SHIKAMARU

AI Compliance, Simplified.

Navigate the EU AI Act and beyond
with confidence.

La complessità normativa dell'IA

È indiscutibile rilevare una certa difficoltà nel seguire, comprendere e rispettare la enorme mole di nuovi atti normativi legati al mondo dell'Intelligenza Artificiale. La quantità di contenuto, la sua lunghezza, la sua complessità ed i suoi riferimenti normativi sparsi tra atti diversi mettono largamente in discussione il principio di certezza del diritto, e creano ostacoli per l'innovazione e mettono in pericolo con sanzioni e difformità i soggetti utilizzatori, fino al punto in cui questi rinunciano alle innovazioni del mercato pur di avere una maggiore sicurezza e tranquillità nel loro operare.

Scopo del documento è quello di fare chiarezza sui principali obblighi derivanti dall'utilizzo di strumenti di IA per le imprese, seguendo un approccio onnicomprensivo, che si occupi di sviscerare gli obblighi derivanti non solo dalle normative specifiche di settore (come l'AI Act), ma anche da atti affini, quali il GDPR, il DSA, il DMA. È infatti il connubio di questi regolamenti che dà origine alla normazione complessiva che interessa gli utilizzatori di IA.

Rispetto a produzioni simili, come i documenti di implementazione di procedure ISO 42001 sull'I.A., tale documento mira a raggiungere obiettivi congruenti (che del resto sono vincolati dalle leggi e dai regolamenti sovraordinati), ma vuole offrire prima una base teorica riassunta dello stato legislativo che ha originato le norme rilevanti, poi dare tabelle semplici e comprensibili che fungano da base ad eventuali processi organizzativi che dovranno essere modificati per assicurarsi che le norme siano state senz'altro rispettate (indicando questo con il termine compliance).

Indice

Quadro normativo sull'uso di IA

a) L'assetto normativo dell'Unione Europea in materia di I.A.

In Unione Europea figura oggi un assetto normativo costituito da molteplici fonti che influenzano l'utilizzo dell'I.A. e ne prescrivono regole ed obblighi da seguire, tanto per gli sviluppatori dei sistemi veri e propri, tanto per gli utilizzatori finali, specialmente in ambito professionale.
La combinazione dei principali testi legislativi dell'UE emanati negli ultimi anni, cioè il GDPR, l'AI Act, il Digital Markets Act ed il Digital Services Act creano un groviglio di regole non semplice da definire e non semplice da seguire.

A questo si aggiunge la possibilità, per il momento in fase semplicemente implementativa, di ricevere visite e controlli da parte delle Autorità Nazionali, che, al pari di quelle già presenti, garanti della Privacy, saranno incaricate di vigilare sull'adempimento degli obblighi inerenti all'uso delle intelligenze artificiali ed alla loro corretta implementazione ed utilizzo.

È in particolare l'AI Act che introduce un sistema di governance centralizzato e decentralizzato:

1. A **livello europeo**, sarà istituito un **AI Office** all'interno della Commissione Europea per coordinare l'applicazione delle regole.

2. A **livello nazionale**, ogni Stato membro dovrà designare **autorità di vigilanza** che faranno rispettare l'AI Act.

Da molti anni, lo "stile" legislativo dell'Unione Europea ha portato all'emanazione di norme non precisamente prescrittive, quanto piuttosto generiche nell'ottica di raggiungere certi obiettivi senza castrare il progresso tecnico e organizzativo.

In altre parole, anzichè prescrivere con precisione e per punti ciò che le impres debbono mettere in campo, o ciò a cui devono fare attenzione, sia il GDPR prima, sia l'AI Act poi, hanno inteso dare una cornice normativa basata sul raggiungimento di obiettivi, per lo più basandosi sullo stato dell'arte nella gestione dei sistemi di IA e sulla predisposizione di documentazioni tecniche e di gestione del rischio.

Violazioni delle prescrizioni europee daranno luogo a sanzioni severe, con multe fino al 7% del fatturato annuo globale per le più gravi.

b) Obbligo di risultato e sue problematicità.

È evidente l'intenzione da parte del legislatore europeo di non bloccare il già lento e faticoso progresso tecnologico nel vecchio continente obbligando imprese e privati cittadini ad adempiere ad obblighi precisi, rigidi ed immodificabili. Al contrario, si dà l'idea di un "obbligo di risultato": le cautele messe in campo dagli utilizzatori dei sistemi di IA saranno efficaci e legislativamente congrue nel momento in cui nel concreto saranno in grado di garantire quelle riduzioni del rischio, quei controlli e quelle misure organizzative tali per cui si potrà definire sicuro e benevolo l'uso che dello strumento di IA viene fatto.

Alcuni esempi di prescrizioni con questo grado di genericità, ma che devono comunque essere seguite dagli utilizzatori ed implementatori di sistemi di IA sono:

Articolo	Descrizione
Articolo 9	Impone ai fornitori di sistemi di IA ad alto rischio di implementare un sistema di gestione del rischio continuo, che copra l'intero ciclo di vita del sistema, per identificare, analizzare e mitigare potenziali rischi associati all'IA.
Articolo 10	Stabilisce che i dati utilizzati per l'addestramento, la validazione e il testing dei sistemi di IA devono essere di alta qualità, pertinenti, rappresentativi e privi di bias, al fine di garantire prestazioni accurate e imparziali del sistema.

Articolo 18	Richiede ai fornitori di redigere una documentazione tecnica dettagliata che dimostri la conformità del sistema di IA ai requisiti dell'AI Act.
Articolo 29	Stabilisce la necessità di garantire un'adeguata supervisione umana, permettendo agli utilizzatori di interpretare correttamente
Articolo 51	Obbliga i fornitori a registrare i sistemi di IA ad alto rischio nel registro dell'Unione Europea prima della loro immissione sul mercato o messa in servizio.
Articolo 52	Obbliga gli utilizzatori a informare chiaramente gli individui quando interagiscono con un sistema di IA, garantendo la consapevolezza dell'utente riguardo all'uso dell'IA.
Articolo 60	Richiede agli utilizzatori di sistemi di IA ad alto rischio di conservare registrazioni dettagliate del funzionamento del sistema, inclusi i log delle attività, per un periodo appropriato, al fine di garantire la tracciabilità e facilitare eventuali audit.
Articolo 61	Impone ai fornitori di implementare un sistema di monitoraggio post-commercializzazione per raccogliere e analizzare dati sulle prestazioni dei sistemi di IA ad alto rischio, garantendo la continua conformità e sicurezza del sistema.
Articolo 69	Collega l'uso di sistemi di IA alla conformità al Regolamento Generale sulla Protezione dei Dati (GDPR), garantendo la tutela dei dati personali trattati dai sistemi di IA.

Tutte queste prescrizioni, come si vede, sono piuttosto blande nella loro formulazione e delegano sostanzialmente agli utilizzatori di gestirsi da sé per riuscire a raggiungere gli obiettivi espressi nelle norme.
Farlo non è semplice: il corpus normativo dell'IA Act, al di là di questi pochi articoli citati, è molto grande, e si lega, come si diceva in precedenza, con altre fonti normative, quali il GDPR o il DMA ed il DSA.

c) Ambito applicativo e soggetti sottoposti alle norme.

Si è visto che l'AI Act non è l'unica fonte applicabile al macro-mondo dei sistemi di IA.
Al contempo, non tutti i soggetti che utilizzano sistemi di IA sono sottoposti al notevole quantitativo di obblighi e prescrizioni dell'Atto. Tuttavia, permangono per loro alcuni obblighi derivanti dal quadro normativo europeo completo, cioè al di là del solo AI Act: GDPR, la direttiva e-privacy, le normative di settore e quelle legate alla responsabilità civile e penale sono comuni a tutti, indipendentemente dall'uso che di un sistema IA viene fatto.

In massima sintesi, si possono definire queste due categorie:

1. **L'uso personale o hobbistico, non sottoposto alle regole dell'AI Act**.
   L'uso di un IA per scopi privati o hobbistici (come la generazione di immagini e testo per puro diletto) non è ritenuto rilevante dall'AI Act, che pertanto non si applica al caso.
2. **L'uso professionale o aziendale.**
   Se un'impresa o un professionista impiega l'IA in un contesto lavorativo, possono esserci obblighi se il sistema rientra nelle categorie regolamentate. L'applicazione delle regole dipende dal livello di rischio dell'IA:

Rischio inaccettabile	Rischio alto	Rischio basso
Sono del tutto vietati sistemi di "social scoring", manipolatori per gli utenti (come pubblicità ingannevoli generate da IA) e sistemi di sorveglianza biometrica in tempo reale (con debite eccezioni per le forze di pubblica sicurezza). Intelligenze artificiali che si occupino di tali argomenti sono proibite dall'UE.	In vari settori dove c'è un vero e proprio impatto sulla vita delle persone, come in quello sanitario, finanziario, delle asunzioni, della giustizia e dell'educazione, l'uso dell'IA è sottoposto a vari obblighi. Figurano tra essi, in una lista non esustiva, quello di avere sempre un umano a monitorare e potenzialamente intervenire in caso di errori; tracciare i dati e documentare il funzionamento del sistema; valutarne i rischi prima.	Figurano qui chatbot, assistenti virtuali, sistemi di raccomandazione, traduttori automatici e strumenti di supporto alla scrittura e alla produttività che non hanno impatti sui diritti fondamentali delle persone, né esplicano presso di loro effetti giuridici significativi. Per questi è sufficiente informare gli utenti che stanno interagendo con un IA ed attenersi ad un generico "divieto di manipolazione".

Anche quando un utilizzatore di IA non è soggetto agli obblighi specifici dell'**AI Act**, può comunque dover rispettare **altre normative**.
Al di là dei casi ovvi di violazioni di leggi civili e penali, non è difficile immaginare la possibilità che il sistema di IA venga per esempio utilizzato, per la raccolta ed il trattamento di dati personali, indipendentemente dalla sua natura professionale o hobbistica.
In tal caso, il GDPR impone:

- che vi sia una base giuridica per il trattamento, cioè un motivo valido per raccogliere ed elaborare questi dati;
- che vi sia un obbligo di trasparenza, che stabilisce la necessità di informare gli utenti di come vengono usati questi stessi loro dati e consentirgli di esercitare i diritti di acesso, rettifica e cancellazione;
- che sia rispettato l'obbligo di minimizzazione, che prescrive di raccogliere solo i dati strettamente necessari, per un tempo definito, e di proteggerli adeguatamente.

Normative di settore e leggi civili e penali completano il quadro da seguire per l'utilizzo di un sistema di IA.
Tra le normative di settore, in particolare, è possibile con un po' di forzature inserire i nuovi curpora legislativi del Digital Markets Act e del Digital Services Act, dei quali alcune norme interessano l'uso dell'intelligenza artificiale – seppur legato alle piattaforme digitali, specie se di grandi dimensioni.

Tali obblighi sono così riassunti brevemente:

Normativa	Ambito	Collegamenti con l'IA
DSA	Regolamenta piattaforme digitali e servizi online.	Regola l'uso di IA per moderazione contenuti, trasparenza degli algoritmi, prevenzione disinformazione.
DMA	Limita il potere delle Big Tech e garantisce concorrenza.	Impone trasparenza su IA usata da gatekeeper e obbliga alla condivisione di dati.

c.2) Eccezione open source, open washing.

È dunque evidente la quantità di norme e la complessità legislativa legata allo sviluppo e all'utilizzo dell'IA. Per questo motivo, si vuole in questo scritto offrire una schematizzazione semplice e chiara, tramite la predisposizione di alcune domande alle quali si ritiene importante che un utilizzatore di un sistema di IA debba saper dare risposta.

d) Postilla su responsabilità.

Una ulteriore questione rilevante quando si utilizzano sistemi di IA, specie in ambito professionale, è quella inerente alla responsabilità.
Vi sono alcune caratteristiche intrinseche dei sistemi di Intelligenza Artificiale che rendono infatti particolarmente complesse la comprensione delle possibili cause di un danno, l'attribuzione della colpa e l'applicazione in generale delle norme sulla responsabilità.

Tra le principali difficoltà si annoverano l'opacità degli algoritmi, la scarsa prevedibilità di alcuni output, la pluralità di attori coinvolti (sviluppatori, fornitori, utilizzatori finali) e la presenza di clausole di limitazione di responsabilità nei contratti di licenza e nei termini di servizio delle soluzioni basate su IA.

Questi fattori complicano il percorso per le vittime di danni causati da sistemi di IA, che potrebbero trovarsi di fronte a costi elevati e ostacoli nell'individuare il soggetto responsabile e dimostrare il danno subito. In particolare, una delle questioni più critiche è la dimostrazione del nesso causale tra il funzionamento del sistema IA e il danno, ossia l'onere della prova.

> Per "onere della prova" si intende la necessità di dimostrare certi fatti in un procedimento giuridico. Nel contesto dell'IA, riguarda la capacità della vittima di provare che un danno è stato causato da un sistema AI. L'"alleggerimento" dell'onere facilita le rivendicazioni dei danneggiati, ma dà oneri nei confronti dei produttori; al contrario, inasprire l'onere della prova rende più difficile per i danneggiati dimostrare le loro ragioni, ma consente un più ampio spazio di libertà imprenditoriale per i produttori.

L'attuale quadro normativo della responsabilità civile non è stato concepito per tecnologie con elevata autonomia decisionale e capacità di auto-apprendimento, rendendo quindi difficile applicare le regole tradizionali.

Per affrontare questa sfida, l'UE sta valutando due principali percorsi normativi:

1. **Aggiornamento della Direttiva sulla responsabilità per danno da prodotti difettosi**, con l'estensione delle regole di responsabilità ai software e ai sistemi di IA, rendendole più adatte all'era digitale.
2. **Proposta di una Direttiva sulla responsabilità civile extracontrattuale per l'IA**, che mira a rafforzare la tutela delle vittime alleggerendo l'onere della prova nelle cause per danni causati da sistemi di IA.

Un ulteriore punto centrale del dibattito riguarda l'attribuzione dell'onere della prova e i criteri di responsabilità. Qui emergono due visioni contrastanti:

- Le associazioni dei consumatori sostengono che, essendo i produttori i principali beneficiari economici dell'IA, dovrebbero essere loro a dimostrare l'assenza di difetti o malfunzionamenti, configurando una responsabilità oggettiva, simile a quella applicata ai produttori di automobili.
- Le aziende produttrici e le imprese software sostengono invece che dovrebbe essere la vittima a dimostrare il malfunzionamento del sistema e il legame diretto con il danno subito, poiché l'IA è una tecnologia altamente complessa e il malfunzionamento può essere difficile da determinare con certezza.

Essere compliant, in breve.

a) Il rischio della genericità dei controlli e la conseguente necessità di dimostrare di essere allo stato dell'arte.

La principale necessità, per le imprese che si occupino di sviluppare o anche soltanto di operare sui sistemi di IA, ed anche per quelle che semplicemente ne fruiscono come ultimi utilizzatori, è quella di controllare il rischio degli stessi e rispettare i requisiti legislativi imposti.

L'AI Act, principale fonte normativa sul tema, a partire dall'articolo 2, comprende nel suo ambito applicativo, oltre ai fornitori e distributori di servizi AI, anche i "deployer", "persone fisiche o giuridica, [...] che utilizzano 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".
Da ciò discende la conseguenza che a chiunque utilizzi un sistema di IA per esigenze professionali è demandato seguire le regole dell'AI Act, ed accertarsi pertanto che le prescrizioni sull'utilizzo di tali sistemi siano rispettate dal sistema stesso utilizzato.
È importante, tuttavia, notare quanto segue: l'IA Act è un testo legislativo sterminato, con una notevolissima parte dedicata ai preamboli e numerosi allegati, ai quali è dato rimando spesso negli articoli concreti del testo. Intende essere una fonte generale sul tema dell'I.A., mirando più ad obiettivi che a prescrizioni sul come raggiungerli.

Gli audit propriamente detti di tali sistemi di IA, pur non essendo specificamente obbligatori per i fornitori e gli implementatori ai sensi dell'AI Act, possono logicamente fornire una solida base per garantire la conformità a molte delle sue disposizioni, non dissimilmente di come avveniva in tema di privacy dopo l'introduzione del GDPR. L'AI Act a più riprese infatti pone l'accento sui principi di equità (Racc. 74, 110, 27), supervisione umana (Art. 14), accuratezza (Art. 15) e trasparenza (Art. 50).
Il problema principale di un simile ragionamento è causato dall'indeterminatezza delle procedure da seguire, che, seppure in teoria commisurate al rischio e quindi ragionevolmente desumibili a seconda dell'attività svolta, possono essere diverse per gli utilizzatori finali rispetto a quelle delle autorità nazionali previste dall'AI Act all'articolo 28, incaricate di vigilarne la conformità.

La motivazione di tale genericità va ricercata nell'ottica di non oberare di dettami un settore particolarmente all'avanguardia e in fase di espansione[1]: si preferisce agire per obiettivi, anziché per prescrizioni, lasciando così una certa autonomia decisionale alle imprese utilizzatrici, limitando gli effetti negativi sull'innovazione il più possibile.

Dunque, nell'assenza di precise indicazioni e di un consenso generalizzato sul tema può determinarsi il problema di imprese che operino procedure di audit ritenute poi insufficienti dalle autorità nazionali, senza però che vi sia per esse un'effettiva prescrizione legislativa, a tutto svantaggio del principio di certezza del diritto.

Non solo: la scarsa trasparenza, l'irreplicabilità e la generale opacità dei sistemi di intelligenza artificiale accrescono questo problema, che investe altri ambiti del diritto ancora quando i dati originali sui quali il sistema è stato addestrato non sono pubblicamente disponibili per motivi di riservatezza o proprietà intellettuale.

Così, mancando prescrizioni precise e concrete, in presenza di eventuali controlli determinati dalle autorità garanti, è imperativa la necessità di poter offrire dimostrazione precisa delle procedure seguite e del rispetto dello stato dell'arte delle stesse.

Il seguito di questo documento vuole esplicitare una base teorica esplicativa per i concetti fondamentali legati alla compliance dei sistemi di IA, e, successivamente offrire una serie di tabelle riassuntive, che siano utili nel momento in cui imprese che operino con strumenti di IA vogliano accertarsi della compatibilità del loro utilizzo con le normative vigenti, e siano quindi tranquille nel loro utilizzo anche a fronte di eventuali controlli che potrebbero seguire in futuro.

1 M. Martin Zamorano Barrios, AI Audits: How do you implement the EU AI Act?, Trilateral Research, 24 luglio 2024, https://trilateralresearch.com/artificial-intelligence/ai-audits-how-do-you-implement-the-eu-ai-act#:~:text=The%20introduction%20of%20the%20AI,principles%2C%20and%20relevant%20societal%20values.

b) Compliance normativa sul trattamento dei dati da parte degli sviluppatori di sistemi di IA.

La crescente influenza sociale e tecnologica dei moderni sistemi di intelligenza artificiale ha sollevato interrogativi fondamentali in materia di regolamentazione, etica e sicurezza. In un contesto globale sempre più interconnesso, diventa essenziale adottare un approccio di governance internazionale che permetta di affrontare queste sfide in modo coordinato, idealmente attraverso la collaborazione tra Stati, imprese private e organizzazioni sovranazionali. La definizione di un quadro normativo chiaro e condiviso rappresenta un passaggio imprescindibile per garantire uno sviluppo tecnologico sicuro e rispettoso dei diritti fondamentali.

Un aspetto centrale riguarda la necessità di distinguere ciò che può essere considerato realmente open source e ciò che non lo è, determinando gli elementi costitutivi di tale definizione. L'assenza di una regolamentazione chiara in questo ambito non solo ostacola il progresso scientifico e tecnico, ma comporta anche implicazioni legali significative per lo sviluppo e l'adozione dell'IA.

Uno dei punti critici è la riusabilità dei modelli di IA. Molti di questi sistemi sono infatti altamente specializzati e ottimizzati per specifiche applicazioni, limitando la loro adattabilità ad altri contesti. In particolare, i cosiddetti modelli "pre-trained" (pre-addestrati) rappresentano strumenti potenti ma con una ridotta flessibilità, spesso utilizzabili solo tramite piattaforme centralizzate, come nel caso di ChatGPT. La necessità di accedere a una potenza computazionale significativa rappresenta un ulteriore ostacolo alla decentralizzazione dell'IA, costringendo gli utenti a dipendere da fornitori di servizi terzi per poter usufruire di queste tecnologie.
La disponibilità e la gestione dei dati di addestramento pongono inoltre questioni cruciali in materia di compliance normativa. I dati costituiscono l'input primario su cui si basano i modelli di IA, e la loro qualità e rappresentatività incidono direttamente sulle prestazioni del sistema. Tuttavia, la raccolta e l'utilizzo di enormi quantità di dati sollevano problematiche relative alla tutela della privacy, alla protezione dei dati personali e ai diritti di proprietà intellettuale. Regolamenti come il GDPR impongono vincoli stringenti sulla gestione dei dati, limitando l'uso di informazioni sensibili o raccolte senza un consenso esplicito[1].

L'accesso ai dati rappresenta quindi una delle principali barriere alla riproducibilità dei modelli di IA. Anche nei casi in cui il codice sorgente sia reso disponibile, l'indisponibilità dei dataset di addestramento compromette la possibilità di replicare esattamente i risultati ottenuti. Questo crea problemi di trasparenza e verificabilità, fondamentali per la fiducia nell'IA e nella sua applicazione in settori critici.

1 E. Thelisson, H. Verma, Conformity assessment under the EU AI act general approach, AI and Ethics, Springers, 3 gennaio 2024, vol.4

Soluzioni tecnologiche emergenti, come l'uso di dataset sintetici o il Federated Learning, potrebbero contribuire a mitigare alcuni di questi problemi. I dataset sintetici permettono di addestrare modelli di IA senza esporre dati reali, riducendo il rischio di violazioni della privacy. Il Federated Learning, invece, consente di distribuire l'addestramento su molteplici dispositivi senza la necessità di centralizzare i dati, garantendo una maggiore protezione delle informazioni sensibili. Tuttavia, questi approcci presentano ancora limiti e criticità, in particolare per quanto riguarda la sicurezza e l'integrità dei dati utilizzati.

In massima sintesi, si propone un trittico di elementi essenziali cui gli sviluppatori di sistemi di IA devono prestare attenzione:

1. Gestione e accessibilità dei dati: garantire la legalità e la trasparenza nella raccolta e nell'uso dei dati di addestramento.

2. Sicurezza e responsabilità: definire chi sia responsabile degli output generati dai modelli di IA e delle eventuali conseguenze negative.

3. Trasparenza e verificabilità: trovare formule che oltre ad una mera commercializzazione del prodotto spieghino i suoi funzionamenti negli aspetti rilevanti per gli utilizzatori.

c) Il rischio della genericità dei controlli e la conseguente necessità di dimostrare di essere allo stato dell'arte.

Se la regolamentazione dello sviluppo dell'IA pone problematiche legate ai dataset, alla trasparenza e alla potenza computazionale, la compliance normativa per gli utilizzatori di questi sistemi si concentra invece sulla gestione responsabile dei dati e sulle modalità di impiego dell'IA nelle attività quotidiane.

Gli utenti di sistemi di IA – che siano aziende, enti pubblici o privati cittadini – devono assicurarsi di rispettare le normative vigenti in materia di protezione dei dati, in particolare per quanto riguarda il trattamento delle informazioni personali. L'uso improprio di strumenti basati sull'IA può infatti portare a violazioni della privacy, discriminazioni algoritmiche o decisioni automatizzate potenzialmente lesive dei diritti degli individui.

Un aspetto particolarmente rilevante è il trattamento dei dati da parte di aziende che utilizzano IA per l'analisi e l'elaborazione delle informazioni dei propri clienti.

In molti settori, dall'e-commerce alla sanità, l'IA viene impiegata per personalizzare servizi e prodotti, ottimizzare strategie di marketing o automatizzare decisioni. Tuttavia, questo impiego solleva interrogativi etici e giuridici, soprattutto quando l'utente non è pienamente consapevole delle modalità con cui i suoi dati vengono utilizzati.

In questo contesto, il GDPR stabilisce principi chiave come la minimizzazione dei dati, la necessità del consenso esplicito e il diritto alla spiegabilità delle decisioni automatizzate. Gli utenti di sistemi di IA devono quindi adottare politiche trasparenti e garantire che l'impiego dell'IA sia conforme a queste disposizioni, evitando pratiche come la raccolta massiva di dati, magari senza un consenso esplicito ed informato, al di là di finalità legittime o instaurando una profilazione discriminatoria.

Anche qui, un approccio genericamente tripartito può essere da guida agli utilizzatori finali dei sistemi di IA per porsi le giuste questioni in materia di compliance normativa:

1. Protezione della privacy e trasparenza: garantire il rispetto delle normative sulla gestione dei dati personali.

2. Affidabilità e verificabilità degli output: responsabilità nell'uso dei risultati generati dall'IA.

3. Trasparenza e conoscibilità: dalla parte opposta rispetto agli sviluppatori, gli utilizzatori devono accertarsi di poter rendicontare quel minimo di conoscenza del sistema necessaria per assicurarne il buon uso

d) Compliance normativa per tutti: rischi nell'uso concreto (cautele by design)

I due terzi punti di entrambe le categorie, cioè sviluppatori e utilizzatori, mostrano quella che di fatto è la chiave della legislazione corrente per chiunque interagisca con l'IA: la gestione dei rischi nell'uso concreto. Questo aspetto introduce il concetto di cautele by design, ovvero un insieme di accorgimenti e metodologie di sviluppo e implementazione che devono essere adottati sin dalla progettazione per minimizzare i pericoli insiti nell'impiego delle tecnologie basate su IA, e la conoscenza del funzionamento del sistema limitatamente a ciò che è necessario per assicurare la sua conformità.

Le pratiche tecnologiche migliori promuovono il principio di compliance by design, cioè l'integrazione della sicurezza e della conformità normativa sin dalle prime fasi dello sviluppo e dell'implementazione di un sistema di IA.

Questo approccio si articola in diverse strategie:

a) Trasparenza e spiegabilità

Per ridurre il rischio di opacità, è essenziale sviluppare modelli di IA con caratteristiche di spiegabilità (explainability) e interpretabilità (interpretability). Ciò implica l'adozione di tecniche che permettano di comprendere come un modello giunge a una decisione. Questo è fondamentale sia per lo sviluppatore, sia per l'utilizzatore finale: se è poi il secondo che in ultima istanza dovrà operare tramite uno strumento di IA "spiegabile", è a partire dal primo che questa "spiegabilità" può derivare. Uno strumento IA facilmente "spiegabile", magari unito ad una precisa documentazione da parte dello sviluppatore, è anche più appetibile presso il pubblico, e pertanto più vendibile perchè contiene già in sé, by design, elementi essenziali in tema di compliance.

b) Monitoraggio e auditing continuo

Un sistema di IA non può essere considerato statico: le sue prestazioni devono essere monitorate nel tempo per individuare possibili derive nei risultati. Occorrono processi di auditing periodici con metodologie definite. Anche questo tema riguarda sia gli sviluppatori, che continuano, com'è costume oggi, ad offrire aggiornamenti e migliorie dei loro software, sia gli utilizzatori finali, che devono essere attenti nel controllare l'andamento dei loro sistemi IA lungo l'utilizzo.

c) Meccanismi di supervisione umana

La decisione finale di un processo decisionale con "effetti significativi" sulla sfera giuridica di un interessato dovrebbe sempre essere presa da un essere umano, con l'IA che funge da strumento di supporto. Il supervisore umano entra anche in gioco nel tentativo di risolvere gli enormi problemi di responsabilità che l'utilizzo di sistemi di IA porta con sé, ulteriormente acuiti nel caso in cui si utilizzi un software IA open source, laddove potenzialmente convivono una molteplicità indefinita di sviluppatori ed è difficile pertanto individuare una catena di responsabilità in caso di malfunzionamento.

> In generale, dunque, il tema principale è il seguente:
> come fare ad essere sicuri che l'utilizzo di un software IA sia compatibile con la legge, mettendosi contemporaneamente al riparo da eventuali san zioni seguite a controlli delle autorità nazionali?

Come si è visto, non esistono prescrizioni precise: sta a ognuno essere consapevole dello strumento di IA che sta utilizzando e delle cautele necessarie perché il suo uso sia congruo. Le tabelle nella terza parte di questo documento, oltre alle nozioni teoriche di queste pagine, offriranno un ulteriore e facilmente consultabile strumento per costruire una "checklist" di elementi rilevanti a tale scopo.

e) Decisioni di adeguatezza e località dei server

Un aspetto fondamentale nell'integrazione dell'AI nelle imprese riguarda la gestione della localizzazione dei dati e il rispetto delle normative europee sulla protezione dei dati.

L'UE impone infatti restrizioni sulla conservazione e il trasferimento dei dati personali al di fuori dello Spazio Economico Europeo (SEE), a meno che il paese di destinazione non abbia ottenuto una decisione di adeguatezza dalla Commissione Europea. Questo significa che molte soluzioni di AI basate su cloud, se ospitate in paesi privi di tali decisioni (ad esempio, Cina o India), non possono essere utilizzate senza violare il GDPR. Di conseguenza, le aziende devono assicurarsi che i loro fornitori di AI rispettino le normative europee e, ove necessario, adottino misure tecniche e contrattuali per la protezione dei dati, come le clausole contrattuali standard o il data localization.

Inoltre, il problema della sovranità digitale si intreccia con la questione della sicurezza dei dati. L'uso di infrastrutture cloud localizzate in Europa o in paesi dotati di decisioni di adeguatezza rappresenta un metodo per garantire il rispetto della normativa sui dati personali e ridurre il rischio di accessi non autorizzati ai dati.

Nel momento in cui un'impresa voglia dunque utilizzare uno strumento di IA proveniente da un paese extra-europeo, o i cui dati viaggino su server extra-europei, dovrà accertarsi che tale paese sia stato definito congruo con le obbligazioni legislative, e lo rimanga per tutto il tempo di uso.

f) Integrare l'IA nei sistemi aziendali

A titolo squisitamente esemplificativo, si offrono qui alcuni suggerimenti di utilizzo dell'IA in varie categorie di operazioni, basati sull'attuale stato dell'arte e sulla diffusione maggioritaria di tali pratiche.

Operazione	Suggerimenti
Automazione dei processi (RPA e AI-driven automation)	Le aziende, in particolare quelle manifatturiere e dei servizi, possono beneficiare dell'automazione intelligente per migliorare efficienza e ridurre costi operativi. I sistemi di Robotic Process Automation (RPA) potenziati con AI consentono di automatizzare processi ripetitivi come la gestione della contabilità, la fatturazione e il customer service.

AI per la previsione e l'analisi dei dati (Predictive Analytics)	Nel settore finanziario, nella logistica e nel retail, l'AI può essere impiegata per analizzare grandi volumi di dati (big data) e fornire previsioni più accurate su vendite, rischi di mercato e tendenze dei consumatori. L'adozione di modelli di machine learning avanzati consente di ottimizzare l'inventario, ridurre sprechi e migliorare la personalizzazione dell'offerta.
Miglioramento dell'interazione con i clienti (Chatbot e NLP)	Le imprese attive nella somministrazione di servizi e nel commercio di beni possono adottare chatbot e sistemi di Natural Language Processing (NLP) per fornire assistenza ai clienti in modo più efficiente. L'AI conversazionale riduce i tempi di risposta e migliora la qualità del servizio, riducendo il carico di lavoro degli operatori umani. Si ricorda in tale senso comunque l'obbligo di un supervisore umano finale per questioni di responsabilità nel momento in cui si effettuino operazioni che abbiano un effetto giuridico significativo sulle persone.
AI per il design e la produzione (Generative AI e Industria 4.0)	Nel settore manifatturiero, l'integrazione di sistemi AI per la progettazione (Generative Design) e il controllo della produzione sembra promettente nell'ottimizzare il design di prodotti e migliorarne pertanto la qualità. La cosiddetta "industria 4.0", con l'uso di AI per il monitoraggio predittivo delle macchine, consente alle aziende di evitare fermi produttivi e ridurre i costi di manutenzione.
AI per la sicurezza informatica e la conformità normativa	In un colpo di scena paradossale, si segnala come ultimo elemento il fatto che l'AI può essere impiegata per migliorare la compliance in un quadro normativo – quello delineato – così complesso e oscuro. Le imprese possono, sempre avendo un supervisore umano cui risalire in caso di responsabilità, utilizzare l'IA per migliorare la loro conformità normativa, automatizzando parzialmente il controllo documentale e la gestione del rischio. I sistemi di IA possono essere anche d'ausilio in tema di cybersecurity, per esempio per rilevare intrusioni e monitorare attività sospette in tempo reale.

Tabelle riassuntive e domande utili

Si offrono qui una serie di tabelle e domande utili per assicurare la compliance normativa dei propri sistemi di IA, basandosi sulle precedenti considerazioni in senso legislativo e sullo stato dell'arte: leggi, best practices, standard internazionali, model cards e checker tools concorrono nella definizione di questa sezione, che ha l'obiettivo di mettere al riparo gli utilizzatori finali da eventuali sanzioni derivanti dalle autorità nazionali, che come si visto rispondono a criteri non ben definiti e precisi, a tutto svantaggio della certezza del diritto.

Compliance normativa generica; utile per utilizzatori e sviluppatori allo stesso modo.

1. Rischi di robustezza
I rischi di robustezza riguardano la vulnerabilità dei sistemi IA a comportamenti imprevisti, specie in presenza di dati non visti o alterati, che possono causare errori significativi e compromettere l'operatività aziendale.

Q: Ha l'impresa un piano B nel momento in cui l'IA dovesse malfunzionare?

Q: Sono presenti sistemi per rilevare l'accesso non autorizzato o la manipolazione dei dati e dei modelli di IA?
Es: uno storico o una cronologia degli accessi; una lista di output già noti per controllare che, a input standard, emergano sempre uguali.

2. Rischi di furto e manomissione
Questi rischi includono l'accesso non autorizzato ai dati, la manipolazione dei modelli di IA per alterarne le decisioni o la sottrazione di informazioni riservate, con conseguenti danni finanziari e reputazionali.

3. Rischi di attacchi malevoli
Gli attacchi malevoli comprendono l'inserimento intenzionale di dati falsificati o l'attacco diretto al modello (ad esempio, adversarial attacks) per confonderlo o per causarne il malfunzionamento.

Q: Esistono misure di protezione efficaci contro tentativi intenzionali di compromissione dei sistemi IA, provenienti o dall'impresa utilizzatrice in sé, o dal produttore del software IA, ma comunque noti all'utilizzatore finale?

Q: Esiste un protocollo per validare e correggere rapidamente output errati, inaffidabili, illeciti o sconvenienti generati dai sistemi IA? Es. un soggetto umano esperto del tema che esegua controlli periodici, anche solo a seguito di segnalazioni.

4. Rischi di output inaffidabili o inappropriati
Gli output inaffidabili sono decisioni o informazioni errate o fuorvianti prodotte dall'IA, che possono portare a scelte strategiche errate, perdite economiche o danneggiamento della fiducia dei clienti. Quelli inappropriati sono offensivi, discriminatori o illegali, e espongono l'impresa a controversie legali o a danni reputazionali.

5. Rischi di raccolta e uso illegale dei dati
Questo rischio può causare violazioni delle normative sulla privacy (GDPR), multe elevate, danni reputazionali e perdita di fiducia da parte di clienti e partner commerciali. La raccolta illegale o non autorizzata di dati personali, o il loro uso improprio durante il training dei modelli, può portare a violazioni della privacy e a sanzioni legali pesanti.

Q: L'impresa dispone di procedure per garantire la conformità del trattamento dati che consegue all'uso degli strumenti IA alle normative vigenti, come il GDPR? Se il modello è di terze parti, si è per lo meno cercato di assicurarsi che i dati di training fossero compatibili con le norme in tema di privacy?

Compliance normativa specificamente legata agli utilizzatori finali di IA

1

Protezione della privacy e trasparenza
Gli utilizzatori finali devono assicurarsi del pieno rispetto delle normative come il GDPR, ottenendo consenso esplicito e minimizzando la raccolta di dati personali, dando un tempo limite alla loro conservazione e garantendo trasparenza nelle operazioni.
Se l'IA proviene da terze parti o è fruita tramite un servizio, è opportuno anonimizzare eventuali dati personali immessi.

2

Affidabilità e verificabilità degli output
Gli utenti sono tenuti a verificare e assumersi la responsabilità dei risultati ottenuti, evitando l'applicazione automatica di decisioni che potrebbero essere discriminatorie o lesive di diritti. Qualsiasi decisione che abbia un "effetto giuridico significativo" sulle persone deve essere confermata da un essere umano.

3

Trasparenza e conoscibilità
Gli utilizzatori devono possedere una conoscenza minima ma sufficiente per garantire un utilizzo responsabile e conforme alle normative, documentando e rendicontando le modalità di impiego.
Sono utili una lista di "best practices" da seguire quando si utilizza uno strumento di IA e un'analisi dello stesso, anche sommaria, per ciò che concerne trasparenza e funzionamento degli algoritmi utilizzati.

4

Rischio di discriminazione algoritmica
Per evitare discriminazioni algoritmiche, è opportuno monitorare periodicamente i risultati generati dall'IA per evitare discriminazioni o disparità ingiustificate.
Il controllo umano già citato al punto 2 può tornare utile anche in questo senso.