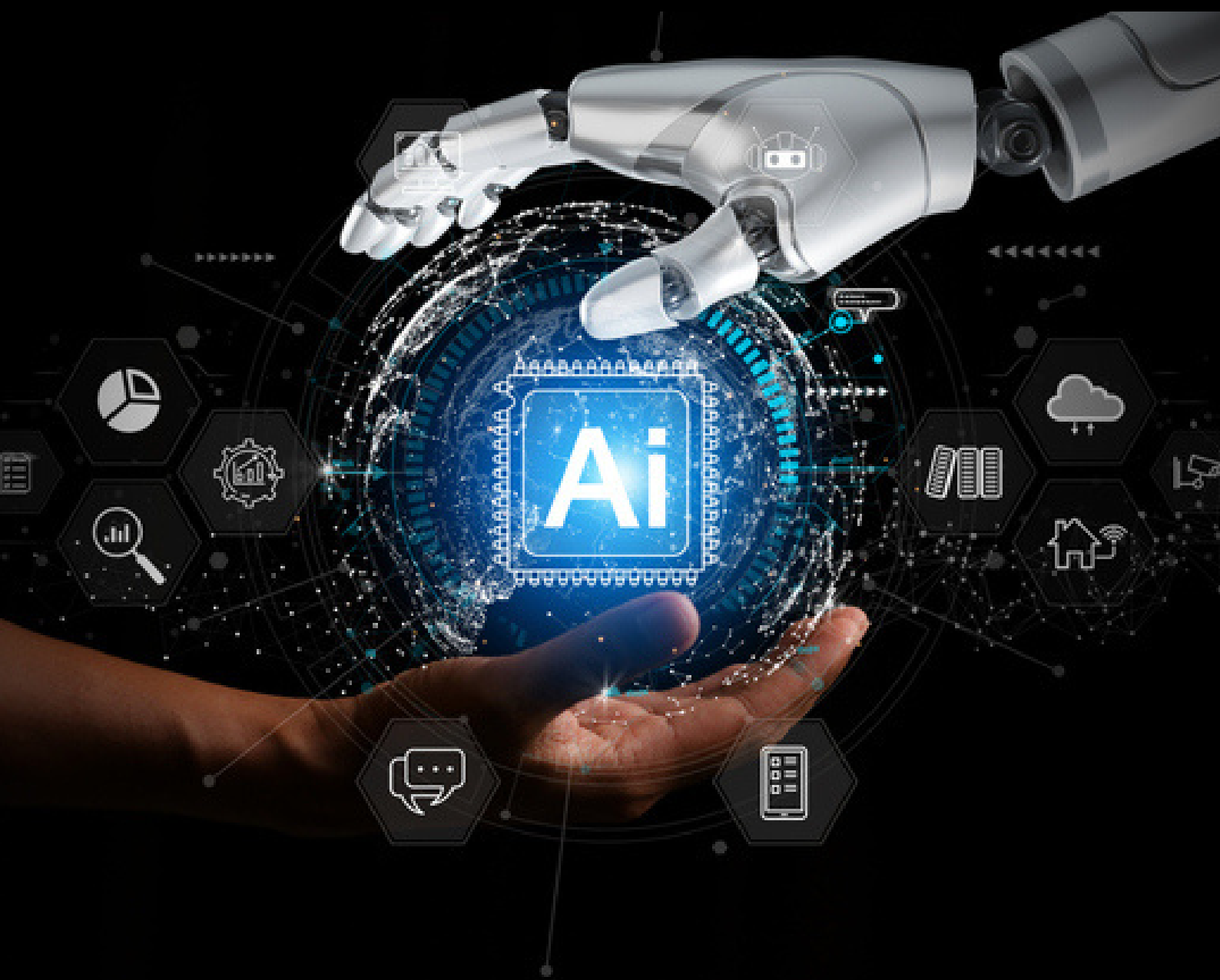


FOCUS

***L'IA TRA REGOLAZIONE EUROPEA E
DISCIPLINA NAZIONALE:
I PROFILI PENALI***



1. PREMESSA

Nel mondo contemporaneo, l'intelligenza artificiale costituisce uno dei più preziosi strumenti che l'evoluzione tecnologica ci consegna.

Come ogni processo innovativo, ha bisogno di tempi di "sviluppo", di "maturazione" ma anche di "gestione". In altri termini, la sua capacità incisiva si promana in maniera così profonda da richiedere uno sforzo di adeguamento da parte di tutti.

Per quello che qui interessa, il diritto penale si trova innanzi nuove sfide.

In che modo si può intervenire per porre dei limiti idonei a mitigare l'impatto dirompente di questi nuovi strumenti? E come si può irrogare sanzioni laddove a commettere il reato sia un algoritmo, perdipiù in continua evoluzione?

La risposta a questi interrogativi presuppone una preliminare, ulteriore, domanda: può l'IA progredire sino al punto di qualificarsi soggetto attivo del reato? E se sì, come può questo coordinarsi coi principi cardine del nostro ordinamento: colpevolezza e personalità della responsabilità penale?

Sotto altro profilo, parallelamente a tale evoluzione tecnologica emergono preoccupazioni relative alla diffusione dei dati, alla tutela della salute e della incolumità personale, e, più in generale, di diritti umani riconosciuti a livello sovranazionale.

La tecnologia nasce come strumento, ma oggi sembra assumere un ruolo più ampio: un sistema capace di mettere in discussione categorie giuridiche consolidate e di incidere sulle risposte punitive dello Stato.

L'impatto dell'intelligenza artificiale è evidente: offre enormi potenzialità, ma se utilizzata in modo inappropriato comporta rischi altrettanto significativi.

È in questo contesto che si comprende l'esigenza di una regolamentazione che detti canoni e principi valevoli in ogni Stato. La funzione di armonizzazione, rimessa al legislatore europeo, si giustifica proprio laddove ci si trovi a fronteggiare fenomeni che assumono caratteri "transfrontalieri".

L'Unione Europea nel 2024 ha adottato il Regolamento (EU) 2024/1689 (cosiddetto "*AI act*"), che costituisce il quadro di riferimento regolatorio.

Il nostro legislatore, con legge 23 settembre 2025 n. 132, entrata in vigore il 10 ottobre 2025, ha introdotto una disciplina nazionale intitolata "*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*", impegnandosi nel cercare di regolare un fenomeno nuovo e complesso da classificare.

Obiettivo comune è cercare un punto di equilibrio tra le potenzialità di questi strumenti offrono e i profili di rischio che comportano.

2. PROFILI PENALI DI RILIEVO

Preliminarmente, appare opportuno rappresentare le difficoltà operative con cui i legislatori (europei e nazionali) si sono dovuti confrontare, al fine di meglio comprendere la *ratio* che ispira questa regolamentazione.

Gli effetti dell'utilizzo di sistemi di IA possono sollevare numerose questioni di grande importanza:

- da un lato, problemi legati alla sempre crescente – e più rischiosa – capacità di adattamento dei sistemi di IA. In particolare, si pongono temi laddove si sfruttano intelligenze che si sviluppano e migliorano in base agli “*input*” di chi li utilizza.

Esse, classificate come strumenti basati sull'apprendimento (“*machine learning*”), non rispondono ad un “algoritmo” pre-individuato, bensì a uno che si evolve sulla scorta delle circostanze esterne, con la conseguenza che sono caratterizzati da una piuttosto estesa imprevedibilità.

In altri termini, vi è il concreto rischio che chi li ha programmati ne perda il controllo. L'essere “autonomi”, la perdita di una qualsivoglia sorveglianza umana sull'attività dell'algoritmo crea una frattura tra chi lo ha progettato e l'eventuale reato “commesso” dall'algoritmo medesimo.

A ciò si affiancano valutazioni di più ampio respiro: può mai una macchina commettere un reato? Si può attribuire la responsabilità della condotta della macchina – per come si è sviluppata nel tempo – a carico di chi lo aveva, inizialmente, impostato diversamente da come poi si è evoluto?

A ben vedere, in tali casi non c'è un nesso di correlazione tra fatto e autore del fatto, al più si può ravvisare un, seppur debole, nesso di derivazione causale.

A tali quesiti ancora non vi è una risposta legislativa univoca; il tema, infatti, sarà oggetto di trattazione nell'ambito della delega effettuata al Governo tramite la legge 132 del 2025.

- dall'altro lato, si paventano rischi a carattere “quantitativo”. La macchina come strumento in grado di facilitare la commissione del reato, potenziando le capacità delinquenziali dell'agente.

A tali questioni di sistema sull'utilizzo dell'IA, se ne aggiungono di ulteriori: come si definisce un sistema di Intelligenza artificiale? Che cosa è e come si caratterizza?

La norma penale deve essere connotata da tassatività, determinatezza e precisione e ciò impone una risposta puntuale a queste domande.

Analizzeremo di seguito come la normativa europea e quella nazionale hanno provato e provano a rispondere a questi interrogativi, nel tentativo di delineare una disciplina organica.

3. IL REGOLAMENTO EUROPEO 2024/1689

Il Regolamento adotta un approccio basato sul rischio “qualificato” (*risk-based approach*). Segnatamente, perché la normativa possa dirsi efficace, è necessario individuare la tipologia di IA a cui si fa ricorso, valutando criticamente i rischi che comporta.

Nella visione europea, al fine di garantire una corretta gestione, i sistemi di intelligenza artificiale dovrebbero essere interamente supervisionati da persone e non da automi. Il fattore umano assume così un ruolo di garante rispetto ai rischi potenziali.

Chiaramente, più elevati sono i rischi di compromissione dei diritti, più stringente sarà la regolamentazione, fino a tradursi in limiti invalicabili quando la qualificazione dello stesso appare “inaccettabile”.

Nella disciplina, il tema della trasparenza assume un rilievo centrale, come richiamato nel primo articolo del Regolamento. Essa si sostanzia in esigenze di tracciabilità e spiegabilità dei sistemi di AI si dà renderne l'utilizzo sicuro.

Per completezza, appare utile precisare che questo regolamento va ad integrarsi a quello relativo alla protezione dei dati – di cui, quindi, rappresenta un completamento, e non invece una

eccezione alla regolamentazione ivi prevista.

Considerati congiuntamente, essi costituiscono il *trait d'union* per la tutela dei dati personali, oggi elemento centrale nella salvaguardia dei diritti di ogni individuo.

Il Regolamento, alla Premessa 12 e successivamente all'articolo 3 paragrafo 1, cerca di affrontare il complesso tema definitorio.

L'IA, come già anticipato, si presenta in forme eterogenee e in costante evoluzione, e ciò reca con sé una difficoltà non di poco conto sulla qualificazione normativa: da un lato, adottare una definizione troppo stringente rischia di “invecchiare” rapidamente, intervenendo quando ormai è troppo tardi; dall'altro, una definizione più ampia comporta il pericolo di includere fattispecie che non costituiscono vere e proprie forme di intelligenza artificiale e, al contempo, di ostacolare eccessivamente l'innovazione.

Il punto di equilibrio nella qualificazione di “sistema di IA” si è trovato basandosi sulle caratteristiche che la qualificano. In particolare, si considera intelligenza artificiale quel sistema dotato di:

1. capacità inferenziale: la possibilità di, a fronte di *input*, ottenere degli *output*, cioè dei contenuti;
2. autonomia: un certo grado di indipendenza, variabile per ciascuno;
3. adattabilità: la capacità di apprendimento che consente di modificare il comportamento durante l'utilizzo in base agli stimoli esterni.

4. LA NORMATIVA NAZIONALE

In questo contesto si inserisce la normativa nazionale, rappresentata dalla legge 132 del 2025, che definisce i principi in materia di ricerca, sperimentazione, sviluppo, adozione e utilizzo dei sistemi e modelli di intelligenza artificiale, promuovendone un impiego corretto, trasparente e responsabile.

La legge in materia di IA interviene sull'intero ordinamento giuridico, compreso il comparto penale.

In essa si prevedono, da un lato, un insieme di misure applicabili a partire dal 10 ottobre 2025, data di entrata in vigore della normativa; dall'altro, si conferisce una delega al Governo affinché, entro dodici mesi dall'entrata in vigore, vengano adottati uno o più decreti legislativi volti a adeguare e specificare la disciplina relativa ai casi di realizzazione e utilizzo illecito di sistemi di intelligenza artificiale.

Sulla scia della regolamentazione europea, viene posto al centro, quale pilastro fondamentale per lo sviluppo dei sistemi di IA, l'essere umano.

Proprio al fine di garantire la tutela dei diritti fondamentali di ciascun individuo, si sottolinea l'esigenza di prevedere un controllo e un intervento della persona, capace di sorvegliare, comprendere e, se necessario, intervenire sul funzionamento dei sistemi.

La legge opera un rinvio integrale alla qualificazione di sistema IA designata dal legislatore europeo. Ciò, se da un lato assicura una perfetta coerenza tra quadro normativo nazionale e quello europeo,

eliminando i rischi di conflitti tra le normative, dall'altro non limita la – ampia – qualificazione sovranazionale. Come anticipato, giungere ad una qualificazione è stato compito particolarmente complesso, per cui il punto di equilibrio individuato e adottato a livello europeo è stato integralmente richiamato a livello nazionale.

Ciò si traduce in una applicazione piuttosto estesa delle nuove regole, comprese le novità, qui di maggiore interesse, in materia penale.

In particolare, la legge sull'IA, sul piano della struttura, è così organizzata:

- nel Capo I (artt. 1-6) vi sono i principi, finalità e definizioni;
- nel Capo II (artt. 7-18) è prevista la normativa di settori (es. sanità o Pubblica amministrazione) che si confrontano con l'utilizzo dell'IA;
- nel Capo III (artt. 19-24) vi è la delega al governo per i casi di realizzazione dell'impiego illecito di sistemi di intelligenza artificiale; in essa si prevedono anche due Agenzie nazionali per l'intelligenza artificiale con la finalità di controllo e gestione dei relativi rischi. In particolare, si prevede:
 1. l'Agenzia per l'Italia digitale (AgID) che assume un ruolo primario nella promozione e sviluppo dell'IA;
 2. l'Agenzia per la Cybersicurezza nazionale (ACN) che, invece, si concentra più sugli aspetti di sicurezza e vigilanza dei sistemi di intelligenza artificiale. Ad essa

spettano compiti ispettivi e di irrogazione di sanzioni, promozione della intelligenza artificiale in coordinamento coi profili sulla cybersicurezza nonché l'attività di referente e coordinamento tra la disciplina nazionale e quella europea;

- nel Capo IV (art. 25) vi è la regolamentazione in tema di tutela del diritto di autore;
- nel Capo V (art. 26) vi sono le disposizioni penali;
- nel Capo VI, infine, (artt. 27-28) vi sono le disposizioni finali che attengono ai poteri privatistici riconosciuti in ambito contrattuale all'ACN.

4.1 I PROFILI PENALI DI INTERESSE

Come anticipato, il Capo V detta le modifiche normative in materia penale che prevedono:

- l'introduzione della nuova fattispecie incriminatrice di *illecita diffusione di contenuti generati o manipolati artificialmente*;
- una nuova incriminazione che guarda alla violazione del diritto di autore;
- una circostanza aggravante comune;
- diverse circostanze aggravanti speciali.

4.1.1 L'ILLECITA DIFFUSIONE DI CONTENUTI GENERATI O MANIPOLATI ARTIFICIALMENTE (ART. 612 QUATER C.P.)

Si punisce “[c]hiunque 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”.

La norma sanziona le condotte di cessione, pubblicazione o diffusione non consensuale dei cosiddetti “deepfake”, ossia di contenuti generati o manipolati mediante sistemi di IA che appaiono realistici, qualora ne derivi un danno ingiusto.

Si punisce la diffusione di contenuti idonei a trarre in inganno, arrecando un pregiudizio all'onore e alla dignità della vittima e incidendo negativamente sulla sua autodeterminazione personale, in particolare nella sfera sessuale.

La norma sembra voler tutelare anzitutto la vittima dalla diffusione dei “deepfakes porn”, contenuti manipolati che violano la stretta intimità di ciascuno.

Tale *ratio* si comprende anche dalla collocazione topografica della norma, ossia

nel Capo dedicato ai delitti contro la libertà morale, nonché subito dopo l'articolo 612 *ter* c.p. che punisce la “*Diffusione illecita di immagini o video sessualmente espliciti*”, norma nel cui ambito applicativo non pare potersi includere i *deepfake porn*.

L'obiettivo è quindi garantire una tutela rafforzata delle vittime di violenze, in linea con la crescente attenzione al tema, che trova le sue radici nella Convenzione di Istanbul del 2011, sulle misure di contrasto alla violenza sulle donne e alla violenza domestica, nonché nella Direttiva Europea de 2024/1385 che impone obblighi di criminalizzazione per condotte di tal fatta.

Il danno arrecato dalla fattispecie in analisi non va inteso nella sua stretta accezione patrimoniale, bensì in una prospettiva più ampia.

Quanto all'elemento soggettivo, esso è individuabile nel dolo generico: è sufficiente la consapevolezza della diffusione, in assenza di consenso, di immagini manipolate. In questa ottica, si comprende la ragione per la quale il reato è perseguibile a querela dell'offeso.

Infine, si osserva che, sebbene la fattispecie appaia principalmente orientata alla tutela della libertà sessuale individuale, essa può trovare applicazione anche in ipotesi di *deepfake* riferite ad altri ambiti, idonee a ledere l'onore e la dignità della persona.

4.1.2 LE MODIFICHE ALLA LEGGE SUL DIRITTO D'AUTORE

La normativa in tema di diritto d'autore (legge 22 aprile 1941, n. 633), come

specificata dall'articolo 25 della l. 132 del 2025, trova applicazione alle opere di intelligenza “umana”, anche quando sono il frutto di un lavoro congiunto dell'impegno umano e dell'intelligenza artificiale.

In questo contesto, appare di particolare rilievo la fattispecie incriminatrice che viene aggiunta dalla legge sull'IA, che modifica l'articolo 171, comma 1 della legge sul diritto di autore, introducendo una nuova lettera *a-ter*): si punisce chiunque estrae o riproduce, anche attraverso sistemi di IA, materiali da opere protette dal diritto di autore.

Chiaramente, tale condotta non è vietata in assoluto: l'articolo 70 *ter* e 70 *quater* della stessa legge prevedono delle eccezioni, giustificate da specifiche ragioni, come la ricerca scientifica, previa autorizzazione, o la mancanza di espressa riserva da parte del titolare dei contenuti. La nuova fattispecie punisce dunque esclusivamente le condotte che esulano da queste ipotesi.

4.1.3. LE NUOVE CIRCOSTANZE AGGRAVANTI

A) L'AGGRAVANTE COMUNE

L'aggravante comune prevista dalla legge 132 del 2025 si va ad aggiungere all'elenco previsto nell'articolo 61 al numero 11-*decies* c.p.

In particolare, essa punisce più gravemente il reato quando commesso “*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”.

Tale inasprimento del trattamento sanzionatorio si giustifica in ragione dello sfruttamento illecito di strumenti di IA che rendono più semplice la commissione del reato.

Con ogni evidenza, ai fini della configurabilità dell'aggravante, l'utilizzo di tali strumenti deve fornire un *quid pluris* di offensività.

L'aggravante richiede che il mezzo sia insidioso, di ostacolo alla difesa e che il suo utilizzo abbia comportato un aggravamento delle conseguenze dannose o pericolose del reato.

Essendo una circostanza aggravante comune è applicabile a qualunque reato, salvo che la legge non disponga altrimenti.

B) LE AGGRAVANTI SPECIALI

Si prevede, infine, per reati specifici, l'introduzione di aggravanti speciali quando il fatto è commesso mediante l'impiego di sistemi di IA.

A differenza dell'aggravante comune, quelle speciali non richiedono che l'impiego dell'intelligenza artificiale apporti un *quid pluris*: ai fini della loro configurabilità, è sufficiente il mero utilizzo dello strumento.

In particolare, le fattispecie interessate dall'aggravamento sono:

- le fattispecie di attentato contro i delitti politici del cittadino (art. 294 c.p.);
- l'aggiotaggio (art. 2637 c.c.);

- la fattispecie di manipolazione del mercato (art. 185 TUF).

5. CONCLUSIONI

Alla luce di quanto esposto, emerge con chiarezza come l'intelligenza artificiale rappresenti una sfida di portata sistemica per l'intero ordinamento giuridico.

Il legislatore, tanto europeo quanto nazionale, ha avviato un percorso di regolamentazione volto a individuare un punto di equilibrio tra le potenzialità offerte da tali strumenti e i rischi che ne derivano.

In questo contesto, il diritto penale è chiamato a confrontarsi con fenomeni nuovi, che mettono in discussione categorie tradizionali e impongono un adattamento delle risposte sanzionatorie. Le innovazioni introdotte – in particolare le nuove fattispecie incriminatrici e le circostanze aggravanti legate all'impiego di sistemi di IA – testimoniano il tentativo di adeguare l'ordinamento a modalità di commissione del reato sempre più sofisticate, le cui previsioni future sono del tutto sconosciute.

Resta, tuttavia, aperta la questione relativa alla piena riconduzione delle condotte poste in essere mediante sistemi autonomi ai tradizionali criteri di imputazione penale, tema che sarà oggetto di ulteriore sviluppo nell'ambito della delega al Governo.

In definitiva, il quadro normativo delineato rappresenta un primo, significativo passo verso una disciplina organica della materia, destinata inevitabilmente a evolversi insieme al progresso tecnologico, nella costante esigenza di garantire una tutela effettiva dei diritti fondamentali.

CONTATTI



Giuseppe Fornari
Founding Partner

g.fornari@fornarieassociati.com



Margherita Cicirillo
Associate

m.cicirillo@fornarieassociati.com

Milano

Via Chiossetto 18

T: +39 0254122206

E: milano@fornarieassociati.com

Roma

Piazza Adriana 5

T: +39 0622201000

E: roma@fornarieassociati.com

Bari

Via Principe Amedeo 25

T: +39 080 918 4280

E: bari@fornarieassociati.com

Questa pubblicazione ha lo scopo di fornire informazioni di carattere generale rispetto all'argomento trattato e non deve quindi essere considerata come un parere legale né come una disamina esaustiva di ogni aspetto relativo alla materia oggetto del documento.

Fornari e Associati
www.fornarieassociati.com