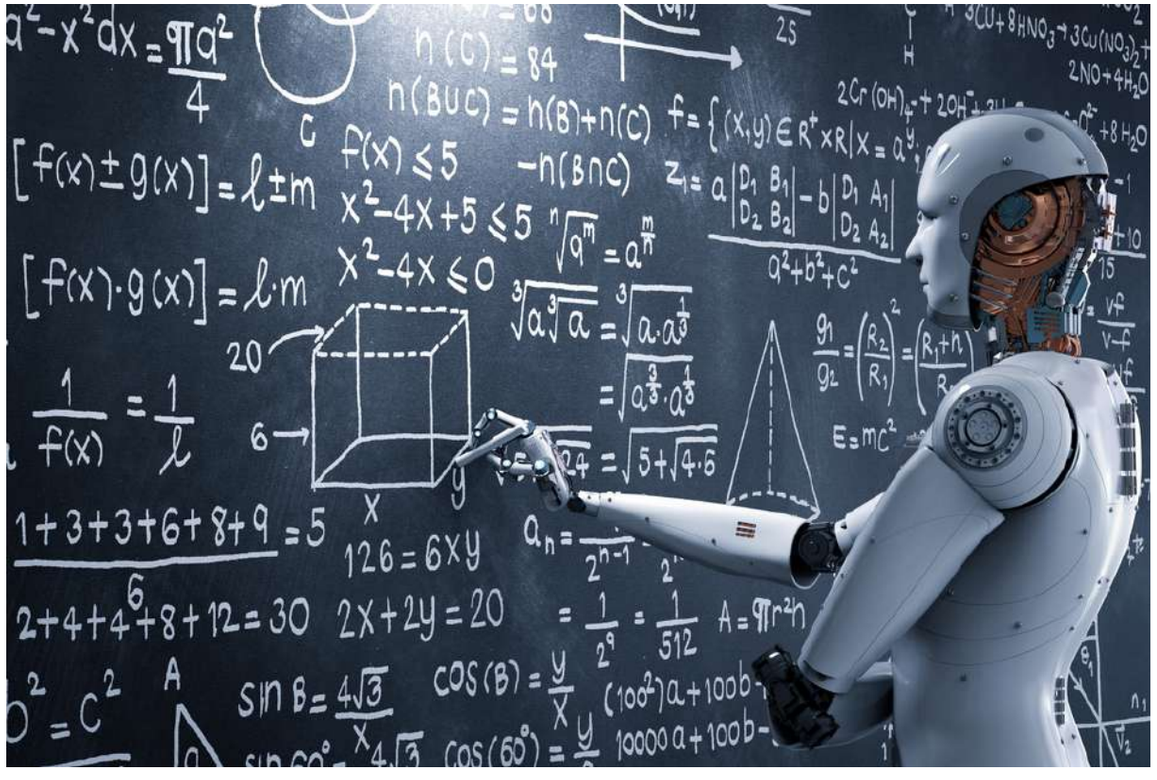
ARTIFICIAL INTELLIGENCE: THE STATE OF THE ART



Intelligenza artificiale: alcune nozioni preliminari

L'intelligenza artificiale ("IA") è una delle tecnologie più promettenti dei nostri tempi, poiché rappresenta il principale fattore della nuova rivoluzione industriale, ossia l'industria 4.0. Più in particolare, con la nozione di "intelligenza artificiale" si indicano tutti i sistemi che – all'esito di un processo di analisi e rielaborazione di dati – sono in grado di tenere un comportamento intelligente che si manifesta attraverso il compimento, in modo autonomo, di azioni volte al raggiungimento di specifici obbiettivi.

In campo economico ed industriale, lo sviluppo delle tecnologie di IA si è manifestato soprattutto nel settore dei servizi collegati alla sanità e alla salute della persona (c.d. healtcare), alla circolazione e ai trasporti, all'istruzione scolastica, al pubblico impiego e ai servizi al cittadino, nonché nel settore della sicurezza. È evidente che da tali innovazioni sul piano tecnologico derivano nuove e importanti sfide per gli operatori del mondo economico, industriale, finanziario e anche giuridico.

PRIVACY:

LA TUTELA DEI DATI PERSONALI

GESTIONE DEI RISCHI DERIVANTI DALL'IMPIEGO DI TECNOLOGIE DI IA.

Cosa può fare il consulente legale?

CYBER-SECURITY:

NORMATIVA DI RIFERIMENTO

NUOVI PROBLEMI PER GLI OPERATORI DEL DIRITTO E POSSIBILI AREE DI INTERVENTO.

Cosa può fare il consulente legale?

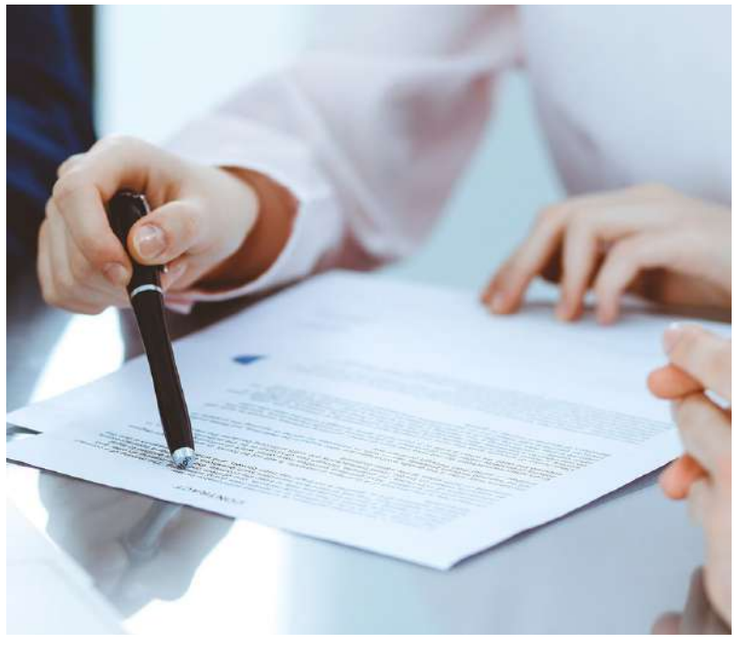
Normativa di riferimento

Il quadro normativo in materia di intelligenza artificiale è ancora in evoluzione. Si segnalano tuttavia i seguenti provvedimenti:

1- il Regolamento UE 679/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

2- la Risoluzione approvata dal Parlamento Europeo in data 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica;

3- la Comunicazione della Commissione Europea del 25 aprile 2018 al Comitato economico e sociale europeo e al Comitato delle Regioni, “L’intelligenza artificiale per l’Europa”.



Nuovi problemi per gli operatori del diritto e possibili aree di intervento

Le nuove tecnologie di IA consentono alla macchina, sulla base delle informazioni acquisite e rielaborate, di interagire anche nei confronti dei terzi: ciò comporta una vera e propria sfida in termini di tenuta del sistema economico-produttivo degli Stati a capitalismo avanzato ma del sistema di regole in essi vigenti. È innegabile, infatti, che il ricorso a forme di robotica e sistemi basati sull’intelligenza artificiale sia foriero di rischi con i quali gli individui dovranno confrontarsi: si pensi – solo per citare quelli più significativi – alla compressione della sfera di riservatezza personale o alle ricadute sociali e occupazionali causate dalla progressiva automazione dei processi produttivi.
D’altra parte, anche sul piano giuridico, lo sviluppo di tecnologie legate all’IA e al c.d. «machine learning» ha comportato l’emersione di problematiche del tutto nuove che sono, in larga misura, ancora oggetto di studio da parte della comunità scientifica (come, ad esempio, la questione legata alla personalità giuridica dei robot, la regolamentazione dei sistemi intelligenti e l’utilizzo di tecnologie nei processi). Tuttavia, esistono alcune tecnologie di IA che, tramite la loro applicazione, pongono - già oggi - nuove sfide con le quali gli operatori giuridici possono confrontarsi. Più in particolare, si allude - da un lato - al trattamento dei dati e alla tutela della privacy e - dall’altro lato - alla definizione di un sistema di governance dell’impresa idoneo a prevenire i rischi derivanti dall’impiego di tecnologie di IA.

PRIVACY:
LA TUTELA DEI DATI PERSONALI

Le tecnologie di IA si basano sulla rielaborazione dei dati che vengono processati in modo dinamico, messi in correlazione fra loro e “traslati” anche per finalità diverse da quelle per cui erano stati acquisiti. È evidente che l’impiego della IA per la raccolta e ’elaborazione dei dati, specialmente qualora questi abbiano natura “personale”, può sollevare delicate questioni di tutela della privacy degli individui dei cui dati si tratta.
Come noto, la disciplina comunitaria in materia di privacy e trattamento dei dati personali è stata recentemente modificata dal Regolamento Europeo per la protezione dei dati personali (Reg. UE n. 2016/679) (“GDPR”). Tale regolamento, applicabile a tutti gli Stati Membri dal maggio 2018, pur non contenendo alcun espresso riferimento all’IA, enuncia alcuni principi e regole che si rivolgono anche

(se non soprattutto) ai sistemi che si avvalgono dell'IA ai fini del trattamento dei dati personali. Infatti, in forza del principio di "neutralità del trattamento" dei dati personali, le norme del GDPR trovano applicazione anche nei confronti del trattamento dei dati interamente o parzialmente automatizzato. Con riferimento a tale materia, inoltre, il GDPR dedica particolare attenzione all'attività di "profilazione" e alla nozione di "processo decisionale automatizzato".
Mediante l'attività di profilazione si raccolgono informazioni riguardo agli individui, si analizzano le loro caratteristiche o i loro modelli di comportamento e s'inseriscono i profili così individuati in una determinata "categoria" per dar luogo ad ulteriori valutazioni o previsioni riguardanti, tra l'altro, le loro capacità di eseguire un'attività, i loro interessi o i loro probabili comportamenti.
Il processo decisionale automatizzato, invece, consente alla macchina di prendere decisioni solo attraverso mezzi tecnologici (ossia senza il coinvolgimento umano) e può basarsi su dati forniti direttamente dall'interessato oppure su dati ricavati da programmi traccianti o dati derivanti da profili precedentemente creati (ad es. l'affidabilità finanziaria in ambito creditizio).
Tuttavia, l'attività di profilazione e quella di decisione automatizzata non sempre sono perfettamente distinguibili. Infatti, può accadere che una decisione automatizzata venga presa senza che sia stato creato il profilo dell'individuo ovvero, al contrario, che una decisione automatizzata possa trasformarsi in attività di profilazione qualora i dati vengano utilizzati secondo determinate modalità.
La tendenziale opacità dei processi e dei meccanismi automatizzati, quindi, comporta che l'individuo spesso non sappia di essere "oggetto" di profilazione. Da tutto ciò derivano significativi rischi per i diritti e le libertà degli individui. Pertanto, il GDPR, al fine di correggere tali asimmetrie informative ed evitare pregiudizi alla sfera giuridica dell'individuo, prevede alcuni requisiti che dovranno essere rispettati in modo tale da rendere i trattamenti automatizzati conformi alla normativa e assicurare una maggiore trasparenza nella progettazione e nell'utilizzo dell'intelligenza artificiale.

I consulenti legali possono fornire un supporto significativo alle imprese, ai General Counsel e, più in generale, alle funzioni di compliance aziendali nella valutazione del rispetto delle normative vigenti e nella sterilizzazione dei rischi connessi con la loro eventuale violazione. Si tratta in particolare di assistere le imprese nell'adozione delle misure minime di sicurezza, nonché di verificare il rispetto degli obblighi regolamentari in caso di marketing diretto e profilazione, di dare supporto dell'analisi delle architetture di rete e delle misure di sicurezza adottate dall'impresa in ottemperanza agli obblighi regolamentari e in funzione della tipologia di servizi resi al pubblico. Oggetto dell'attività di consulenza legale può pertanto essere la predisposizione di un progetto di adeguamento al GDPR e l'assistenza nella sua implementazione mediante la redazione (o revisione e aggiornamento) di modelli di prestazione del consenso al trattamento dei dati personali sensibili, anche per finalità commerciali e promozionali, così come la redazione o la revisione di modelli'informativa circa la presenza di cookies sul sito web visitato dagli utenti, nonché l'assistenza per l'esecuzione e la redazione di documenti di valutazione del rischio.

GESTIONE DEI RISCHI DERIVANTI DALL'IMPIEGO DI TECNOLOGIE DI IA.

I sistemi di IA sono in grado, tra l'altro, di interagire con i terzi, producendo effetti anche nei loro confronti. Si comprende dunque che, da tale interazione, possano derivare conseguenze giuridiche che devono in qualche misura poter essere ricondotte a un soggetto di diritto (dato che i sistemi di IA ancora non lo sono): si pongono dunque significativi problemi d'imputazione della responsabilità.
Tralasciando in questa sede la questione dell'allocazione della responsabilità civile per i danni cagionati dai sistemi di IA (nell'attesa he il quadro normativo di riferimento venga definito ad opera del legislatore nazionale ma, soprattutto, europeo), pare opportuno –

quantomeno per il momento – volgere lo sguardo verso un'area in cui sembra già esservi spazio per un proficuo intervento degli operatori giuridici. Si allude in particolare alla responsabilità per i reati commessi mediante l'impiego di strumenti di IA.
Infatti, comincia ad affermarsi tra gli interpreti l'opinione secondo cui lo "strumento elettivo" per l'imputazione delle responsabilità penali derivanti dall'uso di tali strumenti di IA sia la responsabilità ex d.lgs. 231/2001 della persona giuridica titolare del sistema di IA che ha comportato la commissione del reato. Come noto, il d.lgs. 231/2001 ha inteso introdurre nell'ordinamento una disciplina idonea a colpire e reprimere quel particolare fenomeno che vede l'impresa al centro dell'agire criminale, prevendendo quale specifica esimente per l'ente l'aver adottato efficaci modelli di organizzazione e gestione idonei a prevenire reati della specie di quello in concreto verificatosi.
Tali modelli rappresentano un sistema di gestione dei rischi (c.d. "risk management") articolato in due fasi: da un lato, l'identificazione dei rischi e, dall'altro, la creazione di specifiche procedure in grado di contenere detti rischi. Tenendo conto delle innovazioni di IA che – sul piano del business aziendale – dovessero essere introdotte dalle imprese e dei "nuovi" rischi ad esse correlati, potrebbe derivare la necessità di intervenire per modificare i modelli di prevenzione e gestione ex d.lgs. 231/2001 attualmente adottati, nonché più in generale per adeguare le strutture di c.d. risk management in essere.

La principale sfida per i consulenti legali è quella di fornire il proprio supporto alle imprese nell'identificazione dei rischi connessi all'impiego di strumenti di IA e nella definizione di procedure idonee a contenere tali rischi, contribuendo dunque all'implementazione di efficienti sistemi di governance ovvero intervenendo nella revisione e nel miglioramento di quelli già esistenti.

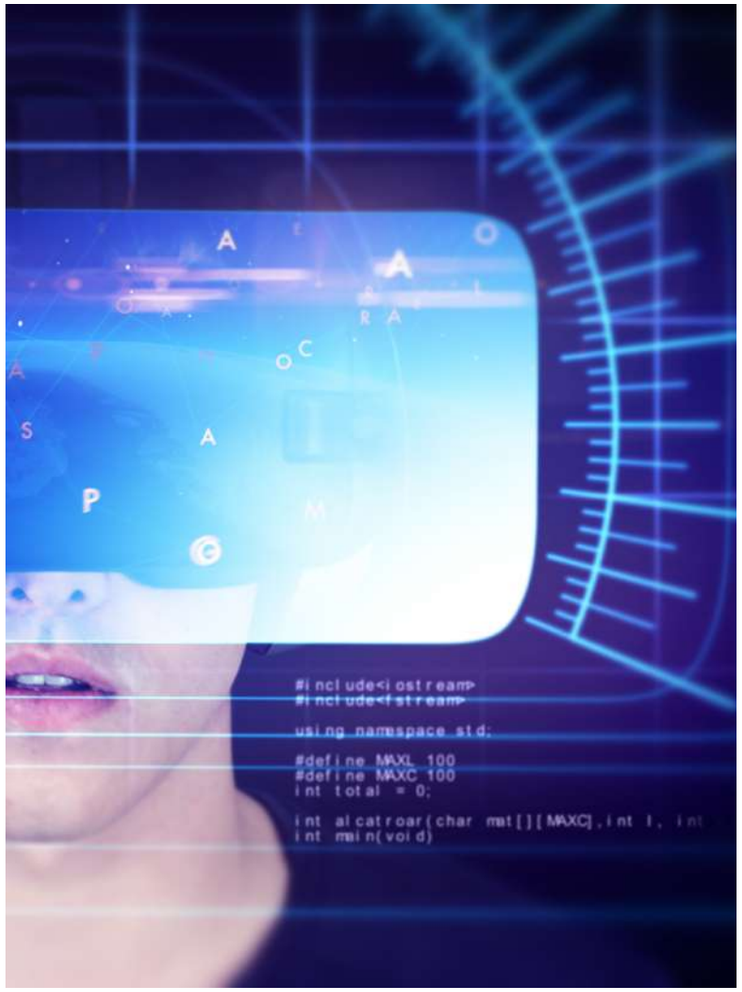
CYBER-SECURITY:
NORMATIVA DI RIFERIMENTO

La c.d. cyber-security rappresenta l'insieme di mezzi attraverso cui è possibile garantire la sicurezza del c.d. cyberspace, vale a dire l'ambiente entro cui avvengono le operazioni via Internet. Infatti, l'evoluzione digitale della società, la riduzione dei costi di accesso alla rete e lo sviluppo delle nuove tecnologie se, da un lato, hanno incrementato l'interazione tra individui, aziende e istituzioni per finalità sociali, economiche e finanziarie, dall'altro lato, anno creato nuove opportunità per il compimento di attività criminose.

Anche in materia di cyber-security il quadro normativo è in evoluzione ma, oltre al già richiamato Reg. UE n. 679/2016, si possono egnalare anche il recente d.lgs. 18 maggio 2018 n. 51 di attuazione della direttiva (UE) 2016/1148, recante misure per un livello comune elevato di scurezza delle reti e dei sistemi informativi dell'Unione.
Quest'ultimo decreto si applica agli operatori di servizi essenziali (ad esempio, nel settore sanitario, dell'energia, dei trasporti, bancario e dei mercati finanziari) e ai fornitori di servizi digitali (ossia persone giuridiche che forniscono servizi di e-commerce, cloud computing o motori di ricerca).
Il decreto non si applica invece alle imprese aventi meno di 50 dipendenti e un fatturato o bilancio annuo non superiore ai 10 milioni di Euro. Il decreto in parola prevede, inter alia, l'istituzione presso la residenza del Consiglio dei Ministri di un unico Computer Security Incident Response Team ("CSIRT") e l'obbligo per gli operatori di servizi essenziali e per i fornitori di servizi digitali di notificare al CSIRT italiano, informandone anche l'Autorità competente, gli incidenti che hanno un "impatto rilevante" rispettivamente sulla comunità e sulla fornitura del servizio.
Il CSIRT in particolare, una volta operativo, avrà la funzione tra l'altro di prevenire e gestire gli incidenti informatici ricevendo le notifiche di incidente e informandone il Dipartimento Informazioni per la Sicurezza.

NUOVI PROBLEMI PER GLI OPERATORI DEL DIRITTO E POSSIBILI AREE DI INTERVENTO.

Il cyberspace consente certamente l'apertura dei mercati nazionali e transnazionali.
Tale apertura, tuttavia, rende i sistemi informatici, su cui il cyberspace si basa, più vulnerabili anche agli attacchi di criminali di hacker e terroristi che intendano comprometterli, danneggiarli o sfruttarli per ottenere, in modo fraudolento, informazioni personali o commerciali.
In tale contesto, possono essere commessi i reati informatici (c.d. "cybercrime"), ossia attività criminose, analoghe a quelle tradizionali ma caratterizzate da un uso distorto di componenti della tecnologia dell'informazione (sia hardware che software).
Tali reati possono essere commessi in modo quasi istantaneo a livello planetario e l'input per la loro commissione può essere impartito in luoghi lontani o, comunque, esterni alle organizzazioni colpite: si comprende dunque quanto siano gravi le conseguenze qualora i reati in discorso siano commessi ai danni di istituzioni pubbliche o di imprese multinazionali.
Tuttavia, anche le imprese di piccole e medie imensioni – che costituiscono il fulcro del tessuto economico italiano – sono un potenziale bersaglio di attacchi informatici, in quanto si tratta di soggetti particolarmente vulnerabili a causa delle limitate risorse organizzative ed economiche delle quali dispongono. Istituzioni ed imprese, pertanto, rischiano di subire il furto e la manipolazione di dati sensibili, anche per via della crescente diffusione del "crime as a service", vale a dire la sottrazione di dati per la successiva rivendita sulla base delle esigenze dei potenziali acquirenti. Lo sfruttamento abusivo dei dati da parte dei cyber-criminali potrebbe essere funzionale alla commissione di reati di frode (relativamente a carte di credito o credenziali bancarie) di estorsione o di cyber-spionaggio (industriale/governativo).



I consulenti legali, oltre a servizi più tradizionali – e secondo logiche ex post – come l'assistenza giudiziale in cause di diffamazione a mezzo internet, blog e social networks, possono offrire anche servizi che – in una prospettiva ex ante – consentano di accrescere i livelli di sicurezza dei sistemi informatici, offrendo consulenza in materia di analisi dei rischi informatici, protezione e trasmissione sicura dei dati, autenticazione informatica, nonché tecniche di sicurezza informatica nelle applicazioni web e mobile, nei siti web e nei social network e nei sistemi cloud.

Da questo punto di vista i consulenti legali dovranno imparare ad interagire con tecnici informatici e ingegneri superando le barriere culturali tra il mondo giuridico e quello più strettamente digitale in un ottica di servizio per il cliente.

Via Gateano Negri 8
20123 – Milan – Italy
Phone: +39 02 94391800
Fax: +39 02 94391819
E-Mail: segreteria@gvalex.it

GRECO VITALI ASSOCIATI