



SENATO DELLA REPUBBLICA

8° E 10° COMMISSIONE (GIUSTIZIA)

*Esame del disegno di legge n. 1146 del 20 maggio 2024 recante
“Disposizioni e delega al Governo in materia di intelligenza artificiale”*

Audizione informale del 9 ottobre 2024

MEMORIA DI OSSERVAZIONI DELLA **A.N.F. ASSOCIAZIONE NAZIONALE FORENSE**

INTRODUZIONE

Ringraziando il Presidente e la Commissione tutta per aver invitato l'**Associazione Nazionale Forense** a partecipare all'audizione informale circa il disegno di legge n. 1146 presentato dal Presidente del Consiglio dei Ministri Giorgia MELONI e dal Ministro della Giustizia Carlo NORDIO, comunicato alla Presidenza il 20 maggio 2024 recante *Disposizioni e delega al Governo in materia di intelligenza artificiale*”, ci permettiamo di svolgere alcune osservazioni seguite da proposte che auspichiamo incontri il favore tecnico e scientifico delle Commissioni.

Le proposte avanzate dall'Associazione Nazionale Forense si pongono nel solco delle posizioni condivise dalla larga parte dell'Avvocatura in tema di intelligenza artificiale nella giurisdizione e nella professione forense, come espresse anche in occasione del XXXV° Congresso Nazionale Forense tenutosi a Lecce il 6, 7 e 8 ottobre 2022, attraverso l'approvazione, da parte della massima assise dell'Avvocatura, della richiesta di adozione di misure per l'utilizzo di strumenti di intelligenza artificiale nel sistema Giustizia con modalità rispettose dei principi e dei valori costituzionali e che garantiscano trasparenza, equità, autonomia e indipendenza della magistratura e di tutti i soggetti coinvolti.

Tra queste, proprio in occasione del Congresso Nazionale Forense, l'Associazione Nazionale Forense ha visto approvare un proprio deliberato congressuale proprio avente ad oggetto il tema dell'intelligenza artificiale, sul quale *infra*.

A ciò aggiungasi che l'Associazione Nazionale Forense ha creato un progetto denominato “Fair PLAI – Professional Legal Artificial Intelligence” (www.fairplai.eu) in collaborazione con la Pontificia Università dell'Antoniano, il Politecnico di Milano, imprese, Ordini e associazioni professionali e di categoria, come laboratorio unico nel suo genere al fine di condividere momenti scientifici, divulgativi, dibattiti sul tema dell'AI applicata alle professioni intellettuali. Allo stato ANF partecipa attivamente anche al Diploma di Alta Specializzazione in materia di Intelligenza Artificiale promosso dalla Pontificia Università dell'Antoniano.

Invero, si è consapevoli che lo sviluppo tecnologico appare maggiormente agile rispetto alla produzione normativa, lenta, al punto che disposizioni aventi ad oggetto tali tecnologie dovrebbero essere oggetto di normative speciali d'urgenza che permettano una costante regolamentazione antropocentrica dei sistemi di IA nei principali settori applicativi, in particolare sanità e giustizia.

Nell'ottica di pronta collaborazione e di sviluppo, le professioni intellettuali, in particolare quella forense, potrebbero essere soggetti attuatori di fasi di sperimentazione del controllo di LLM, al fine di orientarne gli aspetti maggiormente problematici, quali la controllabilità degli output dei sistemi di IA funzionale e generativa.

In tal senso, poi, l'Associazione Nazionale Forense, muovendo dalle suddette posizioni, proprie e condivise con la restante parte dell'avvocatura, propone la “**Carta Etica A.N.F.**”¹, affinché l'emananda disciplina di settore venga radicata nei principi e nei valori costituzionali ed unionali che, oggi, trovano massima espressione nel “Regolamento sull'intelligenza artificiale” (UE) n. 2024/1689 del 13 giugno 2024, c.d. “AI Act”. L'AI Act rappresenta un *corpus* normativo contenente principi giuridici in larga parte inediti, richiedendo, nel tempo, un complesso adattamento interpretativo. È, pertanto, necessario che il Legislatore nazionale tenga conto ciò ed operi, *ab origine*, un coordinamento serrato e sistematico, per evitare di innescare ulteriori problematiche ermeneutiche che potrebbero pregiudicare la certezza del diritto. In questo contesto è imprescindibile lo sviluppo di principi etici finalizzati ad assicurare che i modelli scientifici e matematici si intersechino col diritto in un equilibrio armonico, dove il rispetto dei valori costituzionali della persona siano sempre garantiti. All'uopo, la Carta Etica A.N.F. sancisce i seguenti principi:

1. *Principio del rispetto dei diritti fondamentali;*
2. *Principio di antropocentrismo;*

¹ A cura di Giampaolo Di Marco e Maria Gabriella Saia, e con il contributo di: Paolo Assirelli, Carolina Brunazzetto, Veronica Dettori, Lorenzo Letti, Stefania Migliori, Ingrid Righetti, Guido Rimini, Franco Uggetti.

3. Principio di conoscenza ed uso consapevole dell'intelligenza artificiale;
 4. Principio di lealtà, trasparenza e informazione;
 5. Principio di privacy e cybersecurity;
 6. Principio di responsabilità;
- ritenuti cardini imprescindibili per l'utilizzo dell'IA nel comparto giustizia.

“CARTA ETICA A.N.F.”

1. PRINCIPIO DEL RISPETTO DEI DIRITTI FONDAMENTALI

“L’impiego della I.A. deve avvenire nel pieno rispetto dei diritti fondamentali dell’uomo nelle sue diverse declinazioni, quali: legalità, eticità, rispetto della dignità umana, libertà dell’individuo, rispetto per la democrazia, per la giustizia e il ruolo della legge, eguaglianza, non discriminazione e solidarietà e diritti dei cittadini”.

Questo principio assume varie declinazioni che debbono essere valutate con estremo rigore dall'utilizzatore di un sistema di I.A. e che devono trovare espressa garanzia, da parte del fornitore del medesimo sistema, nel contratto di acquisto e/o di utilizzazione.

Tra le varie declinazioni si riportano di seguito le principali, ritenute imprescindibili nell'utilizzo di sistemi di IA.

Legalità: il sistema di I.A. utilizzato deve rispettare le leggi e i regolamenti in vigore a livello nazionale e sovranazionale. Indispensabile è il rispetto della Carta dei Diritti Fondamentali UE. Pertanto, sarà cura dell'avvocato verificare che i sistemi di I.A. proposti siano stati realizzati nel rispetto della normativa e dei diritti fondamentali dei beneficiari dei servizi, acquisendo e conservando la documentazione dei fornitori.

Eticità: il sistema di I.A. utilizzato deve operare nel rispetto dei principi e dei valori umani.

Rispetto della dignità umana: il sistema di I.A. deve essere realizzato garantendo l'integrità fisica e mentale della persona, sia nei confronti degli utilizzatori che dei beneficiari.

Libertà dell'individuo: i benefici e le opportunità del sistema devono essere facilmente accessibili e frutto di una scelta consapevole da parte degli utilizzatori e dei beneficiari.

Rispetto per la democrazia, per la giustizia e il ruolo della legge: il sistema di I.A. utilizzato deve essere programmato e utilizzato nel rispetto dei principi democratici dell'ordinamento, acquisendo e conservando le attestazioni dei fornitori, anche attraverso specifiche clausole contrattuali.

Eguaglianza, non discriminazione e solidarietà: i sistemi di I.A. utilizzati devono garantire di essere stati realizzati nel rispetto dell'intera popolazione, incluse le persone a rischio di esclusione, e tale circostanza dovrà risultare nel contratto di acquisto.

Diritti dei Cittadini: l'I.A. deve essere a servizio dei beneficiari migliorando l'efficienza della soluzione alle problematiche espresse.

2. PRINCIPIO DELL'ANTROPOCENTRISMO

“L'intelligenza artificiale deve essere una tecnologia antropocentrica, che deve fungere da strumento per migliorare il benessere degli esseri umani”.

Il considerando (6) dell'AI Act afferma che *«In considerazione dell'impatto significativo che l'IA può avere sulla società e della necessità di creare maggiore fiducia, è essenziale che l'IA e il suo quadro normativo siano sviluppati conformemente ai valori dell'Unione sanciti dall'articolo 2 del trattato sull'Unione europea (TUE), ai diritti e alle libertà fondamentali sanciti dai trattati e, conformemente all'articolo 6 TUE, alla Carta. Come prerequisito, l'IA dovrebbe essere una tecnologia antropocentrica. Dovrebbe fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani».*

La tecnologia deve, infatti, mantenere e garantire una natura antropocentrica, il che significa che la mera logica del “funziona oppure no” non può e non deve avere l'ultima parola: il fine ultimo deve invece essere il benessere delle persone. La scelta della soluzione di un problema tecnico non deve essere solamente sotto una chiave funzionale, bensì di benessere per le persone.

Tutto ciò deve esser posto a maggior ragione in luce in un momento nel quale lo sviluppo tecnico e industriale sta mettendo a dura prova la stessa sopravvivenza della biosfera.

Opportunamente, quindi, l'articolo 1 dell'AI ACT afferma che scopo del regolamento è anche quello di *«promuovere un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione».*

Controllo umano, visione antropocentrica, sorveglianza umana (ex art. 14 dell'AI Act) sono aspetti nodali e irrinunciabili, innanzitutto, per l'avvocatura e per tutti i protagonisti della giurisdizione, stante che gli effetti dell'IA verranno a ricadere sulle vite delle persone e sui loro diritti.

Il compito dell'avvocato dovrà quindi essere, dapprima, quello di avviarsi alla conoscenza dei sistemi (attraverso una necessaria alfabetizzazione) e, poi, alla loro verifica e alla loro critica, di modo che venga garantito il “fattore umano” come parametro e canone fondamentale, non negoziabile ed irrinunciabile.

3. PRINCIPIO DI CONOSCENZA ED USO CONSAPEVOLE DELL'INTELLIGENZA ARTIFICIALE

“L’Avvocato deve mantenere una comprensione adeguata ed aggiornata delle tecnologie di Intelligenza Artificiale, garantendo che il loro utilizzo nella pratica legale sia conforme ai principi etici, deontologici e giuridici”.

Con “alfabetizzazione in materia di IA” o “AI Literacy” si intende la capacità di comprendere il funzionamento di base delle intelligenze artificiali. Tale comprensione assume una dimensione anche etica poiché consente all’Avvocato, e all’utente in genere, di farne un uso responsabile e consapevole, valutandone gli impatti sui diritti fondamentali mediante lo sviluppo di capacità di comprensione e valutazione critica.

La definizione giuridica di «alfabetizzazione in materia di IA» è contenuta nell’art. 3, n. 56 dell’AI Act, ed è intesa come: *«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».*

Il suo valore etico è esplicitato nel considerando (20) dell’AI Act, ai sensi del quale: *«Al fine di ottenere i massimi benefici dai sistemi di IA proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza e di consentire il controllo democratico, l’alfabetizzazione in materia di IA dovrebbe dotare i fornitori, i deployer e le persone interessate delle nozioni necessarie per prendere decisioni informate in merito ai sistemi di IA”.*

Nella Carta etica europea sull’utilizzo dell’intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, adottata dalla CEPEJ il 3-4 dicembre 2018, il concetto di alfabetizzazione informatica è invece correlato al “principio del controllo da parte dell’utente”: informazione e conoscenza sono, infatti, gli strumenti attraverso i quali gli utilizzatori possono mantenere autonomia decisionale ed il controllo delle loro scelte.

L’alfabetizzazione in ambito organizzativo: è agevole supporre che, già nei prossimi mesi, assisteremo ad un incremento di prodotti basati sull’intelligenza artificiale espressamente concepiti per lo studio legale: banche dati, gestionali, *tools* di analisi documentale, redattori di bozze di pareri legali e di atti giudiziari.

L’avvocato deve premunirsi di conoscenze utili ad orientarsi in questo mercato per compiere una scelta critica e ponderata su quali prodotti adottare e quali invece scartare, in quanto inadatti a garantire un elevato standard di protezione dei diritti dei clienti.

Sarà opportuno predisporre, anche per l’utilizzo di sistemi non classificabili come ad alto rischio, una check-list ispirata ai requisiti di cui al capo III dell’AI Act, orientandosi verso prodotti:

- sviluppati per garantire un adeguato livello di accuratezza, robustezza e cybersicurezza;

- muniti di adeguata documentazione tecnica;
- che consentano la registrazione automatica dei log;
- addestrati con *dataset* soggetti ad adeguate pratiche di *governance*;
- che favoriscano la sorveglianza umana per tutto il ciclo di vita del sistema;
- che assicurino un appropriato livello di trasparenza.

È, comunque, necessario che l'avvocato sia consapevole che i sistemi di IA sono soggetti ad aggiornamenti e modifiche continue. Il controllo sull'adeguatezza del prodotto scelto deve essere rinnovato ciclicamente per verificare che gli standard richiesti continuino a sussistere. Sarà doverosa a tal fine, l'analisi periodica delle condizioni di utilizzo dei prodotti in uso.

All'interno di studi composti da più professionisti la scelta dei sistemi di IA da adottare dovrebbe essere delegata esclusivamente a soggetti in grado di garantire conoscenze adeguate e non dovrebbe mai essere fondata solo su valutazioni di tipo economico.

L'alfabetizzazione nello svolgimento del mandato professionale: laddove l'avvocato scelga di utilizzare sistemi di IA, deve essere pienamente consapevole che un buon livello di alfabetizzazione ha rilevanti ricadute pratiche anche nell'espletamento del mandato.

Le caratteristiche intrinseche dei sistemi e dei modelli di IA (come i grandi modelli linguistici) comportano per l'avvocato insidie che, nell'ambito di un utilizzo etico della tecnologia, devono essere riconosciute e gestite:

- in relazione alle qualità delle informazioni: i grandi modelli linguistici generalisti ed accessibili gratuitamente utilizzano per la produzione dell'*output* prevalentemente fonti di scarso valore scientifico reperite sul *web*, come i *blog*, e spesso non hanno accesso a *dataset* dall'elevato pregio giuridico, come riviste, manuali, repertori etc.
- in relazione alla correttezza del risultato: i modelli di IA, attualmente, non sono in grado di svolgere un'analisi qualitativa e semantica dei testi ma si affidano solo ad analisi statistiche e probabilistiche. Recentemente una banca dati giuridica specialistica, e quindi alimentata con un *dataset* selezionato, dopo essere stata interrogata sul periodo di sospensione feriale dei termini, ha risposto che lo stesso si conclude il 15 settembre. Se consideriamo che la sospensione dal 1° agosto al 15 settembre ha operato per più anni (dal 1969 al 2015) rispetto a quella di 31 giorni (dal 2015 ad oggi), l'errore potrebbe essere stato determinato dalla prevalenza numerica di sentenze che si riferiscono alla sospensione più lunga.
- in relazione all'affidabilità del risultato: è utile distinguere tra sistemi di IA ad elevata soglia di incertezza e sistemi a bassa soglia di incertezza. I primi sono progettati per produrre risposte anche in mancanza di informazioni sufficienti, tali risposte possono essere altamente plausibili ma non necessariamente veritiere. Il loro funzionamento è alla base delle c.d. "allucinazioni" (*bias*), ossia la

generazione di contenuti inventati. Una delle vittime più note di questo meccanismo è l'avvocato newyorchese sanzionato per avere elaborato le difese del proprio cliente su precedenti inesistenti ed inventati da un sistema di intelligenza artificiale generativa;

- in relazione alla tutela della privacy ed al rispetto del segreto professionale: i modelli di IA continuano ad imparare anche dai dati che ricevono dagli utilizzatori. Questo significa che immettere i dati di un cliente in un grande modello linguistico generalista è pericoloso, illegale e corrisponde alla definitiva perdita di controllo su quelle informazioni. Se l'avvocato non è certo che le banche dati, i *tools* di analisi documentale o redattori di bozze che ha in uso non utilizzino i dati immessi per l'addestramento del modello, dovrebbe procedere sempre ad una preventiva anonimizzazione.

Quanto detto sinora ci porta a fare delle brevi riflessioni anche sul valore delle predizioni dell'IA. In ambito giuridico si parla spesso di giustizia predittiva. Le intelligenze artificiali non sono oracoli. Le predizioni dell'IA sono processi attraverso i quali vengono utilizzati dati passati per fare inferenze o ipotesi su dati futuri o sconosciuti. Si tratta di una funzione certamente interessante in alcuni ambiti, quali la diagnostica medica o la meteorologia. In ambito giuridico la predizione giurisprudenziale ci dice solo che in passato dei giudici si sono espressi più frequentemente in una determinata maniera nella soluzione di casi analoghi. La conoscenza e consapevolezza di questo meccanismo deve indurre il giurista a riflettere sui limiti all'innovazione del diritto che potrebbero derivare dall'uso indiscriminato ed acritico di queste tecnologie, nonché sul rischio di perpetrare all'infinito *bias*, discriminazioni e disuguaglianze.

Ad ogni buon conto l'intelligenza artificiale generativa deve essere "guidata" dall'utilizzatore, mediante la creazione di "*prompt*", ossia domande che vengono poste al LLM in linguaggio naturale. All'aumentare dell'abilità nella creazione e perfezionamento di *prompt* aumenta anche la precisione della risposta. Attualmente, gli avvocati sono abituati all'utilizzo delle banche dati tradizionali che operano mediante ricerca *full text* di parole chiave. Oggi la possibilità di usufruire di nuovi metodi di ricerca impone un cambio di *forma mentis*.

L'alfabetizzazione nei rapporti col cliente: conoscere i meccanismi di base delle intelligenze artificiali pone, infine, l'avvocato nella condizione di spiegare al cliente in modo più efficace come e perché sia stata utilizzata l'IA nell'espletamento della sua pratica. La fiducia del cliente è cruciale, e la trasparenza nell'uso dell'IA è essenziale per mantenere questa fiducia. La consapevolezza e la sicurezza del professionista gioveranno, quindi, al rafforzamento del rapporto fiduciario, infondendo tranquillità nel cliente che potrà percepire l'autorevolezza del professionista, capace di operare con le nuove tecnologie e di assumersene le conseguenti responsabilità.

Il ruolo della formazione continua: per poter cogliere appieno le opportunità dell'IA è necessario ponderarne anche le criticità. Non tutti i rischi, tuttavia, sono insiti nella tecnologia. Sovente è

l'incompetenza dell'utilizzatore a creare il pericolo. Se l'utilizzatore è un avvocato aumenta esponenzialmente anche il rischio di arrecare serie compromissioni dei diritti fondamentali del cliente, tra cui il diritto alla difesa ed il diritto alla protezione dei dati personali. L'avvocato che opera in modo etico deve essere in grado di identificare e mitigare questi rischi. L'uso responsabile delle IA richiede che il professionista acquisisca una adeguata alfabetizzazione e sviluppi competenze specifiche a tutela del Cliente e del buon funzionamento della giustizia. Lo strumento attraverso il quale raggiungere un adeguato livello di consapevolezza e sicurezza è la formazione continua. Sarà, quindi, necessario creare percorsi formativi specifici per sviluppare le conoscenze dell'avvocato ed accrescerne le abilità di utilizzo. Il processo di apprendimento dovrà, inoltre, essere costantemente *in fieri*, poiché l'IA è un campo in rapida ed esponenziale evoluzione e rimanere aggiornati è essenziale per comprenderne i nuovi sviluppi e le implicazioni legali.

4. PRINCIPIO DI LEALTÀ, TRASPARENZA E INFORMAZIONE

“L’Avvocato deve esercitare l’attività professionale con lealtà, trasparenza e informazione. L’uso di sistemi di intelligenza artificiale deve avvenire con la massima cautela e, pertanto, l’avvocato, che nell’esercizio dell’attività professionale utilizza sistemi di intelligenza artificiale, deve informare per iscritto la parte assistita, all’atto dell’assunzione dell’incarico, circa l’utilizzo di tali sistemi, il livello di complessità e funzionamento degli stessi, fornendo tutte le informazioni utili circa il loro uso, e garantendo la riservatezza e la non utilizzabilità da parte degli stessi sistemi dei loro dati personali e sensibili”.

Nell'affrontare con coraggio la sfida che pongono i sistemi di intelligenza artificiale alla professione di avvocato non è possibile sottovalutare l'obbligo di agire con lealtà e nel rispetto dei doveri imposti dal codice deontologico forense.

I doveri di probità, dignità, decoro ed indipendenza sanciti dall'articolo 9 del codice deontologico forense coniugati con il dovere di diligenza costituiscono i principali punti di riferimento del modo in cui l'attività dell'avvocato deve essere esercitata.

L'avvocato deve, infatti, esercitare l'attività professionale con indipendenza, lealtà e correttezza.

Sicuramente “un rapporto fiduciario, quale è quello che lega l'avvocato al suo cliente non può tollerare alcun comportamento che violi un aspetto essenziale della “fiducia”, consistente nella completezza e verità delle informazioni destinate all'assistito” come ha ricordato più volte il Consiglio Nazionale Forense in numerose decisioni in procedimenti disciplinari.

Parimenti nei rapporti con i colleghi e con i magistrati, l'avvocato è tenuto a conformarsi a questi principi.

L'utilizzo di sistemi di intelligenza artificiale dovrà perciò avvenire con la massima cautela, nel senso che chi intende servirsene dovrà conoscere adeguatamente i rischi, le enormi potenzialità, i limiti, ed anche la rapidità che contraddistinguono questi sistemi. La conoscenza specifica di tali sistemi dovrebbe essere imprescindibile così da non poter permettere il suo uso senza una preparazione. Per queste ragioni si ritiene cruciale l'obbligo di utilizzare questi sistemi chiarendo ai propri clienti che se ne potrà far uso, chiarendo altresì ai colleghi che si potrà far uso di questi sistemi, chiarendo anche ai magistrati che se ne può fare uso.

Considerando il rilievo sociale della figura dell'avvocato e l'alto valore costituzionale affidato alla difesa tecnica e la possibile trasformazione che l'uso di sistemi di IA recherà alla professione si rende necessario l'osservanza di un dovere formativo prima di utilizzare questi sistemi più avanzati e l'obbligo di comunicare che si farà uso di specifici sistemi di IA. Tali obblighi potrebbero essere sintetizzati nei principi di trasparenza e informazione.

Nel rispetto del principio di trasparenza, l'avvocato, che nell'esercizio dell'attività professionale utilizzi sistemi di intelligenza artificiale, deve informare per iscritto la parte assistita, all'atto dell'assunzione dell'incarico, circa l'utilizzo di tali sistemi, il livello di complessità e funzionamento degli stessi, fornendo tutte le informazioni utili circa il loro uso (e garantendo la riservatezza e la non utilizzabilità da parte degli stessi sistemi dei loro dati personali e sensibili).

Prima di adottare qualsiasi sistema di intelligenza artificiale l'avvocato è tenuto a verificare il rispetto del dovere di segretezza e riservatezza imposto dall'art. 13 del Codice Deontologico Forense, che concretamente si traduce nel non diffondere né comunicare a terzi i dati dei clienti.

Ed ancora, l'utilizzo di sistemi di I.A. deve avvenire in modo trasparente, privo di indicazioni ingannevoli nei confronti dei beneficiari dei servizi sia per quanto riguarda i risultati ottenuti e/o promessi che in materia di sostenibilità anche ambientale del servizio offerto. In particolar modo l'attenzione dello studio legale deve essere rivolta al rispetto dei seguenti canoni:

Pratiche commerciali corrette: la promozione e la vendita dei servizi offerti dovranno avvenire in modo chiaro, corretto, leale, non aggressivo ma rispettoso della diligenza professionale e degli obblighi deontologici di modo da non sfalsare il comportamento del cliente e il suo processo decisionale. La politica pubblicitaria deve essere veritiera, leale e corretta nel rispetto della legge e degli obblighi deontologici. È vietata qualsiasi forma di pubblicità subliminale.

Non si potranno utilizzare sistemi di I.A. per la promozione dei servizi offerti che abbiano elevate capacità persuasive, che rendano i potenziali clienti vulnerabili o tali da ingenerare un abuso di posizione dominante sul mercato o gettare discredito sui concorrenti.

Dovranno essere evitate pratiche commerciali di pricing, attraverso sistemi di monitoraggio, che acquisiscano i prezzi praticati dalle imprese concorrenti per ricalcolare e aggiornare i prezzi dei servizi, ed essere così di ostacolo alla libera concorrenza o alla scelta consapevole dei consumatori.

Divieto di profilazione automatica: Dovranno essere evitate politiche di profilazione automatica dei clienti attraverso i sistemi di I.A. contenuti nei siti dello studio o utilizzati per la fornitura dei servizi.

5. PRINCIPIO DI PRIVACY E CYBERSECURITY

“L’intelligenza artificiale deve rispettare la riservatezza e la protezione dei dati personali e, in base al principio di minimizzazione, l’avvocato deve utilizzare sistemi di IA che forniscano sufficienti garanzie, inserendo dati adeguati, pertinenti e limitati a quanto strettamente necessario per le finalità perseguite. Ove possibile li dovrà anonimizzare. L’Avvocato – qualunque sia la dimensione dello studio nel quale opera – è chiamato a prestare particolare attenzione alle misure di sicurezza informatiche, sia sul piano software che su quello hardware (infrastrutturale), considerando che anche lavorando da soli è probabile che, anche inconsapevolmente, si usino (o si useranno nel prossimo futuro) apps, programmi o piattaforme che utilizzano sistemi di intelligenza artificiale”.

L’intelligenza artificiale, secondo l’AI Act, deve rispettare i principi posti dalla Carta dei Diritti Fondamentali dell’Unione Europea, tra i quali (artt. 7 e 8 della Carta) il diritto al rispetto della vita privata (e quindi alla riservatezza) ed alla protezione dei dati personali. In quest’ottica di inserisce il Regolamento 2016/679 (GDPR) in materia di trattamento dei dati personali, normativa che dà attuazione ai suddetti diritti fondamentali: si potrebbe dire che i due Regolamenti si pongono in rapporto di complementarità.

Entrambe le leggi si concentrano sulle finalità del trattamento dei dati personali, sull’utilizzo del sistema di IA, sull’approccio *by design*; entrambe richiedono che gli indirizzi del Regolamento identifichino i rischi per i diritti fondamentali.

Oltre a richiamare i principi del GDPR, l’AI Act fa riferimento agli *“Orientamenti etici per un’AI affidabile”* elaborati nel 2019 dall’High-Level Expert Group on Artificial Intelligence (AI HLEG) della Commissione Europea.

Tali orientamenti fanno riferimento a sette principi etici volti a garantire l’elaborazione di una IA in linea con la Carta e con i valori su cui si fonda l’UE. I principi etici, che guidano l’interpretazione delle disposizioni dell’AI Act, sono i principi di *intervento e sorveglianza umana, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione, equità, benessere sociale e ambientale e accountability*.

Vi è un espresso richiamo al GDPR in numerosi “considerando” ed articoli dell’AI Act, specie in quelli che trattano la materia nell’ambito del rispetto dei diritti fondamentali.

Non va poi dimenticata la disposizione del GDPR (art. 22) che sancisce il diritto dell’interessato a non essere soggetto ad una decisione basata unicamente su di un trattamento automatizzato, quale quello dell’IA, che abbia il potere di produrre effetti giuridicamente rilevanti sulla sua sfera di vita.

La norma vieta quindi l’adozione di decisioni prese senza il coinvolgimento di un essere umano che possano influenzare e modificare la sua autorità o competenza.

Il primo problema che si pone per l’uso pratico dell’IA in un contesto professionale è l’inserimento, tra i soggetti che fanno parte di un normale rapporto *privacy* (titolare, interessato e terze parti), tutti con ruoli, diritti ed obblighi ben definiti, di un soggetto senziente non umano (l’IA), capace di utilizzare autonomamente i dati ottenuti.

Il trattamento dei dati personali tramite IA deve avere una finalità ben definita, chiara e legittima, identificata sin dall’inizio. I dati raccolti non devono essere elaborati ulteriormente in modo incompatibile con lo scopo originario, in accordo con i principi di trasparenza, minimizzazione dei dati e limitazione della conservazione previsti dal GDPR.

Un sistema di IA però, nel processo di adattamento all’ambiente e quindi di modifica dei suoi comportamenti, potrebbe autonomamente cambiare tali finalità.

Ulteriore criticità è data dal fatto che l’interessato può liberamente decidere quali dati personali condividere o meno, con chi e in che modo; i dispositivi con IA, però, a partire dai dati forniti, sono in grado di dedurre molte altre informazioni, comprese quelle strettamente personali e che magari l’utente non intendeva condividere. Inoltre, il consenso al trattamento riguarda solo i dati oggetto dell’informativa, e non altri che potrebbero essere condivisi in futuro.

Una criticità, allo stato attuale (nelle more della piena attuazione dell’AI Act), dei sistemi di IA è che non è possibile garantire (quantomeno integralmente) agli interessati le tutele previste dal GDPR (art. 15-22) in relazione al trattamento dei dati personali per quanto riguarda il diritto di accesso, alla rettifica, alla cancellazione, alla limitazione, all’opposizione ed al trattamento dei medesimi mediante processi automatizzati. Una volta, infatti, che i dati personali siano stati immessi in un sistema di IA, governato dagli algoritmi, di fatto non sarebbe possibile (neppure per il programmatore) modificare i dati stessi che siano divenuti parte di un *dataset* ed utilizzati in un numero quasi infinito di combinazioni.

Alla luce di quanto sopra, l’avvocato, nel momento in cui utilizzerà dei dati personali del proprio assistito immettendoli in un sistema di IA, dovrà fornire preventiva informazione di tale trattamento all’interessato (inserendolo altresì nel proprio Registro del Titolare) e dovrà porsi il problema dell’uso successivo che di tali dati verrà fatto dal sistema, chi effettivamente li tratterà, dove verranno

conservati e per quanto tempo. Si tratta di aspetti relevantissimi, parzialmente coperti dal GDPR, ma che richiedono una particolare competenza del professionista in ordine alle conseguenze che potrebbe avere la “semplice” immissione dei dati personali in un sistema di IA.

Prudentemente, ed in base al principio di minimizzazione, l’avvocato dovrà utilizzare un sistema di IA che fornisca sufficienti garanzie, inserendo dati adeguati, pertinenti e limitati a quanto strettamente necessario per le finalità perseguite. Ove possibile li dovrà anonimizzare.

L’AI Act: un nuovo strumento di protezione dagli attacchi informatici.

Per quanto attiene al lato *Cybersecurity*, l’AI Act dell’UE mira a stabilire un quadro normativo completo per un uso sicuro dell’IA nell’Unione Europea, con particolare riguardo a come i sistemi di IA possano essere sfruttati o come le vulnerabilità all’interno dei modelli di IA possano rappresentare minacce alla sicurezza.

Quindi, sebbene l’AI Act si concentri principalmente sulla regolamentazione dell’intelligenza artificiale, alcuni articoli e considerando fanno riferimento a considerazioni specifiche sulla sicurezza e sulla protezione da rischi legati alla cybersecurity.

La prima norma in tale direzione è sicuramente l’articolo 9 (*Requisiti per la qualità dei dati*) che affronta l’importanza della qualità dei dati utilizzati per addestrare i sistemi di intelligenza artificiale. La sicurezza dei dati, e quindi la loro protezione contro manipolazioni e violazioni, è cruciale per garantire che gli algoritmi non siano compromessi, rappresentando un fattore chiave per la sicurezza informatica.

L’AI Act stabilisce delle regole chiare per chi crea **e utilizza l'intelligenza artificiale**, l’obiettivo è far sì che i sistemi di AI siano sicuri e protetti dagli attacchi hacker, contrastando e mitigando il rischio di infiltrazioni/esfiltrazioni illegali nel sistema, *databreachs* di dati sensibili, ecc.

L’articolo 23 (*Resilienza agli attacchi*) richiede appunto che i sistemi di intelligenza artificiale - in particolare quelli ad alto rischio - siano progettati e sviluppati in modo da garantire un livello appropriato di sicurezza contro attacchi intenzionali che potrebbero compromettere la sicurezza o causare danni significativi.

L’AI Act impone quindi che i sistemi di IA siano costruiti in modo sicuro e affidabile, dividendo i sistemi di IA in diverse categorie, a seconda del rischio che rappresentano.

Per esempio, un sistema che decide chi assumere in un’azienda o uno studio legale è considerato a rischio più alto di uno che semplicemente risponde alle domande degli utenti/clienti. Per ogni categoria, ci sono delle regole specifiche da seguire.

L’articolo 15 richiede ai fornitori di sistemi di intelligenza artificiale - ad alto rischio - di implementare un sistema di gestione che consideri i rischi per la sicurezza e includa misure per mitigare le criticità legate alla sicurezza informatica.

Nel contesto della sicurezza informatica, l'AI Act sottolinea l'importanza di adottare solide misure di protezione, inclusa la salvaguardia dei dati e dei sistemi utilizzati nelle operazioni di IA. Poiché le aziende integrano sempre più l'IA generativa nei loro modelli di business, il regolamento impone l'implementazione di misure di sicurezza, come il monitoraggio delle inferenze dei modelli, la gestione sicura dei dati e la protezione delle infrastrutture.

L'AI Act promuove pertanto un approccio di governance orientato alla sicurezza, richiedendo alle organizzazioni e agli studi professionali di integrare strategie di rischio e conformità per proteggere l'intero flusso di valore dell'IA.

Le minacce emergenti nel panorama dell'IA - l'iniezione di *prompt*, gli attacchi di inversione e l'esfiltrazione di dati - obbligano le organizzazioni ad aggiornare i loro modelli di rischio e i piani di risposta agli incidenti, assicurando che l'infrastruttura di sicurezza e i protocolli di governance evolvano insieme ai progressi della tecnologia IA.

È bene evidenziare che l'AI Act dell'UE mira a proteggere non solo i diritti e la *privacy* degli individui, ma anche a garantire che le aziende e gli studi professionali adottino adeguati standard di *cybersecurity* per mitigare i rischi associati all'IA, da qui la necessità di anticipare nuove vulnerabilità e garantire che i sistemi di sicurezza siano progettati per affrontare tali minacce in modo proattivo.

Le organizzazioni che utilizzano l'IA devono quindi dimostrare che la sicurezza e la conformità normativa dei sistemi di IA utilizzati. In particolare l'Allegato IV (*Documentazione tecnica*) richiede che la documentazione tecnica fornita per i sistemi di IA includa informazioni dettagliate sulle misure di sicurezza implementate, tra cui quelle relative alla *cybersecurity*, per garantire che i sistemi siano sicuri e resilienti. I punti chiave per dimostrare la conformità all'AI Act possono essere così individuati, allo stato attuale:

1. Valutazione del rischio.

- Identificazione di tutti i sistemi di IA utilizzati in azienda e loro classificazione in base al livello di rischio che presentano per i diritti fondamentali o la sicurezza delle persone.
- Analisi delle vulnerabilità di ogni sistema per individuare eventuali punti deboli che potrebbero essere sfruttati da attacchi informatici.

2. Documentazione dettagliata.

- Tenere un Registro completo di tutti i sistemi IA utilizzati, specificando le loro caratteristiche, i dati utilizzati e le finalità.
- Adottare procedure di sviluppo e manutenzione, documentando tutte le fasi di sviluppo e manutenzione dei sistemi IA, inclusi i test di sicurezza effettuati.
- Documentare le valutazioni del rischio effettuate per ogni sistema, indicando le misure di mitigazione adottate.

3. Misure di sicurezza.

- Implementare le misure di sicurezza adeguate a proteggere i dati utilizzati dai sistemi IA, in conformità con il GDPR.
- Attuare un continuo Monitoraggio dei sistemi IA per individuare eventuali anomalie o tentativi di intrusione. L'articolo 32 (Vigilanza del mercato) si concentra sulla vigilanza post-mercato, assicurandosi che i sistemi continuino a essere monitorati per eventuali vulnerabilità di sicurezza, compresi rischi informatici.
- Mantenere costantemente aggiornati i sistemi IA e le relative librerie *software* per correggere eventuali vulnerabilità.

4. Trasparenza.

- Informare gli utenti fornendo loro informazioni chiare e comprensibili sul funzionamento dei sistemi IA con cui interagiscono.
- Assicurare che i sistemi IA siano in grado di spiegare le loro decisioni, in particolare per i sistemi ad alto rischio.

5. Cooperazione con le autorità.

- Collaborare con le autorità di controllo competenti a garantire la conformità dei requisiti dei sistemi IA con le norme dell'AI Act.
- Partecipare a iniziative di settore, a gruppi di lavoro volti a definire *standard* e *best practices* per la sicurezza dell'IA.

6. Strumenti utili per dimostrare la conformità.

- Una valutazione dell'impatto sulla protezione dei dati (*Data Protection Impact Assessment* o DPIA) è essenziale per identificare i rischi associati all'utilizzo dei dati personali nei sistemi IA.
- Una valutazione del rischio (*Risk assessment*) permette di identificare le vulnerabilità e le minacce potenziali.
- Un approccio *Privacy by design* che permetta la protezione dei dati fin dalle prime fasi di progettazione di un sistema IA.

Dimostrando in modo chiaro la conformità del proprio sistema IA, le organizzazioni eviteranno il rischio di vedersi comminare le sanzioni economiche - molto elevate - previste dalla legge, al contempo tale impegno verso la sicurezza e la *privacy* dei dati ne protegge la reputazione e aumenta la fiducia degli utenti/clienti che saranno più propensi a utilizzare i prodotti e i servizi di un'azienda o di uno studio professionale che dimostrino di rispettare le normative in materia di IA.

L'Avvocato – qualunque sia la dimensione dello studio nel quale opera – è quindi chiamato a prestare particolare attenzione alle misure di sicurezza informatiche, sia sul piano *software* che su quello

hardware (infrastrutturale) dovendosi considerare che anche lavorando da soli è probabile che, anche inconsapevolmente, si usino (o si useranno nel prossimo futuro) *apps*, programmi o piattaforme che utilizzano sistemi di intelligenza artificiale.

Attenzione che dovrà essere circolare richiedendo una revisione dei modelli di contratto di patrocinio, di informativa *privacy* di procedure specifiche da far adottare a chiunque lavori/collabori nello studio. Revisione che inoltre non potrà più essere fatta una *tantum* e poi destinata all'eternità, ma che richiederà una costante ed accurata attività di evoluzione, di aggiornamento, di manutenzione.

6. PRINCIPIO DI RESPONSABILITA'

“Nel rispetto dei diritti fondamentali, della sicurezza e della dignità umana, gli avvocati, quali “deployer” di sistemi di IA, devono sempre garantire che tali sistemi siano sicuri, affidabili e conformi alle leggi e ai principi etici, adottando tutte le misure necessarie per la prevenzione di danni di qualsiasi natura”.

In ambito di sistemi di IA “forti” si discute sull'opportunità di attribuire loro soggettività giuridica, ovvero di riconoscere ai “robot” la capacità di essere titolari di diritti e di doveri.

L'Unione Europea ha già provato ad occuparsi della questione, anche se non ha trovato il favore di molti.

In particolare, il Parlamento Europeo è intervenuto in passato con la Risoluzione del 16 febbraio 2017, recante *“raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL))”*², sul presupposto che i robot sono oggi in grado di sviluppare una determinata autonomia e capacità cognitiva, quali ad esempio quella di apprendere dall'esperienza, di prendere decisioni quasi autonomamente, così da rendersi sempre più simili ad agenti che si relazionano con l'ambiente circostante, con la possibilità anche di manipolarlo significativamente, diventando, così, essenziale la questione della responsabilità giuridica dell'azione dannosa dei robot.

Il medesimo Parlamento, invero, ritenendo che *«la responsabilità civile per i danni causati dai robot sia una questione fondamentale che deve essere altresì analizzata e affrontata a livello di Unione al fine di garantire il medesimo livello di efficienza, trasparenza e coerenza nell'attuazione della certezza giuridica in tutta l'Unione europea nell'interesse tanto dei cittadini e dei consumatori quanto delle imprese»*³, chiedeva alla Commissione di presentare una proposta di atto legislativo in ordine alle questioni giuridiche in materia di sviluppo e utilizzo della robotica e dell'intelligenza artificiale prevedibili nei successivi 10-15 anni, unitamente ad atti non legislativi, quali linee guida e codici di

² Fonte: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_IT.html#title1.

³ Cfr. punto n. 49 della Risoluzione del Parlamento Europeo del 16 febbraio 2017, in https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_IT.html#title1.

condotta; e che detto atto legislativo - a prescindere dalla soluzione giuridica ritenuta applicabile alla responsabilità civile per i danni causati dai robot in casi diversi da quelli di danni alle cose - non avrebbe dovuto in alcun modo limitare il tipo o l'entità dei danni da risarcire, né avrebbe dovuto limitare le forme di risarcimento da offrire alla parte lesa per il semplice fatto che il danno fosse provocato da un soggetto non umano.

Infine, il medesimo Parlamento invitava la Commissione a valutare, tra le soluzioni giuridiche possibili, *«l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente **il riconoscimento della personalità elettronica dei robot** che prendono decisioni autonome o che interagiscono in modo indipendente con terzi»*⁴.

Come prima accennato, la soluzione prospettata dal Parlamento Europeo, in merito alla costituzione di un *tertium genus* titolare di personalità elettronica, ad oggi non ha avuto seguito, forse perché il contesto sociale non ha ancora maturato quella sensibilità che gli consenta di mettere sullo stesso piano l'intelligenza artificiale autonoma con quella naturale⁵.

A tal proposito, infatti, il “Regolamento sull'intelligenza artificiale” (UE) 2024/1689 del 13 giugno 2024, contenente il quadro normativo sull'intelligenza artificiale, non ha previsto l'introduzione dell'istituto della persona elettronica.

Più in particolare, la Commissione è intervenuta a introdurre delle disposizioni per le azioni di responsabilità civile da esperire soltanto nei confronti delle persone fisiche o giuridiche, quali operatori di sistemi di intelligenza artificiale, qualora detti sistemi cagionino pregiudizio alla vita, alla salute, all'integrità fisica di una persona fisica, ovvero al patrimonio di persone fisiche che giuridiche.

Pertanto, ha previsto una classificazione dei sistemi di intelligenza artificiale sulla scorta del potenziale livello di rischio: più autonomo è un sistema, maggiore sarà il grado di rischio che lo stesso possa causare danni o pregiudizi in maniera casuale. Ad ogni livello di rischio corrisponderà, dunque, uno specifico grado di responsabilità.

Gli operatori di sistemi ad alto rischio⁶ saranno ritenuti oggettivamente responsabili per qualsiasi danno o pregiudizio causati dalle attività, dispositivi, processi derivanti dai sistemi di intelligenza artificiale, e non potranno sottrarsi dalla loro responsabilità sostenendo di avere agito con la dovuta

⁴ Cfr. punto n. 59, lett. f) cit. Risoluzione.

⁵ Cfr. M.G. SAIA, *La soggettività giuridica dei robot*, Rassegna degli avvocati italiani, Newsletter 24 Ore Professionale in coll. con Associazione Nazionale Forense, Il Sole 24 Ore S.p.A., n. 2, marzo 2023, pp. 57-60.

⁶ Cfr. Capo III “Sistemi di IA ad alto rischio” dell'AI Act. In particolare, l'art. 6, comma 5, prevede che «Dopo aver consultato il consiglio europeo per l'intelligenza artificiale («consiglio per l'IA»), e dentro il 2 febbraio 2026, la Commissione fornisce orientamenti che specificano l'attuazione pratica del presente articolo in linea con l'articolo 96, **insieme a un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio**».

diligenza o che derivi dall'autonomia del sistema, salvo che nei soli casi in cui il danno o il pregiudizio derivi da causa di forza maggiore.

E' importante ricordare come gli "Orientamenti etici per un'IA affidabile", fondati sui diritti fondamentali e riflessi in sette principi etici (non vincolanti), elaborati per garantire l'eticità e la robustezza dell'IA, abbiano ricompreso quello relativo alla "responsabilità" ("accountability")⁷, ritenendo che *«L'uso nella nostra società dei sistemi di IA, come di qualsiasi tecnologia potente, pone vari problemi etici, ad esempio in merito al loro effetto sulle persone e sulla società, sulle capacità decisionali e sull'incolumità. Se ricorreremo sempre di più all'assistenza dei sistemi di IA o se delegheremo loro le decisioni dobbiamo essere certi, tramite adeguati processi di accountability, che gli effetti di tali sistemi sulla vita delle persone siano equi, che rispettino valori intransigibili e che siano in grado di agire di conseguenza»*⁸.

Tale principio, infatti, è strettamente connesso a quello di equità e, pertanto, all'uopo di assicurarne il conseguimento è previsto che si debbano adottare dei meccanismi che garantiscano "l'accountability" dei sistemi di IA e dei loro risultati, e dunque sia prima che dopo la loro attuazione. Detto altrimenti, si dovrà avere la possibilità di verificare, e quindi di valutare gli algoritmi, i dati e i processi di progettazione, per poter riferire in ordine ad azioni o decisioni che hanno condotto ad un determinato risultato del sistema, ma anche per poter rispondere delle conseguenze di tale risultato, in caso di ingiusti effetti negativi⁹.

Il legislatore dell'AI Act, ritenendo che tali orientamenti contribuiscono all'elaborazione di un'IA coerente, affidabile e antropocentrica, in linea con la Carta dei diritti fondamentali dell'Unione europea e con i valori su cui si fonda la medesima Unione e che, pertanto, i sette principi dovrebbero trovare applicazione nella progettazione e nell'utilizzo di modelli di IA, fungendo da base per l'elaborazione di codici di condotta a norma del medesimo regolamento¹⁰, ha così previsto che qualunque persona, definita come «fornitore»¹¹, si deve assumere la responsabilità dell'immissione

⁷ Gli "Orientamenti etici per un'IA affidabile" sono stati elaborati nel 2019 da un Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale (istituito dalla Commissione europea nel giugno 2018), al fine di contribuire e garantire l'affidabilità e la validità etica dell'IA, e comprendono sette principi etici non vincolanti, tra i quali: 1) intervento e sorveglianza umani, 2) robustezza tecnica e sicurezza, 3) riservatezza e governance dei dati, 4) trasparenza, 5) diversità, non discriminazione ed equità, 6) benessere sociale e ambientale e 7) accountability; cfr. Commissione europea, Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie, Orientamenti etici per un'IA affidabile, Ufficio delle pubblicazioni, 2019, <https://data.europa.eu/doi/10.2759/640340>. Cfr. anche considerando (27) dell'AI Act.

⁸ Paragrafo (34), *op. ult. cit.*, p. 13.

⁹ Cfr. *op. ult. cit.*, p. 26.

¹⁰ Cfr. considerando (27) dell'AI Act.

¹¹ Art. 3, comma 1, n. 3), AI Act definisce «fornitore»: *una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito».*

sul mercato o della messa in servizio di un sistema di IA ad alto rischio, a prescindere dal fatto che tale persona sia la stessa che abbia progettato o sviluppato il sistema¹².

Sulla scorta di tale assunto e considerata la natura dei sistemi di IA e dei possibili rischi per la sicurezza e i diritti fondamentali associati al loro utilizzo, il medesimo legislatore dell'AI Act ha ritenuto opportuno stabilire delle responsabilità specifiche per i «*deployer*», intesi come: *«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»*¹³.

Ne discende, pertanto, che potrà essere considerato un “*deployer*” anche l’avvocato che utilizza sistemi di IA nell’esercizio della propria attività professionale.

Più in particolare, nel considerando (91) dell'AI Act è prevista l'opportunità per i *deployer* di adottare misure tecniche e organizzative adeguate affinché i sistemi di IA ad alto rischio vengano utilizzati secondo le istruzioni per l'uso, e che prevedano alcuni obblighi di monitoraggio del loro funzionamento e di conservazione delle registrazioni, a seconda dei casi¹⁴. Ed ancora, è prevista l'opportunità per i *deployer* di garantire che le persone alle quali è affidata l'attuazione delle istruzioni per l'uso e della sorveglianza umana dispongano delle competenze necessarie, in particolare un livello adeguato di alfabetizzazione, formazione e autorità in materia di IA per svolgere adeguatamente tali compiti¹⁵.

Alla luce delle superiori argomentazioni, è possibile ritenere che gli avvocati, quali “*deployer*” di sistemi di IA, devono sempre garantire che tali sistemi siano sicuri, affidabili e conformi alle leggi e ai principi etici, adottando tutte le misure necessarie per la prevenzione di danni di qualsiasi natura.

.*.

Sulla scorta dei superiori principi, nonché del Deliberato congressuale n. 85 proposto dall'Associazione Nazionale Forense in seno al XXXV° Congresso Nazionale Forense (Lecce 6-8 ottobre 2022), con il quale si è impegnato l'Organismo Congressuale Forense a dare attuazione al

¹² Cfr. considerando (79) dell'AI Act.

¹³ Art. 3, comma 1, n. 4), AI Act.

¹⁴ L'art. 26 dell'AI Act detta la disciplina in materia di “*Obblighi dei deployer dei sistemi di IA ad alto rischio*”. Cfr. anche Sezione III “*Obblighi dei fornitori e dei deployer dei sistemi di IA ad alto rischio e di altre parti*”, capo III dell'AI Act, artt. 16 e ss. Più in particolare, l'art. 25, comma 1, stabilisce che: «*1. Qualsiasi distributore, importatore, deployer o altro terzo è considerato fornitore di un sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetto agli obblighi del fornitore a norma dell'articolo 16, nelle circostanze seguenti: a) se appone il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi al riguardo; b) se apporta una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o già messo in servizio in modo tale che resti un sistema di IA ad alto rischio a norma dell'articolo 6; c) se modifica la finalità prevista di un sistema di IA, anche un sistema per finalità generali, che non è stato classificato come ad alto rischio e che è già stato immesso sul mercato o messo in servizio in modo tale che il sistema di IA interessato diventi un sistema di IA ad alto rischio a norma dell'articolo 6*».

¹⁵ Cfr. considerando (91) dell'AI Act.

citato deliberato e a «porre in essere ogni necessaria ed opportuna iniziativa volta a favorire l'adozione, da parte degli organi istituzionali nazionali e sovranazionali politici e forensi, di misure che nello sviluppo dei sistemi di intelligenza artificiale nel sistema Giustizia siano rispettose dei principi e dei valori costituzionali e che garantiscano altresì trasparenza, equità, autonomia ed indipendenza della magistratura e di tutti i soggetti coinvolti nell'applicazione della stessa nel sistema Giustizia, dando ove necessario seguito ad interventi a favore della professione forense in termini organizzativi e di rapporti con quest'ultima», nell'odierna sede di audizione, l'Associazione Nazionale Forense intende formulare le seguenti **proposte di integrazione e/o di modifica del disegno di legge n. 1146**¹⁶.

Nella tabella che segue si sintetizzano le principali proposte di modifica.

INDICE DELLA PROPOSTE DI INTEGRAZIONE E CORREZIONE AL DISEGNO DI LEGGE N. 1146	
Art. 4, c. 3	Esplicitare la tutela della facoltà di opposizione che deve essere garantita senza alcun tipo di automatismo del consenso
Art. 4, c. 4	Escludere l'accesso ai sistemi di IA da parte dei minori di anni sedici privi del consenso degli esercenti la responsabilità genitoriale
Art. 7, c. 3 e 5	Assicurare il consapevole coinvolgimento del paziente, che deve essere adeguatamente informato in ogni scelta dell'esercente la professione medica. Evitare l'insorgere di fenomeni di medicina difensiva in relazione all'utilizzo di sistemi di IA
Art. 12, c. 1	Definire il concetto di attività strumentale
Art. 12, c. 1-bis	Estendere l'ambito applicativo della norma anche a soggetti non appartenenti alle professioni intellettuali
Art. 12, c. 3	Prevedere l'applicazione di una sanzione pecuniaria in caso di violazione dell'obbligo di comunicazione
Art. 14, c. 1	Prevedere una compiuta disciplina per l'impiego dell'IA nel settore giustizia, stabilendo dettagliatamente i confini e le modalità specifiche di utilizzo dell'IA; fornire l'esatta definizione dell'espressione " <i>semplificazione del lavoro giudiziario</i> "; espungere l'apposita delega conferita al Ministero della giustizia e ai diversi ordinamenti
Art. 14, c. 2	Prevedere l'esclusività in capo al magistrato della decisione
Art. 22, c. 2, lett. c)	Estendere l'opportunità formativa anche alle associazioni di categoria maggiormente rappresentative
Art. 22, c. 5, lett. a)	Estendere anche in ambito tributario la previsione di strumenti, anche cautelari, finalizzati ad inibire la diffusione e a rimuovere contenuti generati illecitamente
Art. 22, c. 5, lett. b) e c)	Espungere la delega in ambito penale. In via subordinata, espungere il carattere "professionale" dell'utilizzo di sistemi di IA

¹⁶ A cura di Giampaolo Di Marco e Maria Gabriella Saia, e con il contributo di: Paolo Assirelli, Veronica Dettori, Lorenzo Letti, Stefania Migliori, Ingrid Righetti, Guido Rimini, Franco Uggetti.

Art. 22, c. 5, lett. d)	Espungere la delega per la revisione della normativa sostanziale e processuale vigente
Art. 25, c. 1, lett. a)	Eliminare il termine insidioso e mantenere l'aggravante nel caso di commissione del reato mediante l'uso di un sistema di IA

. * .

PRINCIPI IN MATERIA DI INFORMAZIONE E DI RISERVATEZZA DEI DATI PERSONALI

<i>Proposta di modifica</i>	
Art. 4 <i>(Principi in materia di informazione e di riservatezza dei dati personali)</i> <u>comma 1</u> L'utilizzo di sistemi di intelligenza artificiale nell'informazione avviene senza recare pregiudizio alla libertà e al pluralismo dei mezzi di comunicazione, alla libertà di espressione e all'obiettività, completezza, imparzialità e lealtà dell'informazione. <u>comma 2</u> 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 con il diritto dell'Unione Europea in materia di dati personali. <u>comma 3</u> Le informazioni e le comunicazioni relative al trattamento dei dati connesse all'utilizzo di sistemi di intelligenza artificiale avvengono con linguaggio chiaro e semplice, in modo da garantire all'utente la piena conoscibilità e la facoltà di opporsi ai trattamenti non corretti dei propri dati personali. <u>comma 4</u> L'accesso alle tecnologie di intelligenza	Art. 4 <i>(Principi in materia di informazione e di riservatezza dei dati personali)</i> <u>comma 1</u> L'utilizzo di sistemi di intelligenza artificiale nell'informazione avviene senza recare pregiudizio alla libertà e al pluralismo dei mezzi di comunicazione, alla libertà di espressione e all'obiettività, completezza, imparzialità e lealtà dell'informazione. <u>comma 2</u> 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 con il diritto dell'Unione Europea in materia di dati personali. <u>comma 3</u> Le informazioni e le comunicazioni relative al trattamento dei dati connesse all'utilizzo di sistemi di intelligenza artificiale avvengono con linguaggio chiaro e semplice, in modo da garantire all'utente la piena conoscibilità e la facoltà di opporsi esplicitamente ai trattamenti non corretti dei propri dati personali. <u>comma 4</u> L'accesso alle tecnologie di intelligenza

artificiale dei minori di anni quattordici richiede il consenso di chi esercita la responsabilità genitoriale. Il minore degli anni diciotto, che abbia compiuto quattordici anni, può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili.	artificiale dei minori di anni quattordici sedici richiede il consenso di chi esercita la responsabilità genitoriale. Il minore degli anni diciotto, che abbia compiuto quattordici sedici anni, può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili.
---	---

L'**art. 4, comma 3**, nel prevedere la tutela dell'utente disciplina la facoltà di opporsi ai trattamenti non corretti dei propri dati personali.

La **proposta di A.N.F.** è di esplicitare la tutela della facoltà di opposizione che deve essere garantita senza alcun tipo di automatismo del consenso.

L'**art. 4, comma 4**, tutela l'accesso ai sistemi di intelligenza artificiale da parte dei minori di anni 18, tuttavia le precauzioni indicate sono generiche e non sufficientemente tutelanti.

La **proposta di A.N.F.** è di escludere l'accesso ai minori di anni sedici privi del consenso degli esercenti la responsabilità genitoriale, posto che il minore di anni 14 è imputabile in caso di reato.

. * .

DISPOSIZIONI DI SETTORE

Proposta di modifica	
Art. 7 <i>(Uso dell'intelligenza artificiale in ambito sanitario e di disabilità)</i> <u>comma 1</u> L'utilizzo di sistemi di intelligenza artificiale contribuisce al miglioramento del sistema sanitario, alla prevenzione e alla cura delle malattie, nel rispetto dei diritti, delle libertà e degli interessi della persona, anche in materia di protezione dei dati personali. <u>comma 2</u> L'introduzione di sistemi di intelligenza	Art. 7 <i>(Uso dell'intelligenza artificiale in ambito sanitario e di disabilità)</i> <u>comma 1</u> L'utilizzo di sistemi di intelligenza artificiale contribuisce al miglioramento del sistema sanitario, alla prevenzione e alla cura delle malattie, nel rispetto dei diritti, delle libertà e degli interessi della persona, anche in materia di protezione dei dati personali. <u>comma 2</u> L'introduzione di sistemi di intelligenza

artificiale nel sistema sanitario non può selezionare e condizionare l'accesso alle prestazioni sanitarie secondo criteri di discriminazione. <u>comma 3</u> L'interessato ha diritto di essere informato circa l'utilizzo di tecnologie di intelligenza artificiale e sui vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo delle nuove tecnologie, nonché di ricevere informazioni sulla logica decisionale utilizzata. <u>comma 4</u> La presente legge promuove lo sviluppo, lo studio e la diffusione di sistemi di intelligenza artificiale che migliorano le condizioni di vita delle persone con disabilità, agevolano l'accessibilità, l'autonomia, la sicurezza e i processi di inclusione sociale delle medesime persone anche ai fini dell'elaborazione del progetto di vita di cui all'articolo 2, comma 2, lettera c), della legge 22 dicembre 2021, n. 227. <u>comma 5</u> I sistemi di intelligenza artificiale in ambito sanitario costituiscono un supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che è sempre rimessa agli esercenti la professione medica. <u>comma 6</u> I sistemi di intelligenza artificiale utilizzati in ambito sanitario e i relativi dati impiegati devono essere affidabili, periodicamente verificati e aggiornati al fine di minimizzare il	artificiale nel sistema sanitario non può selezionare e condizionare l'accesso alle prestazioni sanitarie secondo criteri di discriminazione. <u>comma 3</u> L'interessato ha diritto di essere informato e di esprimere il proprio diniego, nelle forme, nei modi e con le finalità di cui agli artt. 1 e 3, della L. 22 dicembre 2017 n. 219, circa l'utilizzo di tecnologie di intelligenza artificiale e sui vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo delle nuove tecnologie, nonché di ricevere informazioni sulla logica decisionale utilizzata. <u>comma 4</u> La presente legge promuove lo sviluppo, lo studio e la diffusione di sistemi di intelligenza artificiale che migliorano le condizioni di vita delle persone con disabilità, agevolano l'accessibilità, l'autonomia, la sicurezza e i processi di inclusione sociale delle medesime persone anche ai fini dell'elaborazione del progetto di vita di cui all'articolo 2, comma 2, lettera c), della legge 22 dicembre 2021, n. 227. <u>comma 5</u> I sistemi di intelligenza artificiale in ambito sanitario costituiscono un supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che è sempre rimessa agli esercenti la professione medica, fatti salvi i principi in materia di riparto della responsabilità civile, penale ed erariale. <u>comma 6</u> I sistemi di intelligenza artificiale utilizzati in ambito sanitario e i relativi dati impiegati devono essere affidabili, periodicamente
---	---

rischio di errori.	verificati e aggiornati al fine di minimizzare il rischio di errori.
--------------------	--

L'**art. 7 al comma 3** disciplina l'utilizzo nella professione medica dell'intelligenza artificiale come supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica senza precisare la necessaria informazione e assenso del paziente.

La **proposta di A.N.F.** è volta ad assicurare il consapevole coinvolgimento del paziente, che deve essere adeguatamente informato in ogni scelta dell'esercente la professione medica.

L'**art. 7 al comma 5**, sancisce la centralità e prevalenza della decisione umana in ambito sanitario, escludendo il ricorso a decisioni totalmente automatizzate.

La norma sulla riserva di decisione, tuttavia, può prestarsi ad interpretazioni volte ad attribuire ai soli esercenti la professione sanitaria ogni responsabilità in caso di danni ai pazienti, laddove si sia fatto ricorso a sistemi di IA.

La **proposta di A.N.F.** è, quindi, di far salvo il riparto di responsabilità, al fine di prevenire possibili conflitti interpretativi con la L. 8 marzo 2017 n. 24, anche con riferimento alla responsabilità organizzativa della struttura, e per evitare la totale deresponsabilizzazione dei produttori e/o fornitori di sistemi di IA che, con i loro output, abbiano indotto il medico ad assumere incolpevolmente una decisione errata. Ciò anche allo scopo di evitare l'acuirsi di fenomeni di medicina difensiva in relazione all'utilizzo di sistemi di IA.

. * .

PROFESSIONI INTELLETTUALI

Proposta di modifica	
Art. 12 <i>(Disposizioni in materia di professioni intellettuali)</i> <u>comma 1</u> L'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è consentito esclusivamente per esercitare attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera.	Art. 12 <i>(Disposizioni in materia di professioni intellettuali)</i> <u>comma 1</u> L'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è consentito esclusivamente per esercitare attività strumentali, da intendersi come tutti quegli adempimenti, ricerche, elaborazioni dei dati e ogni altra attività direttamente o indirettamente prodromica e/o necessaria per l'espletamento

<u>comma 2</u> 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.	dell'incarico e di supporto all'attività professionale, e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera. <u>comma 1 bis</u> Le medesime limitazioni si applicano alle stesse attività oggetto di prestazione d'opera intellettuale quando vengano svolte da soggetti non appartenenti alle professioni intellettuali. <u>comma 2</u> 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. <u>comma 3</u> L'inosservanza degli obblighi di comunicazione determina l'applicazione di una sanzione pecuniaria da euro 1.000,00 ad euro 5.000,00.
---	---

L'art. 12 al primo comma disciplina l'utilizzo dell'intelligenza artificiale nelle professioni intellettuali limitandolo alle attività strumentali e di supporto senza precisare la nozione di attività strumentale, mentre al secondo comma non prevede conseguenze circa la violazione dell'obbligo di informazione.

La **proposta di A.N.F.** è diretta a rendere maggiormente intellegibile da parte del professionista quali siano le attività per le quali possa avvalersi dello strumento di intelligenza artificiale, nonché ad applicare le medesime limitazioni quando lo stesso tipo di attività richiesta ai professionisti intellettuali venga svolta da soggetti non appartenenti alle professioni intellettuali, onde evitare una ingiustificata disparità di trattamento tra professionisti intellettuali ed altri soggetti (a mero titolo di esempio le società di consulenza) quando svolgano le medesime attività. Si ritiene preferibile e più equo, in un'ottica di tutela della concorrenza, spostare il *focus* sulle attività e non sul soggetto che le pone in essere.

Al contempo, si ritiene di dare copertura tra le altre anche alle attività dell'arbitro, del mediatore e del consulente tecnico.

Con riferimento alla mancata osservanza dell'obbligo di comunicazione, A.N.F. propone di introdurre delle sanzioni pecuniarie, applicabili anche a soggetti diversi dai professionisti intellettuali.

. * .

ATTIVITÀ GIUDIZIARIA

<i>Proposta di modifica</i>	
Art. 14 <i>(Uso dell'intelligenza artificiale nell'attività giudiziaria)</i> <u>comma 1</u> I sistemi di intelligenza artificiale sono utilizzati esclusivamente per l'organizzazione e la semplificazione del lavoro giudiziario, nonché per la ricerca giurisprudenziale e dottrinale. Il Ministero della giustizia disciplina l'impiego dei sistemi di intelligenza artificiale da parte degli uffici giudiziari ordinari. Per le altre giurisdizioni l'impiego è disciplinato in conformità ai rispettivi ordinamenti. <u>comma 2</u> È sempre riservata al magistrato la decisione sulla interpretazione della legge, sulla valutazione dei fatti e delle prove e sulla adozione di ogni provvedimento.	Art. 14 <i>(Uso dell'intelligenza artificiale nell'attività giudiziaria)</i> <u>comma 1</u> I sistemi di intelligenza artificiale sono utilizzati esclusivamente per l'organizzazione e la semplificazione del lavoro giudiziario, nonché per la ricerca giurisprudenziale e dottrinale. Il Ministero della giustizia disciplina l'impiego dei sistemi di intelligenza artificiale da parte degli uffici giudiziari ordinari. Per le altre giurisdizioni l'impiego è disciplinato in conformità ai rispettivi ordinamenti. <u>comma 2</u> È sempre riservata esclusivamente al magistrato, senza che la si possa estendere a terzi, la decisione sulla interpretazione della legge, sulla valutazione dei fatti e delle prove e sulla adozione di ogni provvedimento, ed in ogni caso la decisione che sia riferita e/o riferibile a qualsiasi provvedimento anche endoprocessuale e/o endoprocedimentale del giudice, anche se adottato in sede di volontaria giurisdizione e/o in caso di processi e/o procedimenti nei quali non vi sia l'obbligo di difesa tecnica.

La disciplina di settore prevista dall'**art. 14** per l'uso dell'intelligenza artificiale in ambito giudiziario si appalesa davvero esigua, in quanto si limita soltanto, **al comma 1**, a stabilire dei criteri guida, e

non a dettare una compiuta disciplina di settore tanto attesa, prevedendo l'utilizzo esclusivo dell'IA per la sola organizzazione del lavoro e di ricerca giurisprudenziale e dottrinale, e rimettendo, invece, al Ministero della giustizia (per la giurisdizione ordinaria) e ai diversi ordinamenti (per le altre giurisdizioni) il potere di disciplinarne l'uso da parte degli uffici giudiziari, così venendo meno quelle garanzie che sono proprie della riserva di legge, ma anche alimentando la proliferazione di differenti modalità d'utilizzo dell'IA nelle molteplici giurisdizioni, che solo in minima parte potrebbe giustificarsi nelle specifiche esigenze di ciascuna.

A ciò aggiungasi il “pericoloso” riferimento al concetto di “*semplificazione del lavoro giudiziario*” che in un futuro non molto prossimo, potrebbe favorire lo sviluppo di sistemi su base predittiva, fatto salvo quanto previsto dal c. 2, seppur limitato alla sola interpretazione della legge, ovvero alle decisioni.

La **proposta di A.N.F.** è che venga dettata una compiuta disciplina per l'impiego dell'IA nel settore giustizia, stabilendo dettagliatamente i confini e le modalità specifiche di utilizzo dell'IA, oltre che fornire l'esatta definizione dell'espressione “*semplificazione del lavoro giudiziario*”, ed espungere l'apposita delega conferita al Ministero della giustizia (per la giurisdizione ordinaria) e ai diversi ordinamenti (per le altre giurisdizioni).

L'**art. 14 co. 2** individua una riserva al magistrato in merito alla fase decisionale e di interpretazione della legge e ciò nel rispetto della prospettiva antropocentrica.

La **proposta di A.N.F.** è che venga esplicitato come la suddetta riserva debba intendersi rigorosamente esclusiva, senza che la si possa estendere a terzi ed in ogni caso che sia riferita e/o riferibile a qualsiasi provvedimento anche endoprocessuale e/o endoprocedimentale del giudice, anche se adottato in sede di volontaria giurisdizione e/o in caso di processi e/o procedimenti nei quali non vi sia l'obbligo di difesa tecnica.

. * .

DELEGHE AL GOVERNO

<i>Proposta di modifica</i>	
Art. 22 <i>(Deleghe al Governo in materia di intelligenza artificiale)</i> <u>comma 1</u> Il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente	Art. 22 <i>(Deleghe al Governo in materia di intelligenza artificiale)</i> <u>comma 1</u> Il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente

legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n.234, acquisito il parere delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi per l'adeguamento della normativa nazionale al regolamento del Parlamento europeo e del Consiglio sull'intelligenza artificiale, adottato dal Parlamento europeo nella seduta del 13 marzo 2024. <u>comma 2</u> Nell'esercizio della delega di cui al comma 1 il Governo si attiene, oltre che ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n.234, ai seguenti principi e criteri direttivi specifici: a) designazione, in coerenza con quanto previsto dall'articolo 18 della presente legge, come autorità nazionali competenti ai fini dell'attuazione del regolamento di cui al comma 1, di un'autorità di vigilanza del mercato, di un'autorità di notifica, nonché del punto di contatto con le istituzioni dell'Unione europea; b) previsione di percorsi di alfabetizzazione e formazione in materia di utilizzo dei sistemi di intelligenza artificiale; c) previsione, da parte degli ordini professionali, 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; d) potenziamento, all'interno dei curricula scolastici, dello sviluppo di competenze scientifiche, tecnologiche, ingegneristiche e	legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n.234, acquisito il parere delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi per l'adeguamento della normativa nazionale al regolamento del Parlamento europeo e del Consiglio sull'intelligenza artificiale, adottato dal Parlamento europeo nella seduta del 13 marzo 2024. <u>comma 2</u> Nell'esercizio della delega di cui al comma 1 il Governo si attiene, oltre che ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n.234, ai seguenti principi e criteri direttivi specifici: a) designazione, in coerenza con quanto previsto dall'articolo 18 della presente legge, come autorità nazionali competenti ai fini dell'attuazione del regolamento di cui al comma 1, di un'autorità di vigilanza del mercato, di un'autorità di notifica, nonché del punto di contatto con le istituzioni dell'Unione europea; b) previsione di percorsi di alfabetizzazione e formazione in materia di utilizzo dei sistemi di intelligenza artificiale; c) previsione, da parte degli ordini professionali, e delle associazioni di categoria maggiormente rappresentative, 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; d) potenziamento, all'interno dei curricula scolastici, dello sviluppo di competenze
--	---

matematiche legate alle discipline STEM, nonché artistiche, al fine di promuovere la scelta da parte delle studentesse e degli studenti, anche attraverso mirate attività di orientamento personalizzato, di percorsi di formazione superiore relativi alle menzionate discipline; e) previsione, nei corsi universitari e delle istituzioni di alta formazione artistica, musicale e coreutica (AFAM), nonché nei percorsi di istruzione tecnologica superiore offerti dagli istituti tecnologici superiori (ITS Academy), coerentemente con i rispettivi profili culturali e professionali, di attività formative per la comprensione tecnica e l'utilizzo consapevole anche sotto il profilo giuridico delle tecnologie, anche con riferimento ai sistemi di intelligenza artificiale così come definiti dalla disciplina europea, nonché per la corretta interpretazione della produzione di tali sistemi in termini di previsioni, contenuti, raccomandazioni o decisioni; f) valorizzazione delle attività di ricerca e di trasferimento tecnologico in materia di intelligenza artificiale svolte da università, istituzioni dell'AFAM, ITS Academy ed enti pubblici di ricerca, mediante disposizioni finalizzate al perseguimento dei seguenti obiettivi: 1) agevolare il coinvolgimento del sistema dell'università e della ricerca nella promozione, nella realizzazione e nell'utilizzo di spazi di sperimentazione normativa in collaborazione con il mondo produttivo; 2) incentivare le attività di supporto esemplificare gli strumenti di collaborazione tra il sistema dell'università e della ricerca, degli ITS Academy e le Autorità nazionali di cui all'articolo 18.	scientifiche, tecnologiche, ingegneristiche e matematiche legate alle discipline STEM, nonché artistiche, al fine di promuovere la scelta da parte delle studentesse e degli studenti, anche attraverso mirate attività di orientamento personalizzato, di percorsi di formazione superiore relativi alle menzionate discipline; e) previsione, nei corsi universitari e delle istituzioni di alta formazione artistica, musicale e coreutica (AFAM), nonché nei percorsi di istruzione tecnologica superiore offerti dagli istituti tecnologici superiori (ITS Academy), coerentemente con i rispettivi profili culturali e professionali, di attività formative per la comprensione tecnica e l'utilizzo consapevole anche sotto il profilo giuridico delle tecnologie, anche con riferimento ai sistemi di intelligenza artificiale così come definiti dalla disciplina europea, nonché per la corretta interpretazione della produzione di tali sistemi in termini di previsioni, contenuti, raccomandazioni o decisioni; f) valorizzazione delle attività di ricerca e di trasferimento tecnologico in materia di intelligenza artificiale svolte da università, istituzioni dell'AFAM, ITS Academy ed enti pubblici di ricerca, mediante disposizioni finalizzate al perseguimento dei seguenti obiettivi: 1) agevolare il coinvolgimento del sistema dell'università e della ricerca nella promozione, nella realizzazione e nell'utilizzo di spazi di sperimentazione normativa in collaborazione con il mondo produttivo; 2) incentivare le attività di supporto esemplificare gli strumenti di collaborazione tra il sistema dell'università e della ricerca, degli ITS Academy e le Autorità nazionali di cui
--	---

comma 3

Il Governo è, altresì, delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi per definire organicamente la disciplina nei casi di uso di sistemi di intelligenza artificiale per finalità illecite.

comma 4

Gli schemi dei decreti legislativi di cui al comma 3 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con il Ministro dell'interno, e sono successivamente trasmessi alle Camere per il parere delle Commissioni parlamentari competenti. Decorsi sessanta giorni dalla data della trasmissione, i decreti possono essere emanati anche in mancanza dei pareri. Qualora detto termine venga a scadere nei trenta giorni antecedenti alla scadenza del termine previsto per l'esercizio della delega o successivamente, quest'ultimo è prorogato di sessanta giorni.

comma 5

Nell'esercizio della delega di cui al comma 3, il decreto o i decreti legislativi sono adottati nel rispetto dei seguenti principi e criteri direttivi:

a) previsione di strumenti, anche cautelari, in ambito civile, amministrativo e penale, finalizzati a inibire la diffusione e a rimuovere contenuti generati illecitamente anche con sistemi di intelligenza artificiale, assistiti da un sistema di sanzioni effettive, proporzionate e dissuasive;

b) introduzione di una o più autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sulla omessa adozione o l'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale,

all'articolo 18.

comma 3

Il Governo è, altresì, delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi per definire organicamente la disciplina nei casi di uso di sistemi di intelligenza artificiale per finalità illecite.

comma 4

Gli schemi dei decreti legislativi di cui al comma 3 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con il Ministro dell'interno, e sono successivamente trasmessi alle Camere per il parere delle Commissioni parlamentari competenti. Decorsi sessanta giorni dalla data della trasmissione, i decreti possono essere emanati anche in mancanza dei pareri. Qualora detto termine venga a scadere nei trenta giorni antecedenti alla scadenza del termine previsto per l'esercizio della delega o successivamente, quest'ultimo è prorogato di sessanta giorni.

comma 5

Nell'esercizio della delega di cui al comma 3, il decreto o i decreti legislativi sono adottati nel rispetto dei seguenti principi e criteri direttivi:

a) previsione di strumenti, anche cautelari, in ambito civile, amministrativo, **tributario** e penale, finalizzati a inibire la diffusione e a rimuovere contenuti generati illecitamente anche con sistemi di intelligenza artificiale, assistiti da un sistema di sanzioni effettive, proporzionate e dissuasive;

~~b) introduzione di una o più autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sulla omessa adozione o~~

nonché introduzione di ulteriori fattispecie di reato, punite a titolo di dolo, dirette a tutelare specifici beni giuridici esposti a rischio di compromissione per effetto dell'utilizzazione di sistemi di intelligenza artificiale e che non siano adeguatamente tutelabili mediante interventi su fattispecie già esistenti; c) introduzione di una circostanza aggravante speciale per i delitti dolosi puniti con pena diversa dall'ergastolo nei quali l'impiego dei sistemi di intelligenza artificiale incida in termini di rilevante gravità sull'offesa al bene giuridico tutelato, includendovi i casi di offesa ai beni attinenti alla persona e allo Stato; d) revisione, anche a fini di razionalizzazione complessiva del sistema, della normativa sostanziale e processuale vigente, in conformità ai principi e ai criteri enunciati nelle lettere a), b) e c) del presente comma. <u>comma 6</u> Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni competenti provvedono ai relativi adempimenti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.	l'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, nonché introduzione di ulteriori fattispecie di reato, punite a titolo di dolo, dirette a tutelare specifici beni giuridici esposti a rischio di compromissione per effetto dell'utilizzazione di sistemi di intelligenza artificiale e che non siano adeguatamente tutelabili mediante interventi su fattispecie già esistenti; e) introduzione di una circostanza aggravante speciale per i delitti dolosi puniti con pena diversa dall'ergastolo nei quali l'impiego dei sistemi di intelligenza artificiale incida in termini di rilevante gravità sull'offesa al bene giuridico tutelato, includendovi i casi di offesa ai beni attinenti alla persona e allo Stato; d) revisione, anche a fini di razionalizzazione complessiva del sistema, della normativa sostanziale e processuale vigente, in conformità ai principi e ai criteri enunciati nelle lettere a), b) e c) del presente comma. <u>comma 6</u> Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni competenti provvedono ai relativi adempimenti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.
---	---

Il **comma 2 dell'art. 22 alla lettera c)** prevede che soltanto gli ordini professionali possano proporre dei percorsi di alfabetizzazione e formazione, per i professionisti e per gli operatori dello specifico settore, all'uso dei sistemi di intelligenza artificiale.

La **proposta di A.N.F.** è di estendere l'opportunità formativa anche alle associazioni forensi maggiormente rappresentative e/o a altre associazioni portatrici di interessi di natura professionale, purchè adeguatamente rappresentative su base nazionale.

Il **comma 5 dell'art. 22 alla lettera a)** stabilisce che nell'esercizio della delega vengano previsti degli strumenti, anche cautelari, in ambito civile, amministrativo e penale, finalizzati a inibire la diffusione e a rimuovere contenuti generati illecitamente.

La **proposta di A.N.F.** è di ampliare le ipotesi di adozione degli strumenti, anche cautelari, finalizzati a inibire la diffusione e a rimuovere contenuti generati illecitamente, non limitando la previsione all'ambito civile, amministrativo e penale, ma di estenderla anche in ambito tributario, al fine di garantire l'esercizio della difesa in tutti gli ambiti della giurisdizione.

Il **comma 5 dell'art. 22 alla lettera b) e c)** conferisce delega al Governo per l'introduzione di fattispecie di reato e di circostanze aggravanti realizzati mediante l'utilizzo "professionale" di sistemi di intelligenza artificiale.

La **proposta di A.N.F.** è di espungere il conferimento della delega al Governo per l'introduzione di disposizioni di rilevanza penale, poiché, considerata la natura afflittiva, la tecnica normativa utilizzata non appare adeguata. In subordine, si propone l'eliminazione del carattere "professionale" dell'utilizzo di sistemi di intelligenza artificiale ai fini della configurazione della fattispecie di reato, in quanto rimarrebbe impunito l'utilizzo per fini differenti da quello professionale.

Il **comma 5 dell'art. 22 alla lettera d)** conferisce delega al Governo per la revisione della normativa sostanziale e processuale vigente, in conformità ai principi e ai criteri enunciati nelle lettere a), b) e c) del medesimo comma 5.

La **proposta di A.N.F.** è di espungere il conferimento della delega al Governo per la revisione della normativa sostanziale e processuale vigente, oltre che per i motivi sopra esplicitati anche, perché appare trattarsi di delega in bianco.

. * .

DISPOSIZIONI PENALI

<i>Proposta di modifica</i>	
Art. 25 <i>(Modifiche al codice penale e ad ulteriori disposizioni penali)</i> <u>comma 1</u> Al codice penale sono apportate le seguenti modificazioni: a) all'articolo 61, primo comma, dopo il numero 11-novies) è aggiunto il seguente:	Art. 25 <i>(Modifiche al codice penale e ad ulteriori disposizioni penali)</i> <u>comma 1</u> Al codice penale sono apportate le seguenti modificazioni: a) all'articolo 61, primo comma, dopo il numero 11-novies) è aggiunto il seguente:

«11-decies) 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»; b) all’articolo 294, dopo il primo comma è aggiunto il seguente: «La pena è aumentata se il fatto è commesso mediante l’impiego di sistemi di intelligenza artificiale»; c) all’articolo 494, dopo il primo comma è aggiunto il seguente: «La pena è della reclusione da uno a tre anni se il fatto è commesso mediante l’impiego di sistemi di intelligenza artificiale»; d) all’articolo 501, terzo comma, dopo il numero 2) è aggiunto il seguente: «2-bis) se il fatto è commesso mediante l’impiego di sistemi di intelligenza artificiale»; e) dopo l’articolo 612-ter è inserito il seguente: «Art. 612-quater. – (<i>Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale</i>) – Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l’impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni. Il delitto è punibile a querela della persona offesa. Si procede tuttavia d’ufficio se il fatto è connesso con altro delitto per il quale si deve procedere	«11-decies) 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»; b) all’articolo 294, dopo il primo comma è aggiunto il seguente: «La pena è aumentata se il fatto è commesso mediante l’impiego di sistemi di intelligenza artificiale»; c) all’articolo 494, dopo il primo comma è aggiunto il seguente: «La pena è della reclusione da uno a tre anni se il fatto è commesso mediante l’impiego di sistemi di intelligenza artificiale»; d) all’articolo 501, terzo comma, dopo il numero 2) è aggiunto il seguente: «2-bis) se il fatto è commesso mediante l’impiego di sistemi di intelligenza artificiale»; e) dopo l’articolo 612-ter è inserito il seguente: «Art. 612-quater. – (<i>Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale</i>) – Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l’impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni. Il delitto è punibile a querela della persona offesa. Si procede tuttavia d’ufficio se il fatto è connesso con altro delitto per il quale si deve procedere
---	--

d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate.»; f) all'articolo 640, secondo comma, dopo il numero 2-bis è aggiunto il seguente: «2-ter. se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale»; g) all'articolo 640-ter, terzo comma, dopo le parole: «è commesso» sono inserite le seguenti: «mediante l'impiego di sistemi di intelligenza artificiale o»; h) all'articolo 648-bis, terzo comma, dopo le parole: «un'attività professionale» sono aggiunte le seguenti: «ovvero mediante l'impiego di sistemi di intelligenza artificiale»; i) all'articolo 648-ter, terzo comma, dopo le parole: «un'attività professionale» sono aggiunte le seguenti: «ovvero mediante l'impiego di sistemi di intelligenza artificiale»; l) all'articolo 648-ter.1, sesto comma, dopo le parole: «altra attività professionale» sono aggiunte le seguenti: «ovvero mediante l'impiego di sistemi di intelligenza artificiale». <u>comma 2</u> All'articolo 2637, primo comma, del Codice civile, è aggiunto, in fine, il seguente periodo: «La pena è della reclusione da due a sette anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale». <u>comma 3</u> All'articolo 171, primo comma, della legge 22 aprile 1941, n.633, dopo la lettera a-bis) è inserita la seguente: «a-ter) riproduce o estrae testo o dati da opere o	d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate.»; f) all'articolo 640, secondo comma, dopo il numero 2-bis è aggiunto il seguente: «2-ter. se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale»; g) all'articolo 640-ter, terzo comma, dopo le parole: «è commesso» sono inserite le seguenti: «mediante l'impiego di sistemi di intelligenza artificiale o»; h) all'articolo 648-bis, terzo comma, dopo le parole: «un'attività professionale» sono aggiunte le seguenti: «ovvero mediante l'impiego di sistemi di intelligenza artificiale»; i) all'articolo 648-ter, terzo comma, dopo le parole: «un'attività professionale» sono aggiunte le seguenti: «ovvero mediante l'impiego di sistemi di intelligenza artificiale»; l) all'articolo 648-ter.1, sesto comma, dopo le parole: «altra attività professionale» sono aggiunte le seguenti: «ovvero mediante l'impiego di sistemi di intelligenza artificiale». <u>comma 2</u> All'articolo 2637, primo comma, del Codice civile, è aggiunto, in fine, il seguente periodo: «La pena è della reclusione da due a sette anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale». <u>comma 3</u> All'articolo 171, primo comma, della legge 22 aprile 1941, n.633, dopo la lettera a-bis) è inserita la seguente: «a-ter) riproduce o estrae testo o dati da opere o
---	---

altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-ter e 70-quater, anche attraverso sistemi di intelligenza artificiale». <u>comma 4</u> All'articolo 185, comma 1, del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n.58, è aggiunto, in fine, il seguente periodo: «Se i fatti sono commessi mediante l'impiego di sistemi di intelligenza artificiale, la pena è aumentata».	altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-ter e 70-quater, anche attraverso sistemi di intelligenza artificiale». <u>comma 4</u> All'articolo 185, comma 1, del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n.58, è aggiunto, in fine, il seguente periodo: «Se i fatti sono commessi mediante l'impiego di sistemi di intelligenza artificiale, la pena è aumentata».
---	---

L'**art. 25, c. 1, lett. a)**, nel prevedere una serie di modifiche al codice penale, al comma 1, lettera a), nel formulare una nuova ipotesi di aggravante comune inserisce il termine insidioso, il quale non avendo un significato univoco si presterebbe a interpretazioni differenti alterando la certezza del diritto e il diritto di difesa con il rischio di vanificare anche l'intento punitivo.

La **proposta di A.N.F.** è di eliminare il termine insidioso e di mantenere l'aggravante nel caso di commissione del reato mediante l'uso di un sistema di intelligenza artificiale come avviene nelle altre ipotesi disciplinate dal medesimo articolo.

Roma, 9 ottobre 2024

ANF – Associazione Nazionale Forense
Il Segretario Generale
Avv. Giampaolo Di Marco