'entrata in vigore, il **2 febbraio 2025**;
- ✓ le norme in materia di **governance e gli obblighi per l'IA per finalità generali (***Capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78)* diventano applicabili 12 mesi dopo l'entrata in vigore, il **2 agosto 2025**;
- ✓ gli **obblighi per i sistemi di IA ad alto rischio**, che si classificano come ad alto rischio perché integrati in prodotti regolamentati, elencati nell'allegato II (elenco della normativa di armonizzazione dell'Unione), si applicano 36 mesi dopo l'entrata in vigore, il **2 agosto 2027**.

(https://ec.europa.eu/commission/presscorner/detail/it/qanda_21_1683)

AI Act: le sanzioni

Gli Stati membri dovranno stabilire sanzioni effettive, proporzionate e dis*suasive in caso di violazione delle norme relative ai sistemi di IA.*

Il regolamento stabilisce le soglie da tenere in considerazione:

- ✓ **fino a 35 milioni di € o al 7%** del fatturato mondiale totale annuo dell'esercizio precedente (se superiore) per violazioni relative a **pratiche vietate o per l'inosservanza di requisiti** in materia di dati;
- ✓ **fino a 15 milioni di € o al 3%** del fatturato mondiale totale annuo dell'esercizio precedente per **l'inosservanza di qualsiasi altro requisito** o obbligo del regolamento;
- ✓ **fino a 7,5 milioni di € o all'1,5%** del fatturato mondiale totale annuo dell'esercizio precedente per la **fornitura di informazioni inesatte, incomplete o fuorvianti** agli organismi notificati e alle autorità nazionali competenti in risposta a una richiesta;
- ✓ per ciascuna categoria di violazione, la soglia per le PMI sarebbe l'importo più basso tra i due previsti, mentre per le altre imprese sarebbe l'importo più elevato.

La Commissione può inoltre applicare le norme sui fornitori di modelli di IA per finalità generali mediante sanzioni pecuniarie, tenendo in considerazione la seguente soglia:

- ✓ ***fino a 15 milioni di € o al 3%*** *del fatturato mondiale totale annuo dell'esercizio precedente per l'inosservanza di qualsiasi obbligo o misura richiesta dalla Commissione a norma del regolamento.*

Le istituzioni, le agenzie o gli organismi dell'UE sono chiamate a dare l'esempio e saranno quindi soggette anch'esse alla normativa e a eventuali sanzioni. Il Garante europeo della protezione dei dati avrà il potere di infliggere loro sanzioni pecuniarie in caso di non conformità

(https://ec.europa.eu/commission/presscorner/detail/it/qanda_21_1683)

AI Act: settori ad alto rischio

- **componenti di sicurezza** di prodotti disciplinati dalla normativa di armonizzazione dell'Unione (o in qualità di prodotti autonomi) che sono tenuti a sottoporsi a una valutazione di conformità di terze parti ai sensi della stessa normativa;
- **biometrica**, se usata per l'identificazione remota, per classificare le persone da attributi sensibili (come la razza o la religione), o per il riconoscimento delle emozioni, salvo quando utilizzata per verificarne semplicemente l'identità;
- **infrastrutture critiche**, quando l'IA è una componente di sicurezza in settori quali le infrastrutture digitali, il traffico, l'acqua, il gas, il riscaldamento e l'elettricità;
- **istruzione e formazione professionale**, compreso l'accesso alle questioni educative, la valutazione dei risultati dell'apprendimento, la valutazione dei livelli di istruzione o il monitoraggio del comportamento durante le prove;
- **occupazione**, comprese l'assunzione, la selezione dei candidati, l'adozione di decisioni in materia di condizioni di impiego (promozioni, cessazioni del rapporto di lavoro), l'assegnazione dei compiti o il monitoraggio delle prestazioni;
- **servizi essenziali**: sistemi di IA utilizzati dalle autorità pubbliche per valutare l'ammissibilità alle prestazioni e ai servizi di assistenza pubblica (compresi i servizi di assistenza sanitaria), il merito di credito, la valutazione del rischio di assicurazione e la priorità delle risposte di emergenza;
- **attività di contrasto**: sistemi di AI utilizzati per valutare i rischi di reato, poligrafi, valutare l'attendibilità delle prove, prevedere la recidività o la profilazione di persone per le indagini penali;
- **migrazione e controllo delle frontiere**: sistemi di AI utilizzati per valutare i rischi legati alla migrazione, alle domande di asilo e ai visti, o per individuare e identificare le persone in contesti migratori;
- **gestione della giustizia e dei processi democratici**: sistemi di IA utilizzati dalle autorità giudiziarie per la ricerca e l'interpretazione legale o sistemi che potrebbero influenzare i risultati delle elezioni.

*Tratto dal documento UE «*Regole per un'intelligenza artificiale affidabile nell'Unione europea» *(https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=LEGISSUM:4762484)*

I sistemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito, ***a eccezione dei sistemi di IA utilizzati allo scopo di individuare frodi finanziarie [all. III punto 5 lettera b) ad AI Act]***

AI Act: obblighi del *deployer*

- ✓ *«deployer»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un 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 (art. 3 c. 4 AI Act)*
- ✓ *L'art. 26 di AI Act disciplina gli obblighi del deployer (con particolare riguardo agli «istituti finanziari soggetti a requisiti in materia di governance, di dispositivi o di processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari «) tra cui:*
  - *monitoraggio del funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso, comunicando a fornitore ed Autorità l'esistenza di rischi di cui art. 79 c. 1 di AI Act (rischi per la salute o la sicurezza o per i diritti fondamentali delle persone) e incidenti gravi;*
  - *Conservazione dei log generati automaticamente da sistemi AI per periodo adeguato (6 mesi) salvo diversa indicazione normativa (**in particolare GDPR**);*
  - *«Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio.»;*
  - *«Se del caso, i deployer di sistemi di IA ad alto rischio usano le informazioni fornite a norma dell'articolo 13 (1) del presente regolamento per adempiere al loro obbligo di effettuare **una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del regolamento (UE) 2016/679**»*

(1) «I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso, in un formato appropriato digitale o non digitale, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per i deployer » (Art. 13 c. 2 AI Act)

AI Act: valutazione d'impatto

I deployer di sistemi di IA ad alto rischio destinati a essere utilizzati per valutare ***l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito****, effettuano una* ***valutazione dell'impatto sui diritti fondamentali*** *(Fundamental Right Impact Assessment, FRIA) che l'uso di tale sistema può produrre (art. 27 AI Act).*
Tale valutazione comprende:

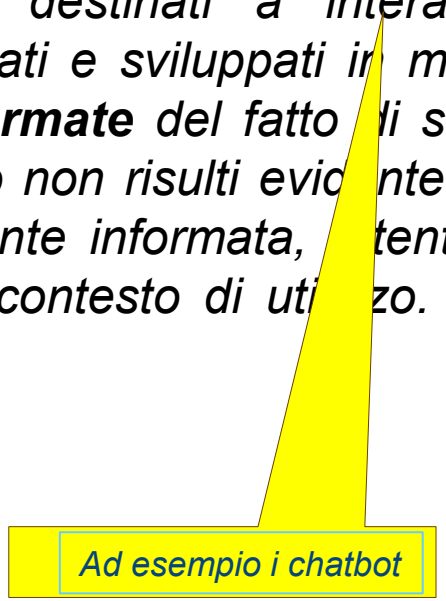
a) *una descrizione dei processi del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista;*
b) *una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza;*
c) *le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico;*
d) *i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13;*
e) *una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso;*
f) *le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.*

*«****Se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679*** *o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo integra tale valutazione d'impatto sulla protezione dei dati.» (art. 27 c. 4 AI Act)*

AI Act: trasparenza di determinati sistemi IA

Specifiche regole di trasparenza caratterizzano alcuni tipi di sistemi IA ad alto rischio tra cui:

*«I fornitori garantiscono che i sistemi di IA destinati a interagire **direttamente** con le persone fisiche sono progettati e sviluppati in modo tale che le persone fisiche interessate **siano informate** del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo. …» (Art. 50 c. 1 AI Act)*



AI Act: supervisione (sorveglianza) umana

*Il principio della human oversight, o **supervisione (sorveglianza) umana**, è una delle sette linee guida etiche per una IA affidabile sviluppate dal gruppo di esperti sull'IA designato dalla Commissione UE nel 2019; tale principio è oggetto di specifica disciplina, art. 14, nell'AI Act.*

*«I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, **in modo tale da poter essere efficacemente supervisionati da persone fisiche** durante il periodo in cui sono in uso» (art. 14 c. 1 AI Act).*

Il sistema di IA ad alto rischio è fornito al deployer in modo che le persone fisiche alle quali è affidata la supervisione abbiano la possibilità, ove opportuno e proporzionato, di (art. 14 c. 4 AI Act):

- ✓ *comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese;*
- ✓ *restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche;*
- ✓ *interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili;*
- ✓ *decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio;*
- ✓ *intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza.*

AI Act: suggerimenti per il prossimo futuro

- ✓ *Alfabetizzazione in materia di AI del personale;*
- ✓ ***Mappatura dei sistemi AI in essere** e delle interazioni esistenti tra essi e con le componenti del sistema informativo aziendale;*
- ✓ ***Verifica dell'impatto e della trasparenza** dei sistemi di AI utilizzati;*
- ✓ ***Policy sull'utilizzo della AI generativa** (responsabilità, proprietà industriale);*
- ✓ ***Modello AI Act***
  - *Policy;*
  - *Procedure;*
  - *Governance aziendale (es. costituzione Comitato AI con DPO, IT, U.O. di produzione, HR, CEO).*

Relazioni con altre normative (2): DSA e DMA

«Il Digital Services Act (DSA) è stato definito la nuova costituzione digitale dell'Unione europea, diretto a rafforzare i diritti e creare un ambiente online più sano, sicuro trasparente. Il Digital Markets Act (DMA) cerca di limitare il ruolo dominante dei padroni dei flussi informativi …»

[questo brano è tratto da «Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei» di L. Bolognini , E. Pelino e M. Scialdone (Giuffrè Francis Lefebvre 2023)]

Il regolamento sui servizi digitali (DSA) disciplina intermediari e piattaforme online come mercati online, social network, piattaforme per la condivisione di contenuti, app store e piattaforme online per viaggi e alloggi. L'obiettivo principale è prevenire le attività illegali e dannose online e la diffusione di notizie false. Garantisce la sicurezza degli utenti, protegge i diritti fondamentali e crea un contesto equo e aperto per le piattaforme. Il DSA è in vigore dal 16 novembre 2022 e pienamente applicabile dal 17 febbraio 2024.

Il regolamento sui mercati digitali (DMA) stabilisce una serie di criteri oggettivi e molto precisi per qualificare le piattaforme online di grandi dimensioni come «gatekeeper» e assicura che si comportino in modo equo online e lascino spazio alla contendibilità.
Il DMA è in vigore dal 1 novembre 2022 e pienamente applicabile dal 2 maggio 2023.
Il 6 settembre 2023 la Commissione europea ha designato per la prima volta sei gatekeeper: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, che offrono in totale 22 servizi di piattaforma essenziali.

DSA: sintesi

*Il **Digital Services Act (DSA)** ha l'obiettivo di creare uno spazio digitale più sicuro e responsabile. Si applica a tutte le piattaforme digitali che offrono servizi all'interno dell'UE, in particolare ai grandi intermediari online e alle piattaforme molto grandi (VLOP e VLOSE).*

Obiettivi principali

- ✓ *Garantire la sicurezza degli utenti online,*
- ✓ *Contrastare la disinformazione, l'odio e i contenuti illegali,*
- ✓ *Aumentare la trasparenza delle piattaforme digitali,*
- ✓ *Rafforzare la responsabilità delle piattaforme verso i contenuti ospitati,*
- ✓ *Proteggere i diritti fondamentali, come la libertà di espressione e la privacy.*

Prescrizioni chiave:

- ✓ *Obbligo di rimuovere tempestivamente contenuti illegali,*
- ✓ *Meccanismi trasparenti di segnalazione e ricorso per gli utenti,*
- ✓ *Valutazioni annuali dei rischi sistemici per le piattaforme molto grandi,*
- ✓ *Divieto di pubblicità mirata ai minori e basata su dati sensibili,*
- ✓ *Obbligo di trasparenza sugli algoritmi e i criteri di raccomandazione,*
- ✓ *Cooperazione rafforzata tra Stati membri e Commissione Europea.*

DSA: a chi si applica

Quali fornitori sono interessati?

Il regolamento sui servizi digitali contiene regole per i servizi di intermediazione online, che milioni di europei utilizzano quotidianamente. Gli obblighi dei diversi operatori online corrispondono al loro ruolo, alle loro dimensioni e al loro impatto sull'ecosistema digitale.

- Le **piattaforme online e i motori di ricerca di grandi dimensioni** comportano rischi particolari per la diffusione di contenuti illegali e i danni che possono arrecare alla società. Sono previste norme specifiche per le piattaforme che raggiungono più del 10% dei 450 milioni di consumatori europei.

  Accedi all'elenco delle piattaforme designate

- Le **piattaforme online** riuniscono venditori e consumatori, come mercati online, app store, piattaforme dell'economia collaborativa e piattaforme dei social media.
- I **servizi di hosting** includono i servizi cloud e di webhosting (anche piattaforme online).
- I **servizi di intermediazione** offrono infrastrutture di rete: fornitori di accesso a Internet e registrar di nomi di dominio (compresi i servizi di hosting).

Tutti gli intermediari online che prestano i loro servizi nel mercato unico, con sede o meno nell'UE, sono tenuti a rispettare le nuove norme. Le microimprese e le piccole imprese hanno obblighi proporzionati alla loro capacità e alle loro dimensioni, rimanendo nel contempo responsabili. Inoltre, anche se dovessero registrare una forte crescita, le microimprese e le piccole imprese potranno beneficiare di un'esenzione mirata da una serie di obblighi durante un periodo transitorio di 12 mesi.

Fonte: Commissione UE (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_it)

DSA: VLOP e VLOSE designati

Very Large Online Platforms:

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

Very Large Online Search Engines:

- Bing
- Google Search

DSA: servizio intermediario [art. 3 comma g) del DSA]

g) «servizio intermediario»: uno dei seguenti servizi della società dell'informazione:

i) un servizio di semplice trasporto (cosiddetto «mere conduit»), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio o nel fornire accesso a una rete di comunicazione;

ii) un servizio di memorizzazione temporanea (cosiddetto «caching»), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite dal destinatario del servizio, che comporta la memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficiente il successivo inoltro delle informazioni ad altri destinatari su loro richiesta;

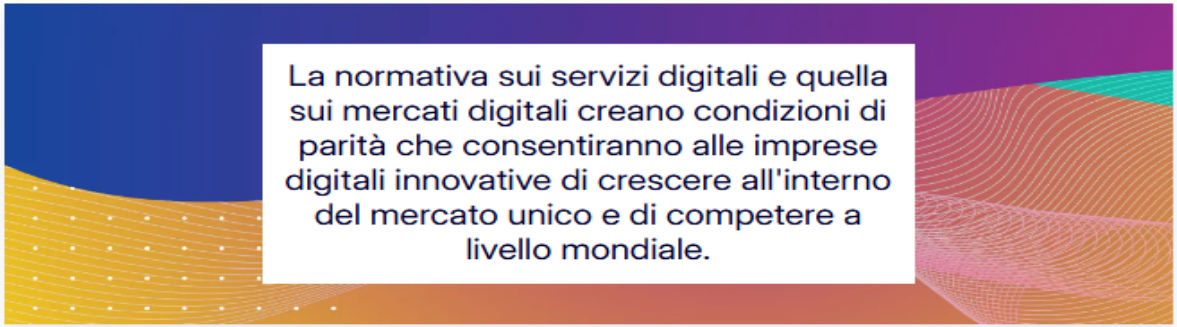
iii) un servizio di memorizzazione di informazioni (cosiddetto «hosting»), consistente nel memorizzare informazioni fornite da un destinatario del servizio su richiesta dello stesso;

DSA: obblighi per i prestatori di servizio intermediario

- ✓ **Obblighi generali di trasparenza**:
  - Fornire informazioni chiare nei termini di servizio, inclusi i criteri di moderazione dei contenuti.
  - Pubblicare rapporti periodici sulla moderazione dei contenuti (per hosting e piattaforme).
- ✓ **Obbligo di cooperazione con le autorità**:
  - Rispondere tempestivamente agli ordini delle autorità giudiziarie o amministrative per la rimozione di contenuti illegali o per l'accesso a dati.
- ✓ **Notifica e azione ("notice and action")** *(per hosting e piattaforme)*:
  - Stabilire meccanismi facilmente accessibili per segnalare contenuti illegali.
  - Agire rapidamente per rimuovere o disabilitare l'accesso ai contenuti segnalati.
- ✓ **Sistema di reclamo e ricorso** *(per piattaforme online)*:
  - Consentire agli utenti di contestare decisioni di rimozione/sospensione dei contenuti o dell'account.
- ✓ **Tracciabilità dei trader** *(per piattaforme che consentono transazioni commerciali)*:
  - Verificare l'identità dei venditori presenti sulla piattaforma (obbligo di due diligence).
- ✓ **Gestione dei rischi e auditing** *(solo per piattaforme molto grandi)*:
  - Valutazioni annuali dei rischi sistemici (es. disinformazione, manipolazione elettorale).
  - Adozione di misure di mitigazione e verifiche indipendenti.
- ✓ **Obblighi di design e pubblicità**:
  - Divieto di dark patterns (modelli di progettazione ingannevole)
  - Trasparenza sulla pubblicità e spiegazione degli algoritmi di raccomandazione.

DSA: cosa cambia per le aziende

Un'Europa pronta per l'era digitale: nuove norme online per le imprese



INDICE

Espansione delle piattaforme online innovative nell'UE
Attività lecite e fiorenti
Più responsabilità per le PMI e le start-up
Un mercato interno equo ed equilibrato
Maggiore certezza giuridica per le imprese
Mercati contendibili
Più posti di lavoro

Espansione delle piattaforme online innovative nell'UE

+ di 10 000
piattaforme operano nell'UE

Il 90%
di queste sono piccole e medie imprese

Nell'UE i servizi digitali devono attualmente osservare 27 diverse normative nazionali. Solo le imprese più grandi possono far fronte ai costi di conformità che ne derivano.

Cosa cambia con la nuova normativa sui servizi digitali

- Le stesse norme si applicheranno in tutta l'Unione e costituiranno la base di un vasto mercato interno che creerà le condizioni adatte per consentire ai servizi digitali di crescere e prosperare Si prevede che il commercio digitale transfrontaliero nel mercato unico aumenterà fino al 2%
- I piccoli operatori avranno la certezza giuridica di poter sviluppare i propri servizi e proteggere gli utenti dalle attività illecite e potranno contare sul sostegno di norme, codici di condotta e orientamenti
- Le piccole imprese e le microimprese sono esentate dagli obblighi più onerosi, ma libere di applicare le migliori pratiche per assicurare il proprio vantaggio competitivo
- Sostegno all'espansione (scale-up): le esenzioni per le piccole imprese saranno prorogate di 12 mesi dopo il superamento delle soglie relative al fatturato e al personale che le qualificano come piccole imprese

Fonte: Commissione UE (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_it)

DSA: sanzioni (art. 52 c. 3 del DSA)

3. Gli Stati membri provvedono affinché l'importo massimo delle sanzioni pecuniarie che possono essere irrogate in caso di inosservanza di un obbligo stabilito dal presente regolamento sia pari al 6 % del fatturato annuo mondiale del fornitore di servizi intermediari interessato nell'esercizio finanziario precedente. Gli Stati membri provvedono affinché l'importo massimo della sanzione pecuniarie che può essere irrogata in caso di comunicazione di informazioni inesatte, incomplete o fuorvianti, di mancata risposta o rettifica di informazioni inesatte, incomplete o fuorvianti e di inosservanza dell'obbligo di sottoporsi a un'ispezione sia pari all'1 % del reddito annuo o del fatturato mondiale del fornitore dei servizi intermediari o della persona interessati nell'esercizio finanziario precedente.

Per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi le sanzioni previste sono riportate all'art. 73 del DSA

EDPB ha pubblicato il 12 settembre 2025 «*Guidelines 3/2025 on the interplay between the DSA and the GDPR*», poste in consultazione pubblica fino al 31 ottobre 2025

Principali indicazioni:

- ✓ DSA e GDPR hanno obiettivi complementari;
- ✓ Il considerando 10 del DSA specifica che la protezione delle persone fisiche con riguardo al trattamento dei dati personali è disciplinata dalle norme del diritto dell'Unione in materia, in particolare il GDPR e la direttiva e-Privacy.
- ✓ Evidenziazione di problematiche specifiche di cui sono riportate le principali nelle slide che seguono (slide con LG in rosso nel titolo)

LG: indagini volontarie e conformità normativa per rimozione contenuti illegali

Le piattaforme adottano iniziative proprie, per individuare e rimuovere contenuti illegali, che comportano trattamenti a rischio alto (anche automatizzati con *machine learning*, massivi, rischio errori e *bias*). La base giuridica è l'interesse legittimo (obbligo LIA considerando ipotesi meno invasive, aspettativa interessati, minori) o l'obbligo di legge in caso di ordine di Autorità (il trattamento deve essere necessario, proporzionato, prevedibile dall'interessato e l'ingerenza limitata a quanto strettamente necessario).
Laddove non sia previsto intervento umano occorre considerare proibizione art. 22 GDPR (è necessario avvertire gli interessati ed è raccomandata la DPIA) .

LG: meccanismi di “notice and action” e sistemi interni di gestione dei reclami

DSA impone ai fornitori di servizi intermediari di predisporre meccanismi per la segnalazione di contenuti illegali (notice and action) e sistemi di gestione interna dei reclami. Questi meccanismi comportano inevitabilmente il trattamento di dati personali dei segnalatori, dei destinatari dei contenuti e di chi presenta reclami contro le decisioni prese. Tutti i trattamenti devono rispettare i principi del GDPR, garantendo trasparenza, necessità, proporzionalità e correttezza. L’identificazione del segnalatore deve avvenire solo quando strettamente indispensabile.

Indipendentemente dal fatto che l'azione intrapresa sia qualificabile come decisione automatizzata ai sensi dell'articolo 22 del GDPR, DSA prevede l'obbligo di fornire agli interessati (ossia ai destinatari interessati quando si tratta di persone fisiche) alcune informazioni specifiche, tra cui l'azione prevista, i fatti e le circostanze su cui si basa la decisione, l'uso di mezzi automatizzati nel prendere la decisione, ma anche se la decisione è stata presa in relazione a contenuti rilevati o identificati utilizzando mezzi automatizzati, sulla base giuridica su cui si è basata e sui motivi per cui le informazioni sono considerate contenuti illegali su tale base e sulle possibilità di ricorso a disposizione del destinatario del servizio in relazione alla decisione.

DSA (art. 25 c. 1) obbliga i fornitori di piattaforme online a progettare, organizzare e gestire le loro interfacce online in modo tale da non compromettere la capacità dei destinatari del servizio di prendere decisioni autonome e informate.
Ma ai sensi dell'art. 25 c. 2 DSA, il divieto di cui all'art. 25 c. 1 DSA non si applica alle pratiche disciplinate dal GDPR o dalla direttiva 2005/29/CE (direttiva sulle pratiche commerciali sleali, UCPD).
Per valutare se un modello ingannevole rientri anche nell'ambito di applicazione del GDPR occorre verificare se vi sia trattamento di dati personali e se il comportamento dell'utente che viene influenzato riguardi tale trattamento.
Schemi che cercano semplicemente di orientare tutti i destinatari di un servizio verso l'acquisto di un prodotto con tecniche di leva emotiva – come il messaggio "Sono rimasti solo pochi prodotti disponibili" – potrebbero non rientrare nel GDPR.
Diverso è il caso in cui l'utente sia spinto a fornire dati personali aggiuntivi che altrimenti non avrebbe comunicato, ad esempio: "Sono rimasti solo pochi prodotti disponibili. Inserisci subito il tuo indirizzo e-mail per prenotare".
In questo scenario, l'interfaccia manipolativa ricade sotto il GDPR, poiché induce un trattamento di dati personali non necessario e contrario ai principi di liceità e trasparenza sanciti dall'art. 5 GDPR.
Se il destinatario del servizio è una persona giuridica, ad esempio un utente commerciale, il GDPR non si applica, in quanto non verrebbero trattati dati personali relativi a una persona fisica. In ogni caso, l'art. 25 c.1 DSA si applica se il modello di progettazione ingannevole non è coperto dalla UCPD o dal GDPR.

LG: Trasparenza in pubblicità e divieto di annunci basati su profilazione dati particolari

L'articolo 26 DSA stabilisce norme di trasparenza per i fornitori di piattaforme online in materia di pubblicità e vieta ai fornitori di piattaforme online di presentare annunci pubblicitari ai destinatari sulla base della profilazione utilizzando categorie particolari di dati (art. 9 c. 1 GDPR). Il Considerando 68 DSA chiarisce che i requisiti di cui all'articolo 26 del DSA lasciano impregiudicato il GDPR, «*in particolare quelli relativi al diritto di opposizione, al processo decisionale automatizzato, compresa la profilazione, e in particolare alla necessità di ottenere il consenso dell'interessato prima del trattamento dei dati personali per la pubblicità mirata*». Esso non pregiudica inoltre le disposizioni della direttiva ePrivacy, «*in particolare quelle relative alla memorizzazione di informazioni nelle apparecchiature terminali e all'accesso alle informazioni ivi memorizzate*».
Le piattaforme devono informare gli utenti sui motivi per cui vedono un annuncio, sui principali parametri utilizzati per selezionarlo e sui modi per modificarli. Nel caso di pubblicità basata sulla profilazione gli utenti devono essere informati sulla logica della profilazione e sui loro diritti, incluso il diritto di opposizione. Le piattaforme devono anche assicurare che i dati raccolti per la trasparenza siano trattati in sicurezza e rispettando la riservatezza. Se la profilazione comporta decisioni automatizzate con effetti rilevanti sugli utenti, si applicano le protezioni previste dall'articolo 22 del GDPR.

Il "*sistema di raccomandazione*" definito dall'art. 3, lettera s), DSA è un sistema parzialmente o completamente automatizzato utilizzato dalle piattaforme online per presentare contenuti specifici agli utenti della piattaforma con un certo ordine o risalto relativo. Anche i motori di ricerca online possono utilizzare sistemi di raccomandazione quando propongono risultati di ricerca agli utenti.

Anche se tali sistemi potrebbero non trattare dati personali, gli scenari reali comportano sempre più spesso il trattamento automatizzato dei dati personali, con l'obiettivo di personalizzare e rendere più efficiente la presentazione dei contenuti, che possono presentare alcuni rischi che riguardano il trattamento di dati personali su larga scala, la potenziale mancanza di accuratezza e trasparenza per quanto riguarda le inferenze e la combinazione di dati personali, la valutazione o il punteggio (profilazione) e il trattamento di categorie particolari di dati o di natura altamente personale o relativi a soggetti vulnerabili.

Non si può poi che la presentazione di contenuti specifici agli utenti di una piattaforma online tramite un sistema di raccomandazione costituisca una «*decisione*» ai sensi dell'art. 22 c. 1 GDPR, ossia decisione che incide significativamente sull'interessato.

Oltre alla necessità di rispettare tutte le altre disposizioni pertinenti del GDPR, i fornitori devono garantire adeguati obblighi di trasparenza in relazione al trattamento dei dati personali nei loro sistemi di raccomandazione, anche offrendo la possibilità di modificare i principali parametri dei sistemi di raccomandazione. Ai sensi dell'art. 38 DSA, fornitori di VLOP e VLOE devono offrire almeno un'opzione per ciascuno dei loro sistemi di raccomandazione che non sia basata sulla profilazione come definita dal GDPR.

Uno degli obiettivi del DSA è la protezione online dei minori. In linea con tale obiettivo, l'art. 28 DSA prevede che «*i fornitori di piattaforme online accessibili ai minori adottino misure adeguate e proporzionate per garantire un elevato livello di privacy, sicurezza e protezione dei minori sui loro servizi*» ed inoltre, "*non devono presentare annunci pubblicitari sulla loro interfaccia basati sulla profilazione utilizzando i dati personali del destinatario del servizio quando sono ragionevolmente certi che il destinatario del servizio sia un minore*".
Nel DSA è precisato che i fornitori di piattaforme online non hanno l'obbligo di «*trattare ulteriori dati personali al fine di valutare se il destinatario del servizio sia un minore*».
Il trattamento di categorie particolari di dati, ad esempio i dati biometrici allo scopo di identificare in modo univoco una persona fisica, dovrebbe essere evitato, soprattutto quando si prevede il trattamento di dati relativi a minori.
Se la verifica dell'età risulta necessaria, il fornitore deve adottare un approccio basato sul rischio per garantire che i minori non possano accedere alla piattaforma e prevenire potenziali effetti negativi per tutti i destinatari del servizio, anche limitando il trattamento dei dati personali degli utenti a quanto necessario e proporzionato per stimare o verificare la loro età (ad esempio, se una fascia di età fornisce una ragionevole certezza che il destinatario del servizio è un minore, la data di nascita esatta non dovrebbe essere verificata) senza conservare in modo permanente l'età o la fascia di età del destinatario del servizio ma piuttosto limitarsi a registrare se il destinatario del servizio soddisfa le condizioni per l'utilizzo del servizio (minimizzazione dei dati).

Vedi la *Dichiarazione 1/2025 sulla garanzia dell'età adottata da EDPB l'11 febbraio 2025*

DMA: sintesi

*Il **Digital Markets Act (DMA)** è concepito per **garantire una concorrenza leale nel mercato digitale** e per limitare il potere delle grandi piattaforme online, dette «**gatekeeper»**.*

Si applica ai grandi operatori digitali che fungono da accesso obbligato tra utenti commerciali e consumatori.

Obiettivi principali del DMA:

- ✓ *Prevenire pratiche anticoncorrenziali da parte dei gatekeeper*
- ✓ *Garantire la libertà di scelta per imprese e utenti finali*
- ✓ *Favorire l'innovazione e l'ingresso di nuovi attori nel mercato*
- ✓ *Proteggere le imprese più piccole dall'abuso di posizione dominante*
- ✓ *Rafforzare il mercato unico digitale europeo.*

DMA: chi sono i «*gatekeeper*» (art. 3 del DMA)

Designazione dei gatekeeper

1. Un'impresa è designata come gatekeeper se:

a) ha un impatto significativo sul mercato interno;

b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e

c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro.

2. Si presume che un'impresa soddisfi i rispettivi requisiti di cui al paragrafo 1:

a) in relazione al paragrafo 1, lettera a), se raggiunge un fatturato annuo nell'Unione pari o superiore a 7,5 miliardi di EUR in ciascuno degli ultimi tre esercizi finanziari, o se la sua capitalizzazione di mercato media o il suo valore equo di mercato equivalente era quanto meno pari a 75 miliardi di EUR nell'ultimo esercizio finanziario, e se essa fornisce lo stesso servizio di piattaforma di base in almeno tre Stati membri;

b) in relazione al paragrafo 1, lettera b), se fornisce un servizio di piattaforma di base che, nell'ultimo esercizio finanziario, annovera almeno 45 milioni di utenti finali attivi su base mensile, stabiliti o situati nell'Unione, e almeno 10 000 utenti commerciali attivi su base annua stabiliti nell'Unione, identificati e calcolati conformemente alla metodologia e agli indicatori di cui all'allegato;

c) in relazione al paragrafo 1, lettera c), se le soglie di cui alla lettera b) del presente paragrafo sono state raggiunte in ciascuno degli ultimi tre esercizi finanziari.

3. Se raggiunge tutte le soglie di cui al paragrafo 2, l'impresa che fornisce servizi di piattaforma di base notifica tale informazione alla Commissione senza indugio e in ogni caso entro due mesi dal raggiungimento di tali soglie e fornisce alla Commissione le informazioni pertinenti di cui al paragrafo 2. Tale notifica comprende le informazioni pertinenti di cui al paragrafo 2 per ciascuno dei servizi di piattaforma di base dell'impresa che raggiunge le soglie di cui al paragrafo 2, lettera b). Ogniqualvolta un ulteriore servizio di piattaforma di base fornito dall'impresa precedentemente designata come gatekeeper raggiunge le soglie di cui al paragrafo 2, lettere b) e c), tale impresa ne dà notifica alla Commissione entro due mesi dal raggiungimento di tali soglie.

DMA: obblighi e divieti per i *gatekeeper*

Principali obblighi:

- ✓ *rendere i propri servizi interoperabili per i terzi in situazioni specifiche,*
- ✓ *consentire agli utenti commerciali di accedere ai dati che generano utilizzando la piattaforma,*
- ✓ *fornire alle imprese che fanno pubblicità sulla piattaforma gli strumenti e le informazioni necessarie per consentire agli inserzionisti e agli editori di effettuare verifiche indipendenti dei messaggi pubblicitari ospitati dalla piattaforma,*
- ✓ *consentire agli utenti commerciali di promuovere la loro offerta e concludere contratti con clienti al di fuori della piattaforma.*

e divieti :

- ✓ *riservare ai propri servizi e prodotti un trattamento favorevole in termini di classificazione rispetto a servizi o prodotti analoghi offerti da terzi sulla loro piattaforma,*
- ✓ *impedire ai consumatori di mettersi in contatto con le imprese al di fuori della piattaforma,*
- ✓ *impedire agli utenti di disinstallare applicazioni o software preinstallati, se lo desiderano,*
- ✓ *tenere traccia, per motivi pubblicitari, degli utenti finali al di fuori dei servizi essenziali della piattaforma, senza previo consenso dei diretti interessati.*

per i gatekeeper.

Fonte: Commissione UE
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_it

DMA: sanzioni

Articolo 30

Ammende

1. Nella decisione relativa all'inosservanza la Commissione può irrogare a un gatekeeper ammende il cui importo non supera il 10 % del fatturato totale di quest'ultimo realizzato a livello mondiale nel corso del precedente esercizio finanziario se constata che il gatekeeper, intenzionalmente o per negligenza, non rispetta:

a) ciascuno degli obblighi stabiliti agli articoli 5, 6 e 7;

b) le misure specificate dalla Commissione in una decisione adottata a norma dell'articolo 8, paragrafo 2;

c) i rimedi imposti a norma dell'articolo 18, paragrafo 1;

d) le misure provvisorie disposte a norma dell'articolo 24; o

e) gli impegni resi giuridicamente vincolanti a norma dell'articolo 25.

2. In deroga al paragrafo 1 del presente articolo, nella decisione relativa all'inosservanza la Commissione può imporre a un gatekeeper ammende fino al 20 % del fatturato totale di quest'ultimo realizzato a livello mondiale nel corso del precedente esercizio finanziario se constata che il gatekeeper ha commesso, in relazione allo stesso servizio di piattaforma di base, un'infrazione di un obbligo di cui all'articolo 5, 6 o 7 identica o simile a un'infrazione constatata in una decisione relativa all'inosservanza adottata negli otto anni precedenti.

DMA e GDPR

Alcuni punti di attenzione:

Consenso → rispetto delle caratteristiche[(1)] che deve avere il consenso soprattutto in relazione allo squilibrio di potere tra piattaforma e utente (oggi anche modello «*consent or pay*» di Facebook).

Correttivi DMA [alle pratiche di *nudging*[(2)]]:

- ✓ offrire una alternativa meno personalizzata ma equivalente e non subordinare al consenso uso del servizio della piattaforma principale
- ✓ presentare una soluzione user-friendly per fornire, modificare e revocare il consenso
- ✓ divieto di dark pattern

Portabilità → l'obiettivo perseguito è diverso: l'art. 20 GDPR mira a rafforzare il controllo dell'interessato sui suoi dati personali, mentre l'art. 6 c.9, del DMA è volto a garantire la contendibilità ed equità dei mercati nel settore digitale. Per tale ragione, il diritto alla portabilità del DMA si estende anche ai dati non personali e non si limita ai soli dati forniti dagli interessati o risultanti dall'osservazione delle loro attività ma riguarda anche i dati dedotti e derivati, ovvero i dati creati dallo stesso titolare del trattamento.

(1) *«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* (art. 4 c. 11 GDPR)

(2) *Il "nudging" (dall'inglese "nudge", che significa "spinta gentile" o "spintarella") è un concetto dell'economia comportamentale che consiste nell'incoraggiare le persone a prendere decisioni desiderate attraverso piccole "spinte gentili", senza limitare la loro libertà di scelta. Si tratta di un approccio che modifica l'ambiente decisionale per rendere più appetibile o semplice un certo comportamento, sfruttando la psicologia e influenzando le scelte in modo implicito ma efficace.*

Fine presentazione

Grazie...

(Nota bene: le due slide che seguono sono richiamate ipertestualmente all'interno della presentazione)

AI Act: pratiche vietate

- **tecniche subliminali o ingannevoli** per manipolare comportamenti individuali o di gruppo, compromettendone la capacità di prendere decisioni informate e potenzialmente provocando danni;
- **sfruttamento delle vulnerabilità** basate su età, disabilità o situazioni socioeconomiche per manipolare persone o gruppi, causando potenziali danni;
- assegnazione di un **punteggio sociale**, ossia una valutazione o una classificazione delle persone in base al comportamento o alle caratteristiche, che risulta in un trattamento iniquo, indipendentemente dal contesto in cui i dati sono stati raccolti, o sproporzionato rispetto alla gravità del comportamento;
- **valutazione del rischio penale**, che prevede la probabilità di commettere un reato sulla base unicamente di tratti comportamentali o di personalità, a eccezione di indagini penali obiettive;
- **riconoscimento facciale mediante scraping di banche di date** da Internet o videocamere di sicurezza senza target specifico;
- **inferire emozioni in settori sensibili**, come ad esempio nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne quando sia usato per motivi medici o di sicurezza;
- **categorizzazione biometrica** basata su dati per trarre deduzioni o inferenze in merito a razza, religione o opinioni politiche, tranne per l'uso legittimo nel settore delle attività di contrasto;
- **identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto**, a meno che non sia strettamente necessaria per la ricerca mirata di persone scomparse, la prevenzione di una minaccia specifica o l'identificazione di una persona sospettata di aver commesso un reato grave. Ciò deve seguire rigorose procedure giuridiche, compresa l'autorizzazione preventiva, un ambito di applicazione limitato e garanzie per proteggere i diritti e le libertà.

*Tratto dal documento UE «*Regole per un'intelligenza artificiale affidabile nell'Unione europea»
(https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=LEGISSUM:4762484)

AI Act: alfabetizzazione

«*I fornitori e i **deployer** dei sistemi di IA adottano misure per garantire nella misura del possibile un **livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto**, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati*» (Art. 4 «Alfabetizzazione in materia di IA» AI Act)

«***alfabetizzazione in materia di IA***»: *le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai deployer e alle persone interessate, tenendo conto dei loro rispettivi diritti e obblighi nel contesto del presente regolamento, di procedere a una diffusione informata dei sistemi di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa può causare (art. 3 c. 56 AI Act)*

Agenda

- Presentazione relatore
- Privacy & dintorni
- **Bibliografia & sitografia**
- Q&A

Bibliografia & Sitografia

AI:

- ✓ ***Ministero del Lavoro e delle Politiche sociali*** *ha pubblicato le «**Linee guida per l'implementazione dell'IA nel mondo del lavoro**»*
  https://www.lavorosi.it/notizie/min-lavoro-linee-guida-sull-intelligenza-artificiale-nel-mondo-del-lavoro-pubblicato-il-report/
- ✓ ***AGID*** *ha pubblicato le **«Linee guida per l'adozione di IA nella Pubblica Amministrazione**» (https://www.agid.gov.it/it/ambiti-intervento/intelligenza-artificiale)*
- ✓ ***EDPB*** *ha pubblicato (su richiesta della DPA croata) il documento **«AI Privacy Risks & Mitigations Large Language Models (LLMs)»***
  (https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-privacy-risks-mitigations-large_en)
  nel quale si propone una metodologia di gestione del rischio, includendo esempi pratici e casi d'uso, tra cui la chatbot per l'assistenza clienti
- ✓ *Uno studio legale svizzero ha pubblicato una interessante matrice che riporta gli **aspetti data protection per i più diffusi strumenti di AI** da utilizzare in azienda (2^ versione aggiornata all'11 marzo 2025)*
  (https://www.vischer.com/en/knowledge/blog/part-25-ai-tools-what-about-data-protection/)
- ✓ ***The Bridge Blueprint*** *- Interpretive Guidance for AI Deployment Aligning Data Protection and AI Regulation (Data Protection Authority di Amburgo)*
  (https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/EN-Bridge-Blueprint-v.0.9.pdf)

DSA e DMA:

- ✓ ***"Guidelines 3/2025 on the interplay between the DSA and the GDPR"*** *Version 1.0 - 11 September 2025 di EDPB (in **consultazione pubblica fino al 31 ottobre 2025**)*
- ✓ *«**Digital Services Act e Digital Markets Act – Definizioni e prime applicazioni dei nuovi regolamenti europei**» L. Bolognini E. Pelino M. Scialdone – Giuffrè Francis Lefebvre (Collana Tech e-Law) 2023*

Agenda

- Presentazione relatore
- Privacy & dintorni
- Bibliografia & sitografia
- **Q&A**

Q&A

Contatti

- cesare.desantis@primaedintorni.it

Grazie...