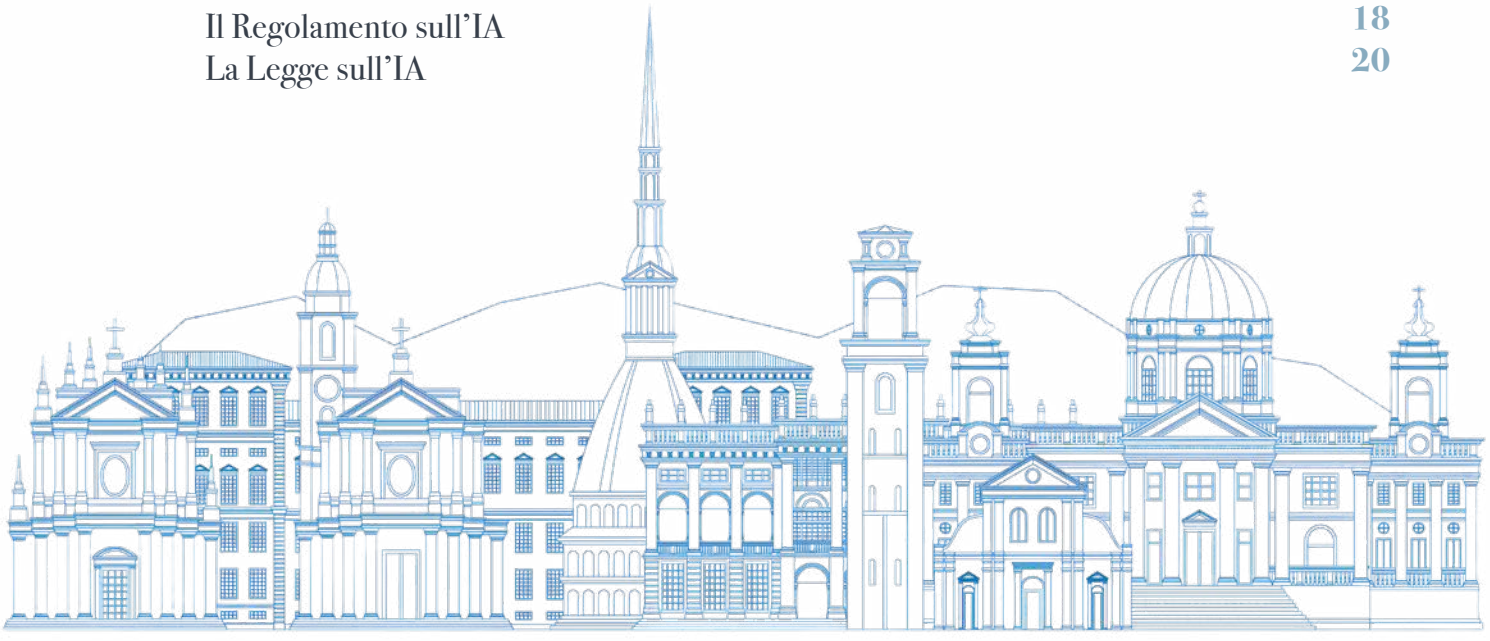
BrevIArio normativo sull'uso dell'IA

ORDINE AVVOCATI DI TORINO

c'è chi fa l'avvocato
e chi è *avvocato.*

ORDINE AVVOCATI DI TORINO

Sommario



Premessa

L'intelligenza artificiale (IA) – locuzione suggestiva e da molti studiosi criticata che designa una eterogenea famiglia di tecnologie basate su complesse reti di calcolo e l'elaborazione di grandi moli di dati – riguarda ormai ogni ambito della vita quotidiana, finendo per incidere – in certi contesti e quantomeno potenzialmente – sui meccanismi stessi di comprensione della realtà. Appare ormai necessario, quindi, che ogni professionista sia consapevole e si interroghi opportunamente sulle conseguenze dell'introduzione dell'IA nella sua attività professionale quotidiana, nel tentativo di tracciare un sentiero virtuoso funzionale ad un uso responsabile e informato.

L'IA deve essere sotto il controllo umano, sviluppata in modo equo (scongiurando il rischio di disuguaglianze e discriminazioni), trasparente e comprensibile. È indispensabile, in altre parole, che sia utilizzata per finalità costruttive e per supportare le capacità umane, non per sostituirle, favorire l'abuso e la violazione dei diritti e il dominio di pochi su molti. Del pari, è necessario comprendere che non tutto quello che è tecnicamente fattibile è – e deve essere automaticamente considerato – deontologicamente e giuridicamente accettabile.

In questo contesto, il diritto è destinato a giocare un ruolo fondamentale non solo sul piano della normazione tecnica ma, a monte, sulla tutela e la salvaguardia di taluni diritti fondamentali che sono infatti divenuti tra i più rilevanti protagonisti del dibattito che ha accompagnato il lungo percorso consultivo/legislativo preliminare all'adozione del Regolamento (UE) 2024/1689 (Regolamento sull'intelligenza artificiale, anche conosciuto come "AI Act", di seguito "Regolamento sull'IA")[1] e della Legge 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di IA di seguito "Legge sull'IA")[2] .

Proprio al fine di mitigare i rischi associati all'uso dell'IA, anche il Regolamento sull'IA ha introdotto (seppur limitatamente ad alcuni ambiti) una apposita procedura di valutazione d'impatto dell'impiego dell'IA sui diritti fondamentali (FRIA - Fundamental rights impact assessment)[3] e l'obbligo di evitare rischi sistemici (che, ai sensi dell'art. 2 n. 65 del Regolamento sull'IA, possono avere "un impatto significativo sul mercato dell'Unione a causa della sua portata o di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso, che può propagarsi su larga scala lungo l'intera catena del valore")[4] .

[1] Vedi https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202401689
[2] Vedi https://www.normattiva.it/eli/id/2025/09/25/25G00143/ORIGINAL
[3] Vedi art. 27 del Regolamento sull'IA
[4] Vedi art. 55 del Regolamento sull'IA

Nonostante l'elevato tecnicismo dei meccanismi di funzionamento dell'IA rischi di far percepire la materia come di esclusiva competenza degli "addetti ai lavori" non deve trascurarsi il fatto che anche i fruitori dei sistemi sono tenuti ad approcciare ogni strumento con consapevolezza e competenza, evitando di incorrere in negligenze evitabili.

Nella proliferazione continua di automatismi digitali la centralità dell'uomo, come è stato recentemente ribadito dalla normativa nazionale appena introdotta, non può e non deve essere messa in discussione, in particolare in ambiti quale l'amministrazione della giustizia, ed è compito di ciascun professionista che si trovi a lavorare con sistemi di IA essere conscio delle questioni (tecniche e deontologiche) che intorno agli stessi gravitano, al fine di assicurare – per sé, per i propri collaboratori e soprattutto per i propri assistiti – un utilizzo compatibile con i principi della professione e, al contempo, scongiurare l'insorgere di "nuove" ipotesi di responsabilità che un uso scorretto dell'IA potrebbe comportare.

Per un utilizzo consapevole di queste tecnologie è necessario aver sempre presente che la locuzione "intelligenza artificiale" non ha una reale corrispondenza con l'intelligenza umana, per quanto la definizione sia così antropoformizzante; i risultati, gli output delle macchine, spesso sorprendenti e utili, sono il frutto di un complesso calcolo sempre meramente probabilistico.

Gli applicativi più rilevanti nel settore legale, ovvero le IA predittive e di analisi (si pensi alle banche dati giurisprudenziali) e soprattutto le IA per finalità generali basate su modelli linguistici di grandi dimensioni (LLM) che generano linguaggio artificiale, sono comunque basate su una mera probabilità statistica generata da una elaborazione informatica dei dati di addestramento. La macchina non "ragiona" sul tema proposto – sebbene in alcuni casi simuli un ragionamento – e non analizza la realtà fattuale: l'IA generativa, ha la capacità di "datificare" il linguaggio (qualunque linguaggio, testuale sonoro o visivo), di scomporlo in numeri, "token", e riassemblarlo sulla base di complesse logiche statistiche o, meglio, probabilistiche. Nella generazione del linguaggio artificiale, nei sin troppo noti chatbot, semplicemente la parola più probabile viene inserita nel contesto dato dalle precedenti; l'output non ha, per la macchina, nessun significato corrispondente alla realtà fattuale o concettuale. Le c.d. allucinazioni – altro termine antropomorfizzante la macchina, suggestivo e falsante – sono errori per l'umano che attribuisce all'output il significato atteso, ma non sono errori per la macchina che, semplicemente, calcola le probabilità.

La consapevolezza di essere di fronte a meri risultati probabilistici elaborati da una macchina e da software evoluti non elide la valenza potenzialmente positiva e l'utilità di queste tecnologie e, in relazione ai diversi settori di applicazione, il loro uso può essere legittimo e indubbiamente utile. Tutti debbono però esser consapevoli dei limiti di queste tecnologie, all'attuale stato dell'arte.

Nel settore legale, nell'ambito della giustizia, lo stato dell'arte di queste tecnologie impone un approccio di grande prudenza e di piena consapevolezza dei limiti e dei rischi.

Nella professione di avvocato, i profili critici e di sicuro interesse possono essere così riassunti:

1. **(In)adeguatezza nell'utilizzo:** fare affidamento su risultati di IA senza una costante valutazione critica e una necessaria convalida umana, può condurre ad errori gravi.

2. **Bias:** i dati di addestramento determinano l'output del sistema e l'algoritmo stesso può determinare risultati errati, discriminatori o iniqui.

3. **(In)spiegabilità:** gli algoritmi di IA sono "black box", scatole nere da cui è difficile capire come e perché si siano generati determinati risultati o suggerimenti; questo aspetto è particolarmente evidente e rilevante nel caso della cosiddetta IA generativa. In ambito giudiziario la mancanza di trasparenza può ledere il contraddittorio e può esser fonte di iniquità e ingiustizie.

4. **Conformità:** Insufficiente sicurezza, privacy, segretezza, con conseguente lesione di molteplici diritti fondamentali.

5. **Trasparenza:** i clienti potrebbero non essere completamente consapevoli del ruolo che l'IA può svolgere nel loro caso.

Anche in considerazione del quadro giuridico attualmente in evoluzione, questo documento vuole aver lo scopo di fornire alcune indicazioni pratiche per l'utilizzo consapevole dei sistemi di IA.

Uso dell'IA: norme applicabili

L'utilizzo di sistemi di IA da parte dello studio legale deve tenere conto del nuovo Regolamento sull'IA e della Legge sull'IA; inoltre, si inserisce in un contesto di norme già esistenti in diverse materie che l'avvocato è tenuto a rispettare.

È necessario, pertanto, fare riferimento ad esse quando lo studio legale (avvocati e collaboratori) decide di avvalersi di sistemi di IA durante lo svolgimento della professione: dalla redazione degli atti, al ciclo di vita dei contratti, alla fase stragiudiziale, alla gestione dell'ufficio, ecc.

Nel presente documento si prendono in considerazione alcuni profili legati all'impiego di sistemi di IA nello svolgimento dell'attività professionale.

A seconda del tipo di sistema e di modalità d'uso rilevano i diversi quadri normativi.

Per esempio, si possono usare sistemi di IA utilizzando traduttori software, di scansione OCR, sistemi generativi esperti tipo RAG (Retrieval-Augmented Generation) e/o sistemi agenti: la differenza di funzionamento tra questi sistemi
è molto profonda e le implicazioni dell'uso di uno o dell'altro sono molto diverse.

Si individuano di seguito alcune aree normative che sono applicabili all'Avvocato che utilizza sistemi di IA che rilevano o meno, a seconda del tipo di sistema di IA e del modo in cui lo stesso viene utilizzato (es. come servizio fornito da terzi o come sistema gestito dall'avvocato e nel suo pieno controllo):

1. **protezione dei dati personali;**
2. **diritti di proprietà intellettuale;**
3. **Regolamento sull'IA e Legge sull'IA.**

Concludendo, si suggerisce di mappare in primis quali strumenti di IA siano già in uso dall'Avvocato verificando se siano rispettosi delle prescrizioni delle aree normative appena citate: spesso, infatti, l'IA può essere già presente negli strumenti di lavoro utilizzati quotidianamente

1. protezione dei dati personali

Usando sistemi di IA si possono trattare dati personali (di clienti o di terzi); per esempio, se sono inclusi nei prompt di interrogazione di un sistema di IA o nelle basi di dati utilizzate per addestrare il sistema di IA, per raffinarne l'addestramento o per farlo funzionare con dati di contesto. Ma l'avvocato potrebbe trattare dati personali anche senza inserirli nei prompt o nelle basi di dati che utilizza con il sistema di IA: se per esempio un sistema di IA generativa fornito da terzi è stato addestrato con dati che includono dati personali, la risposta a un prompt d'interrogazione potrebbe contenere dati personali che non sono stati inseriti dall'utente.

In tutti questi casi l'avvocato che utilizza un sistema di IA tratta dati personali e quindi deve adempiere gli obblighi previsti dalle norme applicabili, in particolare il Regolamento (UE) 2016/679, regolamento generale sulla protezione dei dati (RGPD)[5] che, tra l'altro, all'art. 5 indica i principi e agli artt. 6-10 le condizioni di liceità da rispettare nel trattamenti di dati personali.

ATTIVITÀ SUGGERITE PRIMA DI INIZIARE IL TRATTAMENTO

a. Come documentarsi prima di utilizzare un sistema di IA

La CNIL francese (Commission nationale de l'informatique et des libertès) ha pubblicato una serie di checklist di autovalutazione per aiutare il titolare del trattamento a valutare i rischi associati al sistema di IA prima della fase di progettazione[6]. Allo stesso modo il Garante per la Protezione dei dati personali (d'ora in avanti "Garante") ha pubblicato un repository pubblico[7] dove è possibile rinvenire documentazione utile per chi tratta i dati personali nel contesto dell'IA: provvedimenti, news, interviste e tool. Si possono trovare spunti interessanti anche sul sito dell'autorità garante inglese[8] .

È utile, inoltre, tenersi aggiornati sul sito dell'Ufficio europeo per l'IA[9] e sul sito del Comitato Europeo per la Protezione dei Dati, o European Data Protection Board[10].

[5] Vedi https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679
[6] Vedi https://www.cnil.fr/en/self-assessment-guide-artificial-intelligence-ai-systems
[7] Vedi https://www.garanteprivacy.it/temi/intelligenza-artificiale
[8] Vedi https://ico.org.uk/
[9] Vedi https://digital-strategy.ec.europa.eu/it/policies/ai-office
[10] Vedi https://www.edpb.europa.eu/edpb_it

b. IA come servizio, artt. 28 e 44-50 RGPD

Se il titolare del trattamento (l'Avvocato) non è il fornitore del sistema di IA, la condivisione delle responsabilità tra queste due parti deve essere formalizzata. Tali responsabilità devono essere chiare e devono concretizzarsi in un accordo conforme al disposto dell'art. 28 del RGPD.
Si suggerisce, pertanto, di mappare i propri strumenti di lavoro, verificando la presenza di sistemi di IA, anche all'interno di eventuali nomine a responsabile del trattamento già sottoscritte. Si possono verificare casi in cui lo strumento giuridico vincolante ai sensi dell'art. 28 RGPD consiste in un impegno unilaterale da parte del fornitore delle soluzioni di IA; in tali casi l'assenza di potere negoziale deve essere compensata da uno scrupoloso controllo, da parte dell'Avvocato, delle clausole "imposte".
I fornitori di sistemi di IA potranno essere selezionati sulla base del rispetto dei principi stabiliti dal RGPD.

c. La valutazione di impatto, art. 35 RGPD e sicurezza correlata

Se si usano sistemi di IA che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è necessario realizzare una valutazione d'impatto ai sensi dell'art. 35 del RGPD. L'European Data Protection Board ha specificato che un fornitore non sempre sarà in grado di valutare tutti gli utilizzi del proprio sistema di IA. Quindi, la valutazione del rischio iniziale da lui svolta sarà di natura più generale rispetto a quella effettuata dall'utente del sistema di IA (nel nostro caso l'Avvocato). Anche se la valutazione del rischio iniziale a opera del fornitore non classifichi il sistema di IA come «ad alto rischio» ai sensi del Regolamento sull'IA, non si dovrebbe escludere una successiva (più granulare) valutazione d'impatto sulla protezione dei dati, a norma dell'articolo 35 del RGPD, che dovrebbe essere effettuata dall'Avvocato tenendo conto del contesto dell'utilizzo e dei casi d'uso specifici. La valutazione della possibilità che un determinato trattamento sia tale da comportare un rischio elevato ai sensi del RGPD deve essere eseguita indipendentemente dalle previsioni del Regolamento sull'IA.

Per contro, la classificazione di un sistema di IA come «ad alto rischio» causa del suo impatto sui diritti fondamentali comporta la presunzione dell'esistenza di un «rischio elevato» anche ai sensi del RGPD, nella misura in cui vi sia trattamento dei dati personali. Indipendentemente dal modello di IA adottato ed utilizzato, va valutato sotto il profilo della sicurezza anche il software utilizzato per farlo funzionare, sia quando si utilizza un sistema prodotto da un fornitore, sia quando si programmi del software ad hoc.
Uno strumento raccomandato per effettuare la valutazione di impatto è il tool dell'Autorità garante dei dati personali francesi CNIL[10], presente nel sito web

del Garante per la Protezione dei dati personali italiano[11].
Il tool del CNIL consente di identificare i rischi associati all'utilizzo dei sistemi di IA grazie alla compilazione dello stesso ed all'ottenimento della visualizzazione di tali rischi grazie, anche, ai grafici ad hoc che il suddetto tool genera a seguito dell'inserimento delle informazioni richieste.

Ottenuto il report finale va eseguita l'analisi valutando l'impatto:

- sulla riservatezza dei dati trattati;
- sulla sicurezza dei dati trattati;
- sulla conformità normativa.

Una volta completata questa fase andranno valutate le eventuali misure di mitigazione come, ad esempio, la crittografia dei dati e la formazione del personale dello studio.
La valutazione di impatto, vista la continua evoluzione digitale, richiede un monitoraggio regolare dei sistemi di IA, il relativo aggiornamento (periodico) degli stessi e la conseguente revisione periodica della valutazione di impatto.

d. Il registro dei trattamenti, art. 30 RGPD

Qualora il titolare del trattamento sia soggetto all'obbligo della tenuta del registro, lo stesso dovrà considerare anche i trattamenti che utilizzino sistemi di IA.
Per esempio, qualora lo studio impieghi un sito web per promuovere le proprie attività, che include funzionalità tipo chatbot, permettendo l'inserimento di dati personali, l'avvocato dovrà inserire all'interno del registro delle attività di trattamento, un apposito record dedicato a tale trattamento dei dati sul sito web.

e. Informativa al cliente, art. 13 RGPD

È necessario verificare che l'informativa ai sensi dell'art. 13 del RGPD fornita al cliente includa i trattamenti realizzati con sistemi di IA.
Come illustrato di seguito, la Legge sull'IA prevede un obbligo di informativa specifica relativamente all'uso di sistemi di IA da parte del professionista.
La normativa non sembra ostare all'assolvimento di tali obblighi nel contesto dell'informativa resa ai sensi dell'art. 13 RGPD ma, sul punto, è bene che ogni opportuna valutazione venga effettuata dall'avvocato, essendo certamente legittimo anche fornire un'informativa separata e aggiuntiva.

[11] Vedi https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
[12] Vedi https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-

Operativamente, queste informazioni possono essere:

- incluse nell'accordo con il cliente;
- comunicate via e-mail (anche in occasione della trasmissione di una nota di onorario);
- fornite mediante la pubblicazione di una informativa sul sito web dello studio.

f. Sicurezza, artt. 25 e 32 RGPD

Ai sensi dell'art. 25 del RGPD il titolare del trattamento deve concentrarsi sulla protezione dei dati fin dalla progettazione, nonché per impostazione predefinita, del proprio sistema digitale e fisico di informazioni (queste ultime intese come insieme di dati), includendo "minimizzazione dei dati, pseudonimizzazione e cifratura". In tal senso è ormai comunemente utilizzata l'espressione "Privacy by design e by default", con ciò volendo mettere in risalto la necessità di curare "l'architettura" del proprio sistema di trattamento dati salvaguardando, fin da subito ed in maniera costante e crescente, la sua sicurezza e gli strumenti di protezione deputati a garantirla.

È altresì necessario evidenziare le misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio, ponendo l'attenzione su quanto disciplinato dall'art. 32 RGPD in merito agli strumenti di protezione tecnici ed organizzativi da implementare (almeno quelli di base – vedi infra); mutuando l'espressione utilizzata per l'art. 25, in questa sede, si potrebbe parlare di "Cybersecurity by design e by default".

Ciò premesso, si dovrebbero, ad esempio, implementare le seguenti misure.

1) Misure tecniche

CRITTOGRAFIA

Nel momento in cui si utilizzi un sistema d'IA fornito da terzi come servizio (v. chatbot conversazionali, e piattaforme di servizi legali basati su IA generative) al fine di agevolare il lavoro dello studio legale, è raccomandabile implementare protocolli di crittografia sicuri sia per proteggere i dati in transito, sia per strutturare algoritmi crittografici volti a proteggere i dati a riposo. È utile il supporto di un tecnico specializzato.

Nel momento in cui si utilizzi un sistema di IA che viene gestito internamente per agevolare il lavoro dello studio legale, è ancor più importante avvalersi della collaborazione di un tecnico, che sia anche un programmatore, capace di implementare idonee misure di criptazione del sistema di IA utilizzato.

BACKUP DEI DATI

Va implementato un sistema di backup dei dati trattati, indipendentemente dallo strumento di IA utilizzato dallo studio legale, al fine di garantire la confidenzialità, l'integrità e la disponibilità dei dati in caso di perdita, accesso abusivo o danneggiamento (data breach).

A tal fine è utile eseguire quanto segue:

- identificare i dati che lo studio legale tratta e che devono essere salvati;
- nel caso di utilizzo di modelli di IA, eseguire backup regolari degli output (ove i risultati trattino dati personali) e dei dati di addestramento;
- classificare i dati in base alla loro importanza;
- scegliere la strategia di backup, a seguito della pianificazione temporale di essi e della conservazione dei dati salvati: a) backup completi dei dati trattati e del sistema di IA, inclusi i dati e i modelli di IA modificati/aggiornati; b) backup incrementali solo sui dati modificati/aggiornati (il mercato offre strumenti di backup specializzati e generici);
- verificare che i backup siano eseguiti correttamente ed eseguire test periodici di ripristino per garantire che i dati possano essere ripristinati correttamente;
- criptare i backup e controllare l'accesso agli stessi per garantirne l'accesso solo agli utenti autorizzati.

STRUMENTI DI SICUREZZA BASE PER LA RETE INFORMATICA DELLO STUDIO LEGALE

Gli strumenti e le modalità di sicurezza informatica che si possono applicare (così come per la tutela di ogni categoria di dato digitale) sono per esempio:

- Antivirus;
- E-mail esclusiva quale ID-account per il sistema d'IA;
- Firewall;
- IDS (Intrusion Detection System) eventualmente associato ad un IPS (Intrusion Prevention System);
- Aggiornamento del software;
- Esecuzione sistematica (con cadenza da predefinire, almeno una volta ogni sei mesi) di test di penetrazione;
- Analisi periodica dei log di accesso ai sistemi di IA.

2) Misure organizzative

Definire ed adottare una policy adeguata al corretto utilizzo ed all'analisi preventiva dei sistemi di IA utilizzati, afferente il profilo organizzativo della gestione di sicurezza dati, nonché quello formativo ed informativo.

Per esempio:

- esaminare attentamente i "Termini di condizioni e servizio" stabiliti dai fornitori di sistemi di IA per garantire la conformità agli standard deontologici e legali, ove si tratti di sistemi forniti da terzi (laddove si tratti di sistemi proprietari implementare ed impostare la "compliance" richiesta dalla normativa di settore in punto misure tecniche ed organizzative);

- assicurarsi che i sistemi di IA utilizzati dispongano di adeguate misure di sicurezza;

- implementare un regolamento interno con specifiche regole relative all'adozione degli strumenti IA (casi di utilizzo, limiti di impiego, autorizzazioni al suo utilizzo, regole di anonimizzazione dei dati ove necessarie, comunicazioni sull'utilizzo del sistema di IA da dare al cliente, controllo periodico degli strumenti di sicurezza configurati ed implementati, vaglio delle regole di backup, check programmati e periodici del tecnico informatico, ecc.);

- aggiornare le prassi lavorative dello studio riflettendo l'evoluzione delle norme sull'uso dell'IA;

- prevedere una regolare formazione di tutti i componenti dello studio legale sul trattamento dei dati personali nell'uso di strumenti d'IA;

- pianificare una formazione continua dei membri dello studio legale per metterli a conoscenza di eventuali normative nazionali ed internazionali (o stabilite dagli Ordini Forensi) e sensibilizzarli sull'importanza della sicurezza e sulla necessità di seguire le procedure di sicurezza.

2. proprietà intellettuale

RISPOSTA / OUTPUT

Se si utilizzano sistemi di IA che producono come risultato del loro uso testi, immagini, video e/o audio, va considerata l'eventualità che l'output generato dallo strumento di IA violi diritti di proprietà intellettuale di terzi, disciplinati dalla Legge 22 aprile 1941, n. 633, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (LDA) e dal Decreto Legislativo 10 febbraio 2005, n. 30, Codice della proprietà industriale, a norma dell'articolo 15 della legge12 dicembre 2002, n. 273 (CPI)[14].

Pur non essendo agevole verificare, in concreto, se sussista una violazione dei diritti di terzi, si suggerisce di:

- leggere con attenzione le condizioni contrattuali applicate all'utente finale (c.d. EULA, acronimo di End User License Agreement) unitamente alla documentazione messa a sua disposizione dal fornitore dello strumento di IA, onde verificare la politica di quest'ultimo in ordine alle violazioni. In particolare, è opportuno valutare le clausole inerenti alla responsabilità dell'utente, alle limitazioni di responsabilità del fornitore, alla titolarità degli output e alle obbligazioni poste in capo all'utente al fine di mitigare possibili conseguenze negative derivanti dall'impiego dello strumento, nonché alle eventuali clausole (ad onor del vero, non comuni da riscontrare) che prevedono a carico del fornitore forme indennitarie di ristoro dei danni o di assistenza nell'ambito di un eventuale procedimento giudiziario in cui l'utente sia chiamato a rispondere della violazione di diritti di terzi e a tenere indenne il medesimo dalle conseguenze negative derivanti da un eventuale esito infausto del giudizio;

- verificare se il fornitore dello strumento di IA sia disponibile ad impegnarsi contrattualmente a condizioni ulteriori rispetto a quelle previste nell'EULA;

- verificare che lo sviluppatore del sistema di IA abbia adottato in fase di addestramento del modello misure volte a mitigare il rischio di violazione di diritti di terzi.
  La verifica potrà essere condotta consultando la sintesi dei contenuti utilizzati per l'addestramento del modello che, nel caso di sistemi di IA per finalità generali, il fornitore è tenuto a redigere e a mettere a disposizione del pubblico ai sensi dell'art. 53 del Regolamento sull'IA o, nel caso di sistemi di IA ad alto rischio, le istruzioni per l'uso che il fornitore è tenuto a redigere e mettere a disposizione del deployer ai sensi dell'art. 13 del Regolamento sull'IA;

[13] Vedi https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1941-04-22;633!vig=
[14] Vedi https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-02-10;30!vig=

- verificare se il fornitore dello strumento di IA abbia pubblicato sul proprio sito web o messo altrimenti a disposizione del pubblico, una guida divulgativa che spieghi agli utenti come mitigare i rischi di violazione di diritti di terzi. Il rispetto di tali indicazioni potrebbe non solo diminuire i rischi di violazione, ma anche rendere conforme il proprio utilizzo dello strumento di IA alle condizioni contrattualmente previste;

- revisionare l'output onde identificare violazioni dei diritti di terzi (e la presenza di errori);

- implementare linee guida per minimizzare i rischi di generazione di output in violazione dei diritti di terzi.

PROMPT / INPUT

L'Avvocato che utilizza strumenti di IA forniti come servizio che prevedono che l'utente fornisca istruzioni o sottoponga una domanda (c.d. prompt o input) che il sistema di IA utilizza per generare una risposta o eseguire un'azione specifica (c.d. response o output), deve considerare che il fornitore potrebbe salvare i prompt utilizzati dall'utente ed utilizzarli per l'addestramento del proprio modello (o ad altri fini) e valutare i rischi connessi.

È fondamentale pertanto verificare se il fornitore fornisca garanzie sul fatto che ciò non avvenga e se sussistono condizioni supplementari a tal fine (es. pagamento di abbonamenti particolari, sottoscrizione di accordi).
Nell'ipotesi in cui l'utente includa nei prompt informazioni riservate, non è possibile escludere che queste divengano anche pubbliche se integrate all'interno del modello che alimenta lo strumento di IA e condivise sotto forma di output con altri utenti: l'Avvocato non deve inserire nel prompt informazioni riservate.

Diritti di proprietà intellettuale sui sistemi d'IA

Per utilizzare in modo consapevole gli strumenti di IA, è opportuno che l'Avvocato sia edotto del fatto che i diritti di proprietà intellettuale non riguardano solo input e output, ma anche gli strumenti stessi.
Gli strumenti di IA sono costituiti da (almeno) due fondamentali componenti che possono accedere a tutele assai diversificate tra loro. Essi sono il software e i dati.

SOFTWARE

I programmi per elaboratore che integrino il requisito dell'originalità possono accedere alla tutela autoriale ai sensi degli artt. 1, 2 e 64-bis della LDA. In ossequio ai generali principi che informano la materia, la protezione viene accordata alla sola forma espressiva e non si estende alle idee e i principi ad essa sottesi. Pertanto, troverà protezione in quanto originale l'algoritmo espresso in linguaggio di codice di programmazione, mentre l'algoritmo in quanto tale resterà escluso dal perimetro della protezione.

In prima approssimazione, i programmi per elaboratore in quanto tali sono invece esclusi dalla brevettazione ai sensi dell'art. 45 del CPI, fatta eccezione per quelli in grado di produrre un "effetto tecnico ulteriore" quando vengono eseguiti su un elaboratore. Del pari, gli algoritmi in quanto tali sono di norma esclusi dalla brevettazione, essendo metodi matematici, ai sensi dell'art. 45 del CPI. Non si esclude, tuttavia, la brevettabilità di una invenzione basata su un algoritmo o metodo matematico nell'ipotesi in cui quest'ultimo contribuisca alla produzione di un effetto tecnico per finalità tecniche.

DATI

I dati necessari al funzionamento dei sistemi d'IA possono essere oggetto di diritti di proprietà intellettuale e, se l'avvocato conferisce dati per far funzionare tali sistemi di IA (per addestrarli, per raffinarne l'addestramento o per farli funzionare con dati di contesto) deve verificare d'essere titolare dei diritti necessari per fare uso dei dati stessi; è peraltro utile considerare l'eccezione prevista dagli artt. 70-quater e 70-sexies della LDA che possono facilitare l'uso di dati tutelati dal diritto d'autore e diritti connessi con sistemi di IA.

L'attività di costruzione delle librerie di dati necessarie per il funzionamento dei sistemi di IA può, in alcuni casi, comportare la costituzione di nuovi diritti da tutelare (si pensi ad es. alle attività di pulizia, elaborazione e annotazione dei set di dati originali). Non si può escludere che i set di dati annotati dallo sviluppatore possano accedere alla tutela sui generis delle banche dati non creative ai sensi dell'art. 102-bis della LDA nella misura in cui vengano effettuati investimenti rilevanti nella verifica dei dati. In difetto dei presupposti di accesso al diritto sui generis, lo sviluppatore potrebbe ricorrere alla tutela del segreto commerciale ai sensi dell'art. 98 del CPI o ad una regolamentazione pattizia delle forme di accesso, uso e ri-uso dei set di dati o dei modelli.

Quanto ai modelli di IA (che anche consistono in set di dati) è controverso se gli stessi siano tutelabili con diritto d'autore ai sensi dell'art. 1, 2 e 64-quinquies della LDA o diritto sui generis del costitutore di banca di dati ai sensi dell'art. 102-bis della LDA.

IN GENERALE

È opportuno che l'Avvocato che voglia utilizzare uno strumento di IA sia consapevole se il medesimo sia o meno tutelato da altrui diritti di proprietà intellettuale, da quali diritti e con quali limiti, anche al fine di evitare violazioni.

In ogni caso, non è agevole verificare, in concreto, se un determinato strumento di IA possa essere, o meno, oggetto di tutela e quali siano i limiti della medesima.

Oltre a quanto indicato sopra si suggerisce:

- nel leggere le condizioni contrattuali applicate all'utente finale, di prestare attenzione alle disposizioni relative ai diritti di proprietà intellettuale, onde comprendere se lo strumento di IA che si intende utilizzare sia proprietario – cioè di proprietà esclusiva di una persona/società/ente – e chi sia tale proprietario o se sia open source – cioè disponibile pubblicamente – e fare attenzione alle disposizioni attinenti alle limitazioni d'uso;

- di considerare le indicazioni di utilizzo previste nelle condizioni contrattuali (la violazione di tali limitazioni, oltre ad esporre l'Avvocato a eventuali azioni legali, potrebbe comportare la revoca della licenza d'uso e quindi il blocco dell'accesso allo strumento di IA e la disattivazione dell'account);

- di considerare che a volte i fornitori rivendicano diritti senza un certo e tutelabile fondamento giuridico.

3. Regolamento sull'IA e Legge sull'IA

Il Regolamento sull'IA

L'articolo 5 (Pratiche di IA vietate) del Regolamento sull'IA si applica a chiunque, e quindi anche all'Avvocato.

Quindi l'Avvocato non potrà utilizzare un sistema di IA, per esempio:

- per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità;

- per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione.

L'articolo 3, n. 4 del Regolamento sull'IA definisce «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".

La definizione si applica all'uso del sistema di IA da parte dell'Avvocato nel quadro della propria attività. Il Regolamento sull'IA prevede alcune norme che impongono obblighi al deployer (e quindi all'Avvocato) che, in casi particolari, possono divenire molto onerosi (si pensi, ad esempio, al caso in cui, ai sensi dell'art. 25, l'Avvocato apponga il proprio nome o marchio, apporti modifiche sostanziali o cambi la finalità prevista di un sistema di IA, diventando così fornitore di un sistema di IA e trovandosi a dover rispettare tutti i maggiori obblighi correlati).

L'articolo 4 (Alfabetizzazione in materia di IA) prevede che i deployer di 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.".

Gli articoli 4 e 5 sono in vigore dal 2 agosto 2025.

In alcuni casi (vedi l'art. 6, paragrafo 2, e l'Allegato III del Regolamento sull'IA), l'Avvocato potrebbe utilizzare alcune tipologie di sistemi di IA ad alto rischio; per esempio:

- i sistemi di IA destinati a essere utilizzati per il riconoscimento delle emozioni
- i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicare annunci di lavoro mirati, analizzare o filtrare le candidature e valutare i candidati;
- i sistemi di IA destinati a essere utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro.

L'articolo 26 (Obblighi dei deployer dei sistemi di IA ad alto rischio), prevede alcuni obblighi per i deployer di sistemi di IA ad alto rischio; per esempio, i deployer devono:

- adottare "idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi",
- affidare "la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario" e
- conservare "i log generati automaticamente da tale sistema di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo".

L'articolo 50 (Obblighi di trasparenza per i fornitori e i deployers di determinati sistemi di IA) del Regolamento sull'IA prevede alcuni obblighi di trasparenza che si applicano ai deployer. Per esempio, i "deployer di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema e trattano i dati personali in conformità dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680, a seconda dei casi".

Infine, l'articolo 86 (Diritto alla spiegazione dei singoli processi decisionali) prevede che "Qualsiasi persona interessata oggetto di una decisione adottata dal deployer sulla base dell'output di un sistema di IA ad alto rischio [...] e che produca effetti giuridici o in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali ha il diritto di ottenere

dal deployer spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata.".

Gli articoli 25, 26, 50 e 86 saranno in vigore dal 2 agosto 2026.

La Legge sull'IA

La Legge sull'IA all'art. 13, primo comma, prevede che "L'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è finalizzato al solo esercizio delle attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera".

La norma pare estendere all'utilizzo dei sistemi di IA nelle professionali intellettuali, e quindi nell'attività dell'avvocato, il limite posto dal Regolamento sull'IA all'attività di amministrazione della giustizia[15]: si ricorda che al considerando 61 si legge che "L'utilizzo di strumenti di IA può fornire sostegno al potere decisionale dei giudici o all'indipendenza del potere giudiziario, ma non dovrebbe sostituirlo: il processo decisionale finale deve rimanere un'attività a guida umana.".

L'art. 13, secondo comma, della Legge sull'IA prevede che "Per assicurare il rapporto fiduciario tra professionista e cliente, le informazioni relative ai sistemi di intelligenza artificiale utilizzati dal professionista sono comunicate al soggetto destinatario della prestazione intellettuale con linguaggio chiaro, semplice ed esaustivo.". La norma supera il dibattito che si è aperto nei mesi scorsi in ordine alla doverosità di tale informativa: per esempio, ci si domandava perché l'informativa debba essere fornita solo sui sistemi di IA e non, per esempio, sugli altri sistemi digitali utilizzati, che anche possono porre gravi rischi per il cliente.

Si segnala infine che l'art. 24, secondo comma, lettere e) e f), della Legge sull'IA, nell'attribuire al Governo il compito di emanare decreti legislativi per l'adeguamento della normativa nazionale al Regolamento sull'IA, tra gli altri principi e criteri indica i seguenti:

e) previsione di percorsi di alfabetizzazione e formazione in materia di utilizzo dei sistemi di intelligenza artificiale;

[15] Ai sensi dell'Allegato III, punto 8, lettera a), l'uso di sistemi di IA nell'amministrazione della giustizia è considerato ad alto rischio se gli stessi sono "destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie".

f) previsione, da parte degli ordini professionali e delle associazioni di categoria maggiormente rappresentative, nonché da parte delle forme aggregative delle associazioni di cui all'articolo 3 della legge 14 gennaio 2013, n. 4, di percorsi di alfabetizzazione e formazione, per i professionisti e per gli operatori dello specifico settore, all'uso dei sistemi di intelligenza artificiale; previsione della possibilità di riconoscimento di un equo compenso modulabile sulla base delle responsabilità e dei rischi connessi all'uso dei sistemi di intelligenza artificiale".

Si ringraziano i componenti della commissione IA dell'Ordine Avvocati di Torino

Questa è la prima versione d'un lavoro che sarà sviluppato nel tempo: seguiranno aggiornamenti che saranno disponibili alla pagina **https://www.ordineavvocatitorino.it/vademecum%20AI**

ORDINE AVVOCATI DI TORINO