

Modulo 3

AI Generativa – L. 132/2025 – Tutela della privacy



Avv. Giovanni Battista Gallus
gallus@array.law | GDL FIIF – CNF

Ricognizione biometrica in ambito penale: il quadro normativo

Ricognizione biometrica in ambito penale: il quadro normativo

Art. 5(1)(h) e Art. 26(10) AI Act — Dir. 2016/680 — CDFUE artt. 7-8

RBI IN TEMPO REALE — Art. 5(1)(h) AI Act

PRINCIPIO: Vietata per le attività di contrasto, salvo eccezioni tassative

ECCEZIONI (esaustive, art. 5 §1 h, i-iii):

- (i) Ricerca di vittime di reati/scomparsi (inclusi minori)
- (ii) Prevenzione minaccia imminente terrorismo/incolumità fisica
- (iii) Localizzazione sospettato per reati All. II (≥4 anni detentivi)

CONDIZIONI CUMULATIVE:

- Autorizzazione preventiva da giudice o org. amm. indipendente
- FRIA completata (art. 27 AI Act) | Reg. banca dati UE (art. 49)
- In urgenza: uso consentito a condizione che tale registrazione sia completata senza indebito ritardo.
- Se rifiutata: cessazione immediata + cancellazione dati

RBI POST-FACTUM — Art. 26(10) AI Act

Non vietato, ma classificato come sistema ad alto rischio (All. III §1)

AUTORIZZAZIONE:

- Autorizzazione giudiziaria ex ante
- In urgenza: convalida entro 48h
- Eccezione: quando è utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato

TRE DIVIETI ASSOLUTI (art. 26 §10 e 5 §1 e):

- Sorveglianza indiscriminata di persone non sospettate
- No a decisioni legali basate esclusivamente sull'output biometrico
- Creazione di banche dati tramite scraping (art. 5 §1 e)

Ex ante vs. ex post: confronto per il penalista

Il regime autorizzativo determina le garanzie dell'indagato e le leve difensive

	 IN TEMPO REALE (ex ante)	 A POSTERIORI (ex post)
Qualificazione AI Act	Pratica vietata con eccezioni tassative (art. 5 §1 h)	Sistema ad alto rischio, Allegato III §1 (non vietato)
Autorizzazione	Preventiva da giudice o organo amm. indipendente. In urgenza: entro 24h	Preventiva da autorità giudiziaria. In urgenza: entro 48h
Limiti operativi	Temporalmente e geograficamente definiti. Solo nelle eccezioni tassative (i-iii)	Solo su immagini/registrazioni già acquisite, non in tempo reale
FRIA obbligatoria	Sì — art. 27 AI Act, prima dell'uso	Sì — parte della valutazione conformità sistema ad alto rischio
Sanzione se violato	Art. 99.3: fino a €35M o 7% fatturato.	Art. 99.4: fino a €15M o 3% fatturato.
Conseguenze processuali?	Violazione = pratica vietata → possibile inutilizzabilità art. 191 c.p.p.?	Violazione o mancanza di autorizzazione → quali conseguenze?

CGUE Grande Sezione, 4 ottobre 2024 — Causa C-548/21

Il principio di controllo indipendente sull'accesso ai dati nei dispositivi elettronici – un precedente utile?

FATTO: In un'indagine penale austriaca la polizia accede ai dati contenuti in un telefono cellulare senza autorizzazione giudiziaria preventiva. La Corte Costituzionale austriaca rimette alla CGUE la questione di compatibilità con la Direttiva 2016/680 (trattamento dati personali per fini di contrasto). CGUE si pronuncia in Grande Sezione.

§ 102

Controllo preventivo obbligatorio

Qualora l'accesso comporti il rischio di un'ingerenza grave nei diritti fondamentali, esso deve essere subordinato a un controllo preventivo effettuato da un giudice o da un organo amministrativo indipendente.

§ 104

Tempestività del controllo

Il controllo deve avere luogo prima di qualsiasi tentativo di accesso ai dati. È fatta salva l'urgenza, ma il controllo indipendente deve intervenire entro un breve termine successivo.

§ 103

Equilibrio tra indagine e diritti

Il controllo deve bilanciare le esigenze dell'indagine penale con il rispetto del diritto alla vita privata e alla protezione dei dati personali garantiti dagli artt. 7 e 8 CDFUE.

§ 110

Condizioni per la normativa nazionale

L'art. 4(1)(c) Dir. 2016/680 non osta a normative nazionali che consentano l'accesso purché: definiscano con precisione i reati rilevanti, garantiscano proporzionalità, subordinino l'accesso a controllo preventivo indipendente (salvo urgenza motivata).

IA generativa e modelli general purpose

Art. 50–56 Reg. (UE) 2024/1689

Art. 50 AI Act — Obblighi di trasparenza: schema

Chi	Obbligo	Quando si applica
Fornitore	Informare l'utente che sta interagendo con un sistema IA (chatbot ecc.)	Sempre, salvo eccezioni per forze dell'ordine
Fornitore	Marcare gli output sintetici in formato leggibile meccanicamente (watermarking)	Output audio/immagine/video/testo generati artificialmente
Deployer	Informare le persone esposte a sistemi di riconoscimento emozioni o categorizzazione biometrica	Al momento della prima interazione
Deployer	Dichiarare che il contenuto è un deep fake	Immagini/audio/video manipolati o generati che imitano persone reali
Deployer	Dichiarare che il testo su questioni di interesse pubblico è generato da IA	Tranne se sottoposto a revisione editoriale umana

Cosa sono i modelli GPAI? — Definizioni operative

	GPAI Model (art. 3, n. 63)	GPAI System (art. 3, n. 66)
Definizione	Modello addestrato su grandi quantità di dati in auto-supervisione, capace di svolgere un'ampia gamma di compiti distinti, anche se integrato in altri sistemi	Sistema IA basato su un modello GPAI, in grado di servire varie finalità direttamente o come componente di altri sistemi
Soglia rilevanza	$\geq 10^{25}$ FLOP di calcolo → possibile rischio sistemico (art. 51). Soglia indicativa per generalità significativa: ≥ 1 miliardo di parametri (cons. 98)	L'UI o l'integrazione che rende il modello accessibile (es. ChatGPT, Copilot, Gemini). Il sistema eredita gli obblighi del modello + obblighi propri
Esempi	GPT-4 (OpenAI), Gemini Ultra (Google), Claude 3 Opus (Anthropic), Llama 3 (Meta), Mistral Large	ChatGPT, Microsoft 365 Copilot, Google Workspace + Gemini, assistenti virtuali aziendali basati su LLM
Chi è provider	Chi sviluppa o mette sul mercato il modello (incluse imprese extra-UE che lo rendono accessibile nell'Unione)	Chi integra il modello in un sistema e lo distribuisce. ⚠ Il deployer che modifica sostanzialmente un modello può diventare provider (art. 25 AI Act)

IA Generativa: definizione operativa per l'avvocato

Cosa fa l'IA generativa

- Genera testo, immagini, audio, video e codice a partire da istruzioni (prompt)
- Funziona per probabilità statistiche, non per comprensione semantica
- Esempi: ChatGPT (OpenAI), Gemini (Google), Claude (Anthropic), Copilot (Microsoft)
- Non è un motore di ricerca

Rilevanza per l'avvocato

- Già usata negli studi legali per bozze di atti, ricerche, contratti
- Il cliente la usa: l'avvocato deve saper valutare l'output
- Il fornitore del servizio legale che la usa è potenzialmente un deployer AI Act
- Rischi deontologici: verifica dell'output, riservatezza dei dati, onestà verso il cliente

Il Regime dei Modelli GPAI — Artt. 51–56 AI Act

Obblighi per tutti i fornitori GPAI (art. 53)

- **Chi è fornitore GPAI?**
- Chi sviluppa o mette sul mercato nell'UE un modello GPAI, incluse imprese extra-UE
- La catena si estende ai fornitori che integrano il modello a valle
- **Obblighi art. 53:**
- Documentazione tecnica aggiornata (Allegato XI)
- Informazioni ai fornitori downstream (Allegato XII)
- Policy di rispetto del diritto d'autore UE (art. 53, § 1, lett. c)
- Sommario pubblico dei dati di addestramento (art. 53, § 1, lett. d)
- **Esenzione open source (art. 53, § 2):**
- Parziale per modelli con pesi rilasciati sotto licenza aperta, salvo rischio sistemico

Obblighi aggiuntivi — Rischio sistemico (art. 55)

Soglia: $\geq 10^{25}$ FLOP o impatto equivalente notificato all'AI Office (art. 51)

- Valutazione del modello prima del rilascio
- Red-teaming e test avversariali (adversarial testing)
- Notifica all'AI Office di incidenti gravi
- Misure di cybersicurezza adeguate
- Rapporto annuale sull'energia consumata
- **Codici di buone pratiche (art. 56):**
- Via principale di compliance per i GPAI
- Il rispetto del codice crea presunzione di conformità
- Elaborati da fornitori/stakeholder su impulso AI Office

Trasparenza e Copyright: Art. 53 AI Act + Dir. DSM + L. 132/2025

Art. 53, § 1, lett. c): il fornitore GPAI deve adottare una policy per rispettare il diritto d'autore UE, in particolare la Direttiva 2019/790 (DSM), incluso il rispetto della riserva di diritti (robots.txt / opt-out esplicito)

Fonte	Regola	Ruolo dell'avvocato
Text & Data Mining (art. 4 Dir. DSM 2019/790)	Eccezione TDM obbligatoria per ricerca scientifica. Per usi commerciali: il rightholder può fare opt-out con riserva espressa (es. robots.txt, metadati).	Verificare le clausole di licenza dei modelli usati dal cliente. Esaminare i contratti API per le clausole di indennizzo copyright.
AI Act art. 53, § 1, lett. d)	Sommario pubblico dei dati di training — obbligatorio, non necessariamente esaustivo. Funzione: consentire ai titolari di diritti di verificare l'uso.	Chiedere il sommario al fornitore in sede di procurement. Valutare se il dataset comprende opere del cliente.
L. 132/2025, art. 25 (nuovo art. 70-septies L. 633/1941)	Il TDM per sistemi IA è consentito nei limiti degli artt. 70-ter e 70-quater L. 633/1941. Le opere devono essere legittimamente accessibili.	Per clienti che addestrono modelli: audit del dataset. Per clienti titolari di diritti: verificare opt-out nei contratti di licenza e nei robots.txt.
Autorialità degli output IA (L. 132/2025, art. 25 + art. 1 L. 633/1941)	L'opera è tutelata solo se frutto dell'ingegno "umano". Output puro di IA senza apporto creativo umano: non tutelabile. Con editing umano sostanziale: tutelabile.	Questione aperta: confine tra editing e mera selezione del prompt.

Checklist «GenAI Deployer» — 7 controlli prioritari per lo studio o l'impresa

1. DISCLOSURE CHATBOT	Inserire notice visibile (non nelle FAQ) prima della prima interazione: «Stai interagendo con un sistema IA» (art. 50(1) AI Act)
2. POLICY INTERNA	Definire casi d'uso consentiti, categorie di dati ammesse nel prompt, escalation a un responsabile umano
3. PROMPT HYGIENE	Minimizzazione: no dati identificativi dei clienti nel prompt. Pseudonimizzazione prima dell'input. Limitare plugin/connector al necessario
4. VENDOR CHECK	Verificare: retention dei prompt/output; reuse per training; subfornitori; localizzazione dei dati; clausole DPA art. 28 GDPR + clausole AI Act
5. LOGGING E ACCESSI	Log delle interazioni con principio need-to-know; retention minima; procedure di accesso e cancellazione
6. FORMAZIONE	per tutti gli utenti: cosa può fare l'IA, cosa non fare, come segnalare anomalie

PARTE II

La L. 132/2025

Il recepimento italiano dell'AI Act (esclusi artt. 13,15)

Struttura della L. 132/2025 — Sei Capi, 28 Articoli

Art. 3, c. 5 — clausola-chiave: «La presente legge non produce nuovi obblighi rispetto a quelli previsti dal regolamento (UE) 2024/1689». Interpretazione e applicazione conformi all'AI Act (art. 1, c. 2).


Capo	Articoli	Contenuto	In questo modulo?
Capo I	Artt. 1-6	Principi e finalità: dimensione antropocentrica, trasparenza, sicurezza, non discriminazione, cybersicurezza, esclusioni sicurezza nazionale	✓ Sì
Capo II	Artt. 7-12	Disposizioni di settore: sanità, ricerca, trattamento dati, FSE, lavoro, Osservatorio lavoro	✓ Sì (escluso art. 13)
Capo II	Artt. 13-15	Professioni intellettuali (art. 13), PA (art. 14), Giustizia (art. 15)	⚠ Artt. 13 e 15: Avv. Santinon. Art. 14: ✓ qui
Capo III	Artt. 16-24	Strategia nazionale, autorità (AgID/ACN), deleghe al Governo, investimenti	✓ Sì
Capo IV	Art. 25	Diritto d'autore e TDM — modifica L. 633/1941 (nuovo art. 70-septies)	✓ Sì
Capo V	Art. 26	Disposizioni penali: aggravante art. 61 n. 11-undecies c.p.; art. 612-quater c.p. (deepfake); sanzioni finanziarie	✓ Sì
Capo VI	Artt. 27-28	Clausola invarianza finanziaria; disposizioni finali	✓ Sì

I principi generali — Artt. 1 e 3 L. 132/2025

Art. 1 — Finalità e ambito di applicazione

- Promuove uso corretto, trasparente e responsabile dell'IA
- Dimensione antropocentrica: opportunità + vigilanza sui rischi
- Garantisce vigilanza sui rischi economici/sociali e sull'impatto sui diritti fondamentali
- Interpretazione conforme al Reg. (UE) 2024/1689 (c. 2)

Art. 3 — Principi generali (7 commi)

- C. 1: rispetto diritti fondamentali, trasparenza, proporzionalità, sicurezza, dati personali, non discriminazione, parità di sessi, sostenibilità
- C. 3: rispetto autonomia/potere decisionale dell'uomo + sorveglianza e intervento umano
- C. 5:  nessun nuovo obbligo rispetto all'AI Act
- C. 6: cybersicurezza lungo l'intero ciclo di vita — approccio proporzionale al rischio
- C. 7: accesso pieno per persone con disabilità (Conv. ONU New York 2006)

Artt. 4 e 5 L. 132/2025 — dati personali, informazione e sviluppo economico

Art. 4 — Informazione e riservatezza dati personali

C. 1: uso IA nell'informazione senza pregiudizio a libertà e pluralismo dei media

C. 2: trattamento lecito, corretto e trasparente dei dati personali, conforme al GDPR

C. 3: informazioni rese con linguaggio chiaro e semplice — conoscibilità dei rischi

C. 4:


- Minori < 14 anni: accesso IA richiede consenso del genitore
- Minori 14-18 anni: consenso autonomo del minore se l'informativa è accessibile e comprensibile

Art. 5 — Principi in materia di sviluppo economico

Stato e PA promuovono IA per produttività e competitività

Art. 5, c. 1, lett. d): e-procurement PA — possono essere privilegiate soluzioni che localizzano dati strategici in data center italiani con disaster recovery in Italia

Favoriscono ricerca collaborativa imprese/enti/centri di trasferimento tecnologico

 Clausola lett. d) non è un obbligo assoluto: è un criterio di indirizzo per capitolati e prassi di acquisto pubblico

Art. 6 — sicurezza e difesa nazionale: esclusione dall'ambito

Art. 6, c. 1 — Sono escluse dall'ambito applicativo della L. 132/2025 le attività svolte per scopi di sicurezza nazionale (L. 124/2007), cybersicurezza/resilienza (D.L. 82/2021-ACN), difesa nazionale (Forze armate) e attività di polizia dirette a prevenire reati contro la sicurezza nazionale.

Soggetti esclusi

- Organismi intelligence (artt. 4, 6, 7 L. 124/2007)
- ACN per cybersicurezza (D.L. 82/2021, art. 1, c. 1, lett. a) e b))
- Forze armate per difesa nazionale
- Forze di polizia per prevenire reati contro la sicurezza nazionale (art. 9, c. 1, lett. b) e b-ter) L. 146/2006)

Limiti dell'esclusione

- Anche le attività escluse devono rispettare i diritti fondamentali e le libertà costituzionali
- Devono rispettare l'art. 3, c. 4 L. 132/2025 (tutela del dibattito democratico)
- La disciplina specifica viene adottata con regolamento ex art. 43 L. 124/2007 (intelligence) o modalità ACN

Regime dati personali

- Intelligence: si applica art. 58, cc. 1 e 3 Codice Privacy (D.Lgs. 196/2003)
- ACN: si applica art. 13 D.L. 82/2021
- Esclusione dall'AI Act: cfr. art. 2, c. 3 Reg. (UE) 2024/1689 per attività sicurezza nazionale

Capo II — disposizioni di settore: sanità, lavoro, PA

Articolo	Materia	Regola chiave	Rilevanza pratica
Art. 7	Sanità e disabilità	IA = supporto; decisione sempre rimessa al medico (c. 5). No discriminazione nell'accesso alle prestazioni. Interessato: diritto all'informazione sull'uso dell'IA (c. 3). Sistemi verificati e aggiornati periodicamente (c. 6).	Responsabilità medica non delegabile. IA non è autonoma nel ciclo di cura.
Art. 8	Ricerca scientifica IA in sanità	Trattamenti dati per ricerca IA sanitaria dichiarati di rilevante interesse pubblico. Uso secondario di dati privi di identificativi diretti (anche art. 9 GDPR) sempre autorizzato. Comunicazione preventiva al Garante; avvio dopo 30 gg se no blocco (c. 5).	Base giuridica: art. 9, c. 2, lett. g) GDPR. AGENAS: linee guida su anonimizzazione (c. 4).
Art. 9	Trattamento dati personali (ricerca/sperimentazione IA)	Disciplina semplificata per ricerca/sperimentazione con IA (anche dati particolari art. 9 GDPR) rimessa a D.M. Salute entro 120 gg dall'entrata in vigore, sentiti Garante, enti di ricerca, presidi sanitari.	Decreto ancora non adottato. Fino ad allora si applicano le regole ordinarie GDPR.
Art. 10	FSE e sanità digitale	Inserisce art. 12-bis nel D.L. 179/2012: disciplina soluzioni IA a supporto del FSE. Piattaforma IA sanità affidata ad AGENAS (titolare del trattamento). Dati: strettamente necessari. Misure tecniche/organizzative definite da AGENAS previo parere Garante e ACN.	AGENAS = titolare trattamento. Provvedimento AGENAS specificherà tipi dati e misure di sicurezza.

Capo II — disposizioni di settore: sanità, lavoro, PA

Articolo	Materia	Regola chiave	Rilevanza pratica
Art. 11	Lavoro	IA per miglioramento condizioni di lavoro: sicura, affidabile, trasparente, senza contrasto con dignità umana né violazione riservatezza. Informativa al lavoratore ex art. 1-bis D.Lgs. 152/1997 (aggiornato). No discriminazione per sesso, età, etnia, religione, orientamento sessuale (c. 3).	Informativa preventiva obbligatoria. Rinvio a D.Lgs. 152/1997 (art. 1-bis), non a norma autonoma della L. 132/2025.
Art. 12	Osservatorio lavoro e IA	Istituito presso Min. Lavoro: monitora impatto IA sul mercato del lavoro, identifica settori a rischio, promuove formazione. Componenti e modalità: D.M. entro 90 gg. Senza compensi.	Organismo di indirizzo e monitoraggio, non di vigilanza operativa. Funzione prevalentemente strategica.
Art. 14	Pubblica Amministrazione	IA in PA: solo in funzione strumentale e di supporto. L'unica responsabile dei provvedimenti è sempre la persona fisica. PA adottano misure tecnico-organizzative-formative per uso responsabile dell'IA.	No decisione amministrativa integralmente automatizzata senza responsabilità umana (ribadisce art. 22 GDPR nel contesto PA). Formazione obbligatoria per i dipendenti.

Capo III — Strategia Nazionale e Autorità (Artt. 19–20)

Art. 19 — Strategia nazionale IA

- Predisposta dalla struttura PCM per innovazione/digitale, d'intesa con AgID e ACN
- • Coordina PA, promuove ricerca, indirizza misure e incentivi
- Tiene conto dei principi di diritto internazionale umanitario
- Monitoraggio annuale trasmesso alle Camere

Comitato di coordinamento (c. 6):

Presieduto dal PCM, composto da MEF, MIMIT, MUR, Salute, PA, Difesa, Digitale. Coordina enti/organismi/fondazioni che operano nel campo dell'innovazione IA.

Art. 20 — Autorità nazionali per l'IA

AgID:

- Autorità di notifica (art. 70 AI Act)
- Promozione e sviluppo IA
- Accreditamento organismi di conformità

ACN:

- Vigilanza, ispezioni e sanzioni sui sistemi IA
- Punto di contatto unico con le istituzioni UE
- Profili cybersicurezza IA

Banca d'Italia, CONSOB, IVASS:

Autorità di vigilanza mercato ex art. 74, c. 6 AI Act

Restano ferme competenze Garante Privacy e AGCOM (DSA)

Capo III — Deleghe al Governo: Artt. 16, 17, 24

Art. 16 — Delega su dati e training

Delega al Governo (12 mesi) per disciplina organica su uso di dati, algoritmi e metodi matematici per addestramento di sistemi IA.

Principi: regime giuridico uso dati/algoritmi per training; strumenti tutela (risarcitori/inibitori); attribuzione controversie alle Sezioni specializzate impresa (lett. c).

Art. 17 — Modifica art. 9 c.p.c. (Sezioni Impresa)

Inserisce le cause aventi ad oggetto «il funzionamento di un sistema di intelligenza artificiale» tra le materie del Tribunale delle Imprese (aggiunta all'art. 9, c. 2 c.p.c. dopo «esecuzione forzata»).

Art. 24 — Delega adeguamento normativa nazionale all'AI Act

Delega al Governo (12 mesi) per adeguare la normativa nazionale al Reg. (UE) 2024/1689:

- Attribuzione a AgID/ACN di tutti i poteri di vigilanza, ispezione e sanzione previsti dall'AI Act
- Modifiche normativa di settore (banche, assicurazioni, intermediazione finanziaria)
- Quadro sanzionatorio ex art. 99 AI Act
- Percorsi di alfabetizzazione e formazione per ordini professionali e associazioni di categoria (c. 2, lett. f) — con possibile equo compenso modulato su responsabilità/rischi IA
- Potenziamento STEM nei curricula scolastici (lett. g); disciplina IA per attività di polizia (lett. h)

Art. 26 L. 132/2025 — Disposizioni penali (1/2): Aggravante e Art. 294 c.p.

Art. 26 introduce vari interventi penali: (1) nuova aggravante generale; (2) fattispecie aggravata art. 294 c.p.; (3) nuovo art. 612-quater c.p. (deepfake); (4) modifiche c.c., T.U.F. e diritto d'autore.

Art. 61, n. 11-undecies c.p. — Nuova aggravante generale (portata generale)

Aggiunta dopo il n. 11-decies . Testo: «l'aver commesso il fatto mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato».

Applicazione: qualsiasi reato commesso con IA come mezzo insidioso o che abbia ostacolato la difesa o aggravato le conseguenze. NON è circostanza speciale: ha portata generale.

Art. 294 c.p. — Attentato Attentati contro i diritti politici del cittadino. (comma aggiunto)

Aggiunto in fine: «La pena è della reclusione da due a sei anni se l'inganno è posto in essere mediante l'impiego di sistemi di intelligenza artificiale». Fattispecie base: attentato contro i diritti politici mediante violenza, minaccia o inganno. IA come strumento dell'inganno = fattispecie aggravata.

Art. 26 L. 132/2025 — Disposizioni penali (2/2): Deepfake e sanzioni finanziarie

Art. 612-quater c.p. — Illecita diffusione deepfake (nuovo articolo)

Inserito dopo art. 612-ter c.p. (revenge porn).

Fatto: cedere, pubblicare o diffondere senza consenso immagini, video o voci falsificati o alterati con IA, idonei a indurre in inganno sulla loro genuinità, causando danno ingiusto.

Pena: reclusione da 1 a 5 anni.

Procedibilità: a querela della persona offesa.

Procedibilità d'ufficio se:

- Connessione con delitto procedibile d'ufficio
- Vittima incapace per età o per infermità
- Fatto commesso contro pubblica autorità nell'esercizio delle funzioni

Sanzioni finanziarie e diritto d'autore

Art. 2637 c.c. (aggiotaggio):

Pena da 2 a 7 anni se fatto commesso con IA.

Art. 185, c. 1, D.Lgs. 58/1998 (T.U.F. — manipolazione mercato):

Pena da 2 a 7 anni e multa da €25.000 a €6M se fatto commesso con IA.

Art. 171, c. 1, lett. a-ter) L. 633/1941:

Reato per TDM in violazione artt. 70-ter e 70-quater L. 633/1941 anche tramite sistemi IA.

Consulenza alle imprese — strategia di conformità in 6 fasi

Non è un adempimento una tantum: è un processo continuo. L'AI Act spinge su accountability documentale.

1

AI Inventory

Mappare tutti i sistemi IA in uso o in sviluppo; classificare per livello di rischio AI Act (vietati / alto / trasparenza / minimo)

2

Role Mapping

Identificare se il cliente è provider, deployer, importatore, distributore — o più ruoli contemporaneamente (art. 25 AI Act)

3

Gap Analysis

Confrontare stato attuale con obblighi applicabili: documentazione, registrazione EU database, valutazione conformità, governance

4

Governance & Policy

Redigere/aggiornare: policy uso accettabile IA, registro sistemi IA, procedure incidenti, piano formazione, referente interno

5

Contrattualistica

DPA art. 28 GDPR + clausole AI Act in contratti con fornitori. Allocazione responsabilità provider/deployer. Diritti di audit.

6

Evidence Pack

Policy, verbali di decisione, contratti, procedure incidenti, piano formazione: tutto pronto per audit. Revisioni periodiche programmate.

Policy e istruzioni interne

Uso accettabile IA, dati ammessi nel prompt, escalation a un responsabile umano, regole per la pubblicazione di contenuti IA-generated

Verbali e decisioni documentate

Perché questo sistema? Perché in questa finalità? Chi ha deciso? Documentare la valutazione di classificazione del rischio e il razionale

Contratti e DPA

DPA art. 28 GDPR con ogni fornitore IA; clausole AI Act (obblighi, audit, incident); SCC + TIA per trasferimenti extra-UE; allocazione responsabilità provider/employer

Procedure incidenti

Chi notifica? A chi? In che tempi? Contatti dell'autorità di vigilanza (Garante, AGID, ACN). Piano di comunicazione verso gli interessati.

Piano di formazione

Registri delle sessioni; contenuti (prompt hygiene, rischi deontologici, segnalazione anomalie); aggiornamenti periodici previsti

Risk register e revisioni

Registro dei sistemi IA con livello di rischio, stato compliance, data della prossima revisione. Aggiornare quando cambia il sistema o la normativa.

PARTE III

L'avvocato che usa l'IA in studio: Tutela dei dati personali

Tre domande chiave: Quale strumento usi? Come lo usi? Cosa devi comunicare al cliente?

Il problema: cosa succede ai dati quando usi l'IA in studio?

L'avvocato che usa ChatGPT, Copilot o qualsiasi LLM in cloud per lavoro professionale è, ai sensi del GDPR, titolare del trattamento dei dati personali dei propri clienti. Lo strumento IA è il responsabile del trattamento (art. 28 GDPR). Questa qualificazione attiva obblighi precisi.

Il prompt

Quando scrivi un prompt, i dati inseriti — anche solo nome del cliente, fatti di causa, dati patrimoniali — vengono trasmessi al provider e possono essere:

- Conservati nei log del provider
- Usati per addestrare il modello (salvo opt-out o versione enterprise)
- Accessibili a dipendenti del provider o sub-fornitori
- Trasferiti fuori dall'UE

Il cloud

La quasi totalità dei servizi IA è erogata in cloud. Il dato lascia il perimetro dello studio e finisce su server — spesso negli USA — del provider. Questo configura un trasferimento extra-UE soggetto al Capo V GDPR. Clausole contrattuali standard o adesione al DPF UE-USA sono condizioni necessarie, non opzionali.

Il training reuse

Molti servizi gratuiti o consumer usano le conversazioni per affinare il modello. La versione gratuita di ChatGPT, per default, usa i prompt per il training. Se hai inserito dati del cliente, quei dati possono «entrare» nel modello e potenzialmente riaffiorare in output verso altri utenti.

L'avvocato è titolare (e deployer)

Lo studio legale che usa strumenti IA senza adeguate garanzie è esposto (anche) alle sanzioni GDPR

Prima di scegliere: leggere i termini del servizio

Regola UIA (Guidelines, § 3): prima di usare qualsiasi sistema IA, l'avvocato deve leggere i termini e le condizioni del servizio e capire come vengono usati i dati inseriti.

Domanda da fare al provider	Risposta accettabile	Risposta inaccettabile → azione richiesta
I miei prompt/conversazioni vengono usati per addestrare il modello?	No, mai (zero data retention) — o: sì, ma puoi fare opt-out nelle impostazioni con effetto immediato	Sì, per default → attivare l'opt-out oppure non inserire mai dati del cliente
I miei dati vengono visionati da dipendenti del provider?	Solo per sicurezza e prevenzione abusi, con policy di confidenzialità documentate	Accesso generale per miglioramento del servizio → non usare per dati riservati
Dove vengono elaborati i miei dati? In quale Paese?	In UE/SEE, o in USA con certificazione DPF + SCC e Transfer Impact Assessment	In Paesi terzi senza adeguate garanzie → violazione Capo V GDPR
Esiste un Data Processing Agreement (DPA) art. 28 GDPR?	Sì, disponibile e firmabile — versione enterprise solitamente lo include	No, o non disponibile per versione consumer → non è uno strumento utilizzabile per dati del cliente
Il servizio è disponibile in versione business/enterprise con garanzie rafforzate?	Sì: ChatGPT Enterprise, Microsoft Copilot for Business, Google Workspace AI, Claude for Business	Solo versione consumer → usare esclusivamente per attività senza dati personali identificativi

Il Data Processing Agreement (art. 28 GDPR)

Se usi un servizio IA per trattare dati personali dei tuoi clienti, un DPA scritto con il provider è obbligatorio per legge — non è negoziabile. Senza DPA, sei in violazione dell'art. 28 GDPR a prescindere da qualsiasi altra misura adottata.

Cosa deve contenere il DPA (art. 28, § 3 GDPR)

- **Oggetto e durata:**
- Descrizione precisa del trattamento, categorie di dati, finalità, durata della conservazione
- **Istruzioni vincolanti:**
- Il provider IA deve agire solo su istruzioni documentate dello studio
- Clausola ESPLICITA che vieta l'uso dei dati del cliente per addestrare il modello
- **Sub-responsabili (sub-processor):**
- Lista completa; obbligo di notifica preventiva in caso di variazioni
- Garanzia della catena contrattuale verso i sub-fornitori
- **Trasferimenti extra-UE:**
- SCC versione 2021 + Transfer Impact Assessment (TIA) documentato
- **Sicurezza (art. 32 GDPR):**
- Misure tecniche e organizzative; tempi di notifica breach
- **Audit e cooperazione:**
- Diritto di audit dello studio sul responsabile

Come trovarlo nella pratica (esempi)

OpenAI (ChatGPT)

Versione Enterprise / API: DPA disponibile. Versione gratuita/ NO DPA
→ non usare per dati cliente

Microsoft Copilot

Microsoft 365 Copilot for Business: DPA incluso nel contratto Microsoft.
Copilot consumer gratuito: NO

Google Gemini

Google Workspace AI (piano Business/Enterprise): DPA incluso. Gemini consumer: NO

Claude (Anthropic)

Claude.ai Pro/Team/Enterprise: DPA disponibile. Claude.ai gratuito: NO

Strumenti legali specializzati

Di solito includono DPA — verificare le clausole su uso dati per training, sempre

DPIA: Quando è obbligatoria se usi l'IA?

Art. 35 GDPR: la DPIA (Data Protection Impact Assessment) è obbligatoria quando il trattamento può presentare un rischio elevato per i diritti e le libertà degli interessati. L'uso di IA per dati dei clienti rientra spesso in questa categoria. Il Garante ha pubblicato un elenco di trattamenti che la richiedono (Prov. 11 ottobre 2018).

Quando la DPIA è obbligatoria (art. 35, §3 GDPR)

- Valutazione sistematica su larga scala basata su profilazione o trattamento automatizzato (lett. a)
- Trattamento su larga scala di dati particolari (art. 9) o relativi a reati (lett. b)
- Sorveglianza sistematica su larga scala di aree accessibili al pubblico (lett. c)

La "regola del 2" delle LL.GG. WP248 sulla DPIA può far ritenere spesso obbligatoria la DPIA

Contenuto minimo della DPIA (art. 35, §7 GDPR)

- Descrizione sistematica del trattamento e delle sue finalità
- Valutazione della necessità e proporzionalità rispetto alle finalità
- Valutazione dei rischi per i diritti e le libertà degli interessati
- Misure previste per affrontare i rischi (salvaguardie, misure di sicurezza, meccanismi per garantire la protezione)
- Consultazione preventiva del Garante se i rischi residui restano elevati (art. 36 GDPR)

Pratica per lo studio legale

Uso episodico di ChatGPT Enterprise per prompting (senza dati cliente): DPIA generalmente non richiesta. Uso sistematico di piattaforma IA integrata nella gestione di pratiche con dati dei clienti: DPIA (probabilmente) obbligatoria.

Organizzare lo studio: policy, formazione e governance

L'art. 4 AI Act impone a tutte le organizzazioni (inclusi gli studi legali) di garantire la literacy in materia di IA a tutto il personale che usa sistemi IA.

Policy d'uso accettabile (Acceptable Use Policy)

Definire: quali strumenti IA sono autorizzati; per quali attività; chi può usarli; quali dati possono essere inseriti; procedura di escalation in caso di dubbio. Aggiornare quando arrivano nuovi strumenti.

Registro degli strumenti IA in uso

Elenco di tutti i sistemi IA usati in studio con: nome del provider, versione, DPA in essere sì/no, localizzazione dati, data dell'ultimo check dei termini.

Formazione del personale (art. 4 AI Act)

Per tutti gli utenti su: cosa può e non può fare l'IA; regole di prompt hygiene; come segnalare anomalie; dove trovare la policy interna. Tenere traccia delle sessioni (obbligatorio per accountability).

Procedura di verifica degli output

Chi redige con IA → chi verifica → chi approva prima del deposito/invio al cliente. Anche per studi individuali: documentare il proprio processo di revisione. Non depositare mai un testo IA senza review integrale.

Referente interno per la governance IA

Anche negli studi piccoli: identificare un referente (l'avvocato titolare, o un collaboratore designato) per la governance IA. Gestisce i DPA, aggiorna la policy, è il punto di contatto per incidenti e segnalazioni al Garante.

Gestione degli incidenti e notifica al Garante

Se un dato personale del cliente è stato esposto tramite l'IA (es. breach del provider): notifica al Garante entro 72 ore (art. 33 GDPR) + comunicazione all'interessato se c'è rischio elevato (art. 34 GDPR).

Sintesi — La checklist dell'Avvocato che usa l'IA in studio

Prima di usare qualsiasi sistema IA per attività professionale, verifica questi 8 punti. Tutti devono avere risposta positiva.

✓
1

Ho letto i termini e condizioni?

So come vengono usati i miei dati — in particolare se per il training del modello

✓
2

Ho un DPA firmato con il provider?

Il provider è qualificato come responsabile del trattamento ex art. 28 GDPR, con istruzioni vincolanti e garanzia no-training

✓
3

I dati sono localizzati correttamente?

Il servizio elabora i dati in UE/SEE, o ho SCC + TIA per i trasferimenti extra-UE

✓
4

Ho effettuato la DPIA (se necessaria)?

Trattamento sistematico di dati dei clienti con IA → DPIA (molto probabilmente) obbligatoria.

✓
5

Applico la prompt hygiene?

Non inserisco mai dati identificativi del cliente nel prompt. Anonimizza prima. Uso solo versione enterprise/business.

✓
6

Ho informato il cliente dove necessario?

Se uso l'IA su dati del cliente, lo devo informare. Se uso un bot IA che risponde al cliente, dichiaro che è IA.

✓
7

Verifico sempre l'output?

Ogni riferimento normativo e giurisprudenziale viene verificato sulla fonte primaria. Non deposito mai senza review integrale.

✓
8

Ho adottato processi di governance interna?

Policy d'uso, registro strumenti IA, formazione collaboratori (art. 4 AI Act), referente interno, procedura incidenti.

Grazie per l'attenzione

Avv. Giovanni Battista Gallus
gallus@array.law | GDL FIIF – CNF

