



Bruxelles, 19.2.2020
COM(2020) 65 final

LIBRO BIANCO

sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia

Libro bianco sull'intelligenza artificiale

Un approccio europeo all'eccellenza e alla fiducia

L'intelligenza artificiale si sta sviluppando rapidamente. Cambierà le nostre vite migliorando l'assistenza sanitaria (ad esempio rendendo le diagnosi più precise e consentendo una migliore prevenzione delle malattie), aumentando l'efficienza dell'agricoltura, contribuendo alla mitigazione dei cambiamenti climatici e all'adattamento ai medesimi, migliorando l'efficienza dei sistemi di produzione mediante la manutenzione predittiva, aumentando la sicurezza dei cittadini europei e in molti altri modi che possiamo solo iniziare a immaginare. Al tempo stesso, l'intelligenza artificiale (IA) comporta una serie di rischi potenziali, quali meccanismi decisionali opachi, discriminazioni basate sul genere o di altro tipo, intrusioni nelle nostre vite private o utilizzi per scopi criminali.

In un contesto di forte concorrenza globale, è necessario un solido approccio europeo, basato sulla strategia europea per l'IA presentata nell'aprile 2018¹. Per sfruttare le opportunità e affrontare le sfide derivanti dall'IA, l'UE deve parlare con un'unica voce e definire il suo modo di promuovere lo sviluppo e la diffusione dell'IA basandosi sui valori europei.

La Commissione si impegna a favorire i progressi scientifici, a preservare la leadership tecnologica dell'UE e a garantire che le nuove tecnologie siano al servizio di tutti gli europei e ne migliorino la vita rispettandone i diritti.

La presidente della Commissione Ursula von der Leyen ha annunciato nei suoi orientamenti politici² un approccio europeo coordinato alle implicazioni umane ed etiche dell'intelligenza artificiale e una riflessione volta a migliorare l'uso dei big data per favorire l'innovazione.

La Commissione sostiene pertanto un approccio normativo e orientato agli investimenti con il duplice obiettivo di promuovere l'adozione dell'IA e di affrontare i rischi associati a determinati utilizzi di questa nuova tecnologia. Lo scopo del presente libro bianco è definire le opzioni strategiche su come raggiungere tali obiettivi. Non vengono affrontate in questa sede le questioni dello sviluppo e dell'utilizzo dell'IA per scopi militari. La Commissione invita gli Stati membri, le altre istituzioni europee e tutti i portatori di interessi, compresi l'industria, le parti sociali, le organizzazioni della società civile, i ricercatori, il pubblico in generale e tutte le parti interessate, ad esprimersi in merito alle opzioni presentate di seguito e a contribuire al futuro processo decisionale della Commissione in questo settore.

1. INTRODUZIONE

Poiché la tecnologia digitale diventa una parte sempre più centrale di tutti gli aspetti della vita delle persone, queste ultime dovrebbero potersi fidare di tale tecnologia. L'affidabilità è inoltre un prerequisito per la sua adozione. Si tratta di un'opportunità per l'Europa, dato il suo forte attaccamento ai valori e allo Stato di diritto, nonché la sua comprovata capacità di costruire prodotti e prestare servizi affidabili, sicuri e sofisticati dal settore aeronautico a quello energetico, automobilistico e delle apparecchiature mediche.

La crescita economica sostenibile attuale e futura e il benessere sociale dell'Europa si basano sempre di più sul valore creato dai dati. L'IA è una delle più importanti applicazioni dell'economia dei dati.

¹ L'intelligenza artificiale per l'Europa, COM(2018) 237 final.

² https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_it.pdf.

Oggi la maggior parte dei dati riguarda i consumatori ed è conservata e elaborata in infrastrutture centrali basate su cloud. Un'ampia fetta dei dati di domani, ben più abbondanti di quelli di oggi, proverrà invece dall'industria, dalle imprese e dal settore pubblico e sarà conservata in vari sistemi, in particolare dispositivi di calcolo funzionanti ai margini della rete. Ciò apre nuove opportunità per l'Europa, che ha una posizione forte nel settore del digitale e delle applicazioni tra imprese (*business-to-business*), ma ha una posizione relativamente debole per quanto riguarda le piattaforme destinate ai consumatori.

Semplificando possiamo dire che l'IA è un insieme di tecnologie che combina dati, algoritmi e potenza di calcolo. I progressi compiuti nell'ambito del calcolo e la crescente disponibilità di dati sono pertanto fattori determinanti per l'attuale crescita dell'IA. L'Europa può combinare i suoi punti di forza industriali e tecnologici con un'infrastruttura digitale di elevata qualità e un quadro normativo basato sui suoi valori fondamentali per **diventare un leader mondiale nell'innovazione nell'economia dei dati e nelle sue applicazioni**, come indicato nella strategia europea per i dati³. Su questa base l'Europa può sviluppare un ecosistema di IA che consenta alla sua società e alla sua economia nel loro complesso di godere dei benefici apportati dalla tecnologia:

- i **cittadini** potranno usufruire di nuovi vantaggi, ad esempio una migliore assistenza sanitaria, un minor numero di guasti degli elettrodomestici, sistemi di trasporto più sicuri e più puliti e servizi pubblici migliori;
- nello sviluppo delle **imprese** sarà possibile, ad esempio, avvalersi di nuove generazioni di prodotti e servizi nei settori in cui l'Europa è particolarmente forte (macchinari, trasporti, cibersicurezza, agricoltura, economia verde e circolare, assistenza sanitaria e settori ad alto valore aggiunto come la moda e il turismo); e
- i servizi di **interesse pubblico** potranno beneficiare, ad esempio, della riduzione dei costi di fornitura di servizi (trasporti, istruzione, energia e gestione dei rifiuti), migliorando la sostenibilità dei prodotti⁴ e dotando le forze dell'ordine di strumenti appropriati per garantire la sicurezza dei cittadini⁵, con adeguate garanzie quanto al rispetto dei loro diritti e delle loro libertà.

Dato l'impatto significativo che l'intelligenza artificiale può avere sulla nostra società e la necessità di creare maggiore fiducia, è essenziale che l'IA europea sia fondata sui nostri valori e diritti fondamentali quali la dignità umana e la tutela della privacy.

L'impatto dei sistemi di IA dovrebbe inoltre essere considerato non solo da una prospettiva individuale, ma anche dal punto di vista della società nel suo complesso. L'uso dei sistemi di IA può svolgere un ruolo significativo nel conseguimento degli obiettivi di sviluppo sostenibile e nel sostegno al processo democratico e ai diritti sociali. Con le sue recenti proposte nell'ambito del Green Deal europeo⁶, l'Europa è in prima linea nella risposta alle sfide legate al clima e all'ambiente. Le tecnologie digitali quali l'IA sono fattori abilitanti fondamentali per conseguire gli obiettivi del Green Deal. Data la

³ COM(2020) 66 final.

⁴ L'IA e la digitalizzazione in generale sono fattori abilitanti fondamentali per gli ambiziosi obiettivi del Green Deal europeo. Tuttavia l'attuale impronta ambientale del settore delle tecnologie dell'informazione e della comunicazione è stimata a oltre il 2 % di tutte le emissioni globali. La strategia digitale europea che accompagna il presente libro bianco propone misure per la trasformazione verde del settore digitale.

⁵ Gli strumenti di IA possono costituire un'opportunità per migliorare la protezione dei cittadini dell'UE dalla criminalità e dagli atti di terrorismo. Tali strumenti potrebbero, ad esempio, contribuire a individuare la propaganda terroristica online, scoprire transazioni sospette nelle vendite di prodotti pericolosi, individuare oggetti pericolosi o sostanze o prodotti illeciti nascosti, offrire assistenza ai cittadini in situazioni di emergenza e contribuire a guidare il personale di primo intervento.

⁶ COM(2019) 640 final.

crescente importanza dell'IA, l'impatto ambientale dei sistemi di IA deve essere debitamente preso in considerazione durante il loro intero ciclo di vita e lungo l'intera catena di approvvigionamento, ad esempio per quanto riguarda l'uso di risorse per l'addestramento degli algoritmi e la conservazione dei dati.

È necessario un approccio comune europeo all'IA per raggiungere dimensioni sufficienti ed evitare la frammentazione del mercato unico. L'introduzione di iniziative nazionali rischia di compromettere la certezza del diritto, di indebolire la fiducia dei cittadini e di ostacolare l'emergere di un'industria europea dinamica.

Il presente libro bianco presenta opzioni strategiche che consentano uno sviluppo sicuro e affidabile dell'IA in Europa, nel pieno rispetto dei valori e dei diritti dei cittadini dell'UE. I principali elementi costitutivi del presente libro bianco sono i seguenti:

- il quadro strategico che stabilisce misure per allineare gli sforzi a livello europeo, nazionale e regionale. Tramite un partenariato tra il settore pubblico e privato, l'obiettivo di tale quadro è mobilitare risorse per conseguire un "**ecosistema di eccellenza**" lungo l'intera catena del valore, a cominciare dalla ricerca e dall'innovazione, e creare i giusti incentivi per accelerare l'adozione di soluzioni basate sull'IA, anche da parte delle piccole e medie imprese (PMI);
- gli elementi chiave di un futuro quadro normativo per l'IA in Europa, che creerà un "**ecosistema di fiducia**" unico. A tal fine, deve garantire il rispetto delle norme dell'UE, comprese le norme a tutela dei diritti fondamentali e dei diritti dei consumatori, in particolare per i sistemi di IA ad alto rischio gestiti nell'UE⁷. La costruzione di un ecosistema di fiducia è un obiettivo strategico in sé e dovrebbe dare ai cittadini la fiducia di adottare applicazioni di IA e alle imprese e alle organizzazioni pubbliche la certezza del diritto necessaria per innovare utilizzando l'IA. La Commissione sostiene con forza un approccio antropocentrico basato sulla comunicazione "Creare fiducia nell'intelligenza artificiale antropocentrica"⁸ e terrà conto anche dei contributi ottenuti durante la fase pilota degli orientamenti etici elaborati dal gruppo di esperti ad alto livello sull'IA.

La strategia europea per i dati che accompagna il presente libro bianco ha l'obiettivo di far sì che l'Europa diventi l'economia agile basata sui dati più attraente, sicura e dinamica del mondo, mettendo a sua disposizione i dati necessari a migliorare le decisioni e la vita di tutti i suoi cittadini. La strategia definisce una serie di misure strategiche necessarie per raggiungere questo obiettivo, tra cui la mobilitazione degli investimenti pubblici e privati. Le implicazioni dell'intelligenza artificiale, dell'Internet delle cose e di altre tecnologie digitali per la legislazione in materia di sicurezza e responsabilità sono infine analizzate nella relazione della Commissione che accompagna il presente libro bianco.

2. TRARRE VANTAGGIO DAI PUNTI DI FORZA DEI MERCATI INDUSTRIALI E PROFESSIONALI

L'Europa si trova in una posizione ideale per beneficiare del potenziale dell'IA, non solo in quanto utente, ma anche come creatore e produttore di questa tecnologia. Dispone di centri di ricerca di eccellenza, start-up innovative, di una posizione di leadership a livello mondiale nella robotica e di settori competitivi dell'industria manifatturiera e dei servizi, dal settore automobilistico all'assistenza sanitaria, all'energia, ai servizi finanziari e all'agricoltura. L'Europa ha sviluppato una potente

⁷ Potrebbero essere necessarie ulteriori disposizioni per prevenire e contrastare l'abuso dell'IA per scopi criminali, ma ciò non rientra nel campo di applicazione del presente libro bianco.

⁸ COM(2019) 168 final.

infrastruttura di calcolo (ad esempio i computer ad alte prestazioni), essenziale per il funzionamento dell'IA. L'Europa dispone inoltre di grandi volumi di dati pubblici e industriali, il cui potenziale è attualmente sottoutilizzato, e di punti di forza industriali riconosciuti nell'ambito dei sistemi digitali sicuri a basso consumo energetico che sono essenziali per l'ulteriore sviluppo dell'IA.

Lo sfruttamento della capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione nonché nelle competenze digitali, come l'alfabetizzazione ai dati (*data literacy*), accrescerà la sovranità tecnologica dell'Europa nell'ambito delle tecnologie e infrastrutture abilitanti fondamentali per l'economia dei dati. Le infrastrutture dovrebbero sostenere la creazione di pool europei di dati che consentano lo sviluppo di un'IA affidabile basata su valori e regole europei.

L'Europa dovrebbe sfruttare i propri punti di forza per far crescere la propria posizione negli ecosistemi e lungo la catena del valore, da determinati settori della produzione di hardware al software e ai servizi. Ciò sta già avvenendo, in una certa misura. L'Europa produce più di un quarto di tutti i robot di servizio industriali e professionali (ad esempio per l'agricoltura di precisione, la sicurezza, la salute e la logistica) e svolge un ruolo importante nello sviluppo e nell'utilizzo di applicazioni software per le imprese e le organizzazioni (applicazioni *business-to-business* quali i software per l'ingegneria, il design, e la pianificazione delle risorse aziendali), nonché di applicazioni a sostegno dell'e-government e dell'"impresa intelligente".

L'Europa svolge un ruolo guida per quanto riguarda la diffusione dell'IA nell'industria manifatturiera: oltre la metà dei principali fabbricanti implementano almeno un'istanza di IA nelle operazioni di fabbricazione⁹.

Uno dei motivi alla base della posizione forte dell'Europa nella ricerca è il programma di finanziamento dell'UE, che si è dimostrato fondamentale per mettere in comune le azioni, evitare duplicazioni e mobilitare gli investimenti pubblici e privati negli Stati membri. Nel corso degli ultimi tre anni i finanziamenti dell'UE per la ricerca e l'innovazione nell'IA sono saliti a 1,5 miliardi di EUR, ossia un aumento del 70 % rispetto al periodo precedente.

Tuttavia, gli investimenti nella ricerca e nell'innovazione in Europa sono ancora nettamente inferiori agli investimenti pubblici e privati in altre regioni del mondo. Nel 2016 sono stati investiti in Europa circa 3,2 miliardi di EUR nell'IA, rispetto a circa 12,1 miliardi di EUR in America settentrionale e 6,5 miliardi di EUR in Asia¹⁰. L'Europa ha quindi bisogno di aumentare in modo significativo i suoi livelli di investimento. Il piano coordinato sull'IA¹¹, sviluppato insieme agli Stati membri, si sta rivelando un buon punto di partenza per rafforzare la cooperazione in materia di IA in Europa e per creare sinergie al fine di massimizzare gli investimenti nella catena del valore dell'IA.

3. COGLIERE LE OPPORTUNITÀ FUTURE: LA PROSSIMA ONDATA DI DATI

Sebbene l'Europa sia attualmente in una posizione più debole per quanto riguarda le applicazioni destinate ai consumatori e le piattaforme online, che si traduce in uno svantaggio competitivo nell'accesso ai dati, sono in corso importanti cambiamenti nel valore e nel riutilizzo di dati tra diversi settori. Il volume dei dati prodotti a livello mondiale è in rapida crescita, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2025¹². Ogni nuova ondata di dati offre all'Europa l'opportunità di farsi spazio nell'economia agile basata sui dati e diventare un leader mondiale nel settore. Inoltre le

⁹ Seguita dal Giappone (30 %) e dagli Stati Uniti (28 %). Fonte: CapGemini (2019).

¹⁰ *10 imperatives for Europe in the age of AI and automation* (10 imperativi per l'Europa nell'era dell'IA e dell'automazione), McKinsey (2017).

¹¹ COM(2018) 795 final.

¹² IDC (2019).

modalità di conservazione e elaborazione dei dati cambieranno significativamente nei prossimi cinque anni. Attualmente l'80 % delle elaborazioni e delle analisi dei dati che hanno luogo nel cloud vengono effettuate in centri di dati e strutture di calcolo centralizzate e il 20 % in oggetti connessi intelligenti, quali automobili, elettrodomestici o robot di fabbricazione, e in strutture di calcolo vicine all'utente ("edge computing"). Entro il 2025 tali proporzioni cambieranno in modo significativo¹³.

L'Europa è leader mondiale nel settore dell'elettronica a basso consumo, che è fondamentale per la prossima generazione di processori specializzati per l'IA. Tale mercato è attualmente dominato da soggetti extra UE, ma questa situazione potrebbe cambiare grazie sia a progetti quali l'iniziativa europea in materia di processori, che si concentra sullo sviluppo di sistemi di calcolo a basso consumo sia per l'*edge computing* ad alte prestazioni sia per la prossima generazione di calcolo ad alte prestazioni, sia al lavoro dell'impresa comune per le tecnologie digitali chiave, il cui avvio è stato proposto per il 2021. L'Europa è inoltre leader nelle soluzioni neuromorfiche¹⁴, che sono ideali per l'automazione dei processi industriali (industria 4.0) e dei modi di trasporto e possono migliorare l'efficienza energetica di vari ordini di grandezza.

I recenti progressi nell'ambito del calcolo quantistico genereranno un aumento esponenziale della capacità di elaborazione¹⁵. L'Europa può essere all'avanguardia in questa tecnologia grazie all'alto livello accademico nell'ambito del calcolo quantistico, nonché alla forte posizione dell'industria europea nell'ambito dei simulatori quantistici e degli ambienti di programmazione per il calcolo quantistico. Le iniziative europee volte ad aumentare la disponibilità di strutture di prova e sperimentazione quantistica contribuiranno all'applicazione di queste nuove soluzioni quantistiche a numerosi settori industriali e accademici.

Parallelamente, l'Europa continuerà a guidare il progresso per quanto riguarda le basi algoritmiche dell'IA, basandosi sulla propria eccellenza scientifica. È necessario creare collegamenti tra discipline che attualmente lavorano separatamente, come l'apprendimento automatico (*machine learning*) e l'apprendimento profondo (*deep learning*), che sono caratterizzati da una limitata interpretabilità e dalla necessità di una grande quantità di dati per addestrare i modelli e apprendere mediante correlazioni, e gli approcci simbolici, in cui le regole sono create mediante l'intervento umano. Combinare il ragionamento simbolico con le reti neurali profonde può aiutarci a rendere maggiormente spiegabili i risultati dell'IA.

4. UN ECOSISTEMA DI ECCELLENZA

Per costruire un ecosistema di eccellenza che possa sostenere lo sviluppo e l'adozione dell'IA nell'economia e nella pubblica amministrazione dell'UE è necessario intensificare le azioni su più livelli.

A. COLLABORAZIONE CON GLI STATI MEMBRI

Nell'ambito dell'attuazione della strategia sull'IA adottata nell'aprile 2018¹⁶, la Commissione ha presentato, nel dicembre 2018, un piano coordinato predisposto insieme agli Stati membri per promuovere lo sviluppo e l'utilizzo dell'intelligenza artificiale in Europa¹⁷.

¹³ Gartner (2017).

¹⁴ Per soluzioni neuromorfiche si intendono tutti i sistemi di circuiti integrati su larghissima scala (VLSI) che imitano le architetture neurobiologiche presenti nel sistema nervoso.

¹⁵ I computer quantistici avranno la capacità di elaborare in un tempo inferiore al secondo set di dati molto più grandi rispetto ai computer attuali con le più alte prestazioni, consentendo lo sviluppo di nuove applicazioni di IA in tutti i settori.

¹⁶ L'intelligenza artificiale per l'Europa, COM(2018) 237 final.

Tale piano propone circa 70 azioni comuni per una cooperazione più stretta ed efficiente tra gli Stati membri e la Commissione in settori chiave quali la ricerca, gli investimenti, l'adozione da parte del mercato, le competenze e i talenti, i dati e la cooperazione internazionale. Si prevede che il piano durerà fino al 2027, con monitoraggi e revisioni periodiche.

L'obiettivo è di massimizzare l'impatto degli investimenti in ricerca, innovazione e diffusione dell'IA, valutare le strategie nazionali in materia di IA nonché sviluppare ed estendere il piano coordinato sull'IA in collaborazione con gli Stati membri.

- *Azione 1: la Commissione, tenendo conto dei risultati della consultazione pubblica sul libro bianco, proporrà agli Stati membri una revisione del piano coordinato da adottare entro la fine del 2020.*

Il finanziamento dell'IA a livello di UE dovrebbe attrarre e mettere in comune gli investimenti in settori in cui gli sforzi richiesti vanno al di là di quanto i singoli Stati membri possono ottenere. L'obiettivo è attrarre, nei prossimi dieci anni, oltre 20 miliardi di EUR¹⁷ di investimenti totali annui nell'IA nell'Unione europea. Per stimolare gli investimenti pubblici e privati, l'UE metterà a disposizione risorse provenienti dal programma Europa digitale, da Orizzonte Europa e dai Fondi strutturali e di investimento europei per far fronte alle esigenze delle regioni meno sviluppate e delle zone rurali.

Il piano coordinato potrebbe inoltre considerare il benessere della società e dell'ambiente quale principio chiave per l'IA. I sistemi di IA promettono di contribuire ad affrontare le preoccupazioni più urgenti, tra cui i cambiamenti climatici e il degrado ambientale; è importante che ciò avvenga in modo compatibile con l'ambiente. La stessa IA può e dovrebbe esaminare in modo critico l'uso di risorse e il consumo di energia ed essere addestrata ad effettuare scelte positive per l'ambiente. La Commissione, in collaborazione con gli Stati membri, prenderà in considerazione le opzioni volte a incoraggiare e promuovere soluzioni di IA che svolgano tali funzioni.

B. CONCENTRARE GLI SFORZI DELLA COMUNITÀ DELLA RICERCA E DELL'INNOVAZIONE

L'Europa non può permettersi di mantenere l'attuale panorama frammentato dei centri di competenza, in cui nessuno di questi raggiunge le dimensioni necessarie per competere con i principali istituti a livello mondiale. È indispensabile creare più reti e sinergie tra diversi centri di ricerca europei sull'intelligenza artificiale e allineare i loro sforzi per migliorarne l'eccellenza, trattenere e attrarre i migliori ricercatori e sviluppare le migliori tecnologie. L'Europa ha bisogno di un centro di ricerca, innovazione e competenza di riferimento che coordini tali sforzi, che rappresenti un referente mondiale di eccellenza nell'IA e che possa attrarre gli investimenti e i migliori talenti nel settore.

I centri e le reti dovrebbero concentrarsi nei settori in cui l'Europa ha il potenziale per diventare leader a livello mondiale, come l'industria, la salute, i trasporti, la finanza, le catene del valore agroalimentari, l'energia/l'ambiente, il settore forestale, l'osservazione della Terra e lo spazio. In tutti questi settori si sta svolgendo la corsa alla leadership mondiale e l'Europa offre notevoli potenzialità, conoscenze e

¹⁷ [Piano coordinato sull'intelligenza artificiale, COM \(2018\) 795 final.](#)

¹⁸ COM(2018) 237 final.

competenze¹⁹. Altrettanto importante è la creazione di siti di prova e sperimentazione a sostegno dello sviluppo e della successiva diffusione di nuove applicazioni di IA.

- *Azione 2: la Commissione agevolerà la creazione di centri di prova e di eccellenza che possano combinare gli investimenti europei, nazionali e privati, eventualmente anche con un nuovo strumento giuridico. Nell'ambito del quadro finanziario pluriennale per il periodo 2021-2027 la Commissione ha proposto di dedicare un importo ambizioso a sostegno di centri di prova di riferimento a livello mondiale in Europa nel quadro del programma Europa digitale e di integrare tale misura, ove opportuno, con azioni di ricerca e innovazione nel quadro di Orizzonte Europa.*

C. COMPETENZE

L'approccio europeo all'IA dovrà essere sostenuto da misure fortemente incentrate sulle competenze al fine di sopprimere alla loro mancanza²⁰. La Commissione presenterà a breve un rafforzamento dell'agenda per le competenze, che mira a garantire che tutti in Europa possano beneficiare delle trasformazioni verde e digitale dell'economia dell'UE. Le iniziative potrebbero anche comprendere il sostegno alle autorità di regolamentazione settoriali per migliorare le loro competenze in materia di IA al fine di attuare in modo efficace e efficiente le norme pertinenti. Il piano d'azione per l'istruzione digitale aggiornato contribuirà a migliorare l'uso dei dati e delle tecnologie basate sull'IA, come l'apprendimento e l'analisi predittiva, al fine di migliorare i sistemi di istruzione e di formazione e renderli pronti per l'era digitale. Il piano contribuirà inoltre a far crescere la consapevolezza in merito all'IA a tutti i livelli di istruzione, al fine di preparare i cittadini a decisioni informate che saranno sempre più influenzate dall'IA.

Lo sviluppo delle competenze necessarie per lavorare nel settore dell'IA e il miglioramento del livello delle competenze della forza lavoro per prepararla a una trasformazione guidata dall'IA saranno le priorità della revisione del piano coordinato sull'IA che sarà effettuata insieme agli Stati membri. Ciò potrebbe includere la trasformazione della lista di controllo degli orientamenti etici in un "programma di studi" indicativo per gli sviluppatori di IA che sarà reso disponibile come risorsa per gli istituti di formazione. Occorre impegnarsi in modo particolare per aumentare il numero di donne che ricevono una formazione e sono impiegate in questo settore.

Inoltre un centro di ricerca e innovazione di riferimento per l'IA in Europa attirerebbe talenti da tutto il mondo, grazie alle possibilità che potrebbe offrire, oltre a sviluppare e diffondere l'eccellenza in competenze che si radicano e si sviluppano in tutta Europa.

- *Azione 3: istituire e sostenere, attraverso il pilastro relativo alle competenze avanzate del programma Europa digitale, reti che collegano le università e gli istituti di istruzione superiore principali, al fine di attrarre i migliori professori e scienziati e di offrire corsi di laurea magistrale di eccellenza a livello mondiale nel campo dell'IA.*

Oltre al miglioramento del livello delle competenze, i lavoratori e i datori di lavoro sono interessati direttamente dalla progettazione e dall'uso dei sistemi di IA sul luogo di lavoro. Il coinvolgimento delle parti sociali sarà un fattore cruciale per garantire un approccio antropocentrico all'IA sul lavoro.

¹⁹ Anche il futuro Fondo europeo per la difesa e la cooperazione strutturata permanente (PESCO) offrirà opportunità per la ricerca e lo sviluppo in materia di IA. Tali progetti dovrebbero essere sincronizzati con i più ampi programmi civili dell'UE dedicati all'IA.

²⁰ <https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu>.

D. MAGGIORE ATTENZIONE ALLE PMI

Sarà inoltre importante garantire che le PMI possano accedere all'IA e utilizzarla. A tal fine, è opportuno rafforzare ulteriormente i poli dell'innovazione digitale²¹ e la piattaforma di IA on demand²² e promuovere la collaborazione tra le PMI. Il programma Europa digitale sarà determinante per conseguire questi obiettivi. Mentre tutti i poli dell'innovazione digitale dovrebbero fornire sostegno alle PMI affinché comprendano e adottino l'IA, sarà importante che almeno un polo dell'innovazione per Stato membro sia altamente specializzato in IA.

Le PMI e le start-up avranno bisogno di accedere ai finanziamenti al fine di adattare i loro processi o di innovare usando l'IA. Basandosi sul prossimo fondo pilota per gli investimenti di 100 milioni di EUR per l'IA e la blockchain, la Commissione rafforzerà ulteriormente l'accesso ai finanziamenti per l'IA nell'ambito di InvestEU²³. L'IA è citata esplicitamente tra le aree ammissibili per l'utilizzo della garanzia InvestEU.

- *Azione 4: la Commissione collaborerà con gli Stati membri per garantire che almeno un polo dell'innovazione digitale per Stato membro sia altamente specializzato in IA. I poli dell'innovazione digitale possono ricevere sostegno nell'ambito del programma Europa digitale.*
- *La Commissione e il Fondo europeo per gli investimenti avvieranno un progetto pilota con un investimento di 100 milioni di EUR nel primo trimestre del 2020 per fornire finanziamenti con capitale di rischio per sviluppi innovativi nel campo dell'IA. Fatto salvo l'accordo definitivo sul QFP, l'intenzione della Commissione è di far crescere significativamente tale progetto a partire dal 2021 mediante InvestEU.*

E. PARTENARIATO CON IL SETTORE PRIVATO

È altresì essenziale garantire che il settore privato sia pienamente coinvolto nella definizione dell'agenda per la ricerca e l'innovazione e fornisca il necessario livello di coinvestimenti. Per far ciò è necessario istituire un ampio partenariato pubblico-privato, nonché assicurarsi l'impegno dei massimi dirigenti delle società interessate.

- *Azione 5: nel contesto di Orizzonte Europa, la Commissione istituirà un nuovo partenariato pubblico-privato per l'IA, i dati e la robotica, al fine di unire gli sforzi, garantire il coordinamento della ricerca e dell'innovazione nell'IA, collaborare con altri partenariati pubblico-privati di Orizzonte Europa e lavorare insieme alle strutture di prova e ai poli dell'innovazione digitale precedentemente menzionati.*

²¹ ec.europa.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.

²² www.Ai4eu.eu.

²³ Europe.eu/investeu.

F. PROMUOVERE L'ADOZIONE DELL'IA NEL SETTORE PUBBLICO

È essenziale che le amministrazioni pubbliche, gli ospedali, i servizi di pubblica utilità e di trasporto, le autorità di vigilanza finanziaria e altri settori di interesse pubblico inizino rapidamente a utilizzare nelle loro attività prodotti e servizi che si basano sull'IA. Un'attenzione particolare sarà rivolta ai settori dell'assistenza sanitaria e dei trasporti, in cui la tecnologia è abbastanza matura da consentire una diffusione su vasta scala.

- *Azione 6: la Commissione avvierà dialoghi settoriali aperti e trasparenti dando priorità agli operatori del servizio pubblico, delle amministrazioni rurali e dell'assistenza sanitaria, al fine di presentare un piano d'azione che facili lo sviluppo, la sperimentazione e l'adozione dell'IA. I dialoghi settoriali saranno utilizzati per elaborare uno specifico "Programma di adozione dell'IA", che sosterrà gli appalti pubblici di sistemi di IA e contribuirà a trasformare le procedure stesse degli appalti pubblici.*

G. GARANTIRE L'ACCESSO AI DATI E ALLE INFRASTRUTTURE DI CALCOLO

Le aree di intervento stabilite nel presente libro bianco sono complementari a quelle del piano presentato in parallelo nella strategia europea per i dati. Migliorare l'accesso ai dati e la gestione degli stessi è una questione fondamentale. Senza dati lo sviluppo dell'IA e di altre applicazioni digitali è impossibile. Questo enorme volume di nuovi dati che deve essere ancora generato rappresenta un'opportunità per l'Europa di assumere una posizione di primo piano nella trasformazione basata sui dati e sull'IA. La promozione di pratiche responsabili in materia di gestione dei dati e la conformità dei dati ai principi FAIR²⁴ contribuiranno a creare fiducia e a garantire la riutilizzabilità dei dati. Altrettanto importante è investire nelle tecnologie e nelle infrastrutture di calcolo chiave.

Nell'ambito del programma Europa digitale la Commissione ha proposto più di 4 miliardi di EUR di finanziamento a sostegno del calcolo quantistico e ad alte prestazioni, compresi l'*edge computing* e l'infrastruttura per l'IA, i dati e il cloud. La strategia europea per i dati sviluppa ulteriormente tali priorità.

H. ASPETTI INTERNAZIONALI

L'Europa si trova nella posizione ideale per esercitare una leadership mondiale costruendo alleanze attorno ai valori condivisi e promuovendo l'uso etico dell'IA. Il lavoro svolto dall'UE nel campo dell'IA ha già influenzato le discussioni a livello internazionale. Nell'elaborare i propri orientamenti etici, il gruppo di esperti ad alto livello ha coinvolto una serie di organizzazioni extra UE e vari osservatori governativi. Parallelamente l'UE è stata coinvolta da vicino nello sviluppo dei principi etici per l'IA dell'OCSE²⁵. Il G20 ha successivamente approvato tali principi nella dichiarazione ministeriale sul commercio e l'economia digitale del giugno 2019.

Allo stesso tempo l'UE riconosce che sono in corso importanti lavori sull'IA in altri consensi multilaterali, tra cui il Consiglio d'Europa, l'Organizzazione delle Nazioni Unite per l'educazione, la scienza e la cultura (UNESCO), l'Organizzazione per la cooperazione e lo sviluppo economici (OCSE), l'Organizzazione mondiale del commercio e l'Unione internazionale delle telecomunicazioni (UIT).

²⁴ *Findable, Accessible, Interoperable and Reusable*, cioè dati reperibili, accessibili, interoperabili e riutilizzabili, come indicato nella relazione finale e nel piano d'azione del gruppo di esperti della Commissione sui dati FAIR, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

²⁵ <https://www.oecd.org/going-digital/ai/principles/>.

Nell'ambito delle Nazioni Unite, l'UE sta lavorando per dare seguito alla relazione del gruppo ad alto livello sulla cooperazione digitale, anche per quanto riguarda la raccomandazione sull'IA.

L'UE continuerà a cooperare in materia di IA con i paesi che condividono gli stessi principi, ma anche con gli attori globali, seguendo un approccio che promuova le regole e i valori dell'UE (ad esempio sostenendo la convergenza normativa verso l'alto, garantendo l'accesso alle risorse fondamentali, compresi i dati, e creando condizioni di parità). La Commissione monitorerà da vicino le politiche dei paesi terzi che limitano i flussi di dati e affronterà le restrizioni indebite nei negoziati commerciali bilaterali e mediante iniziative nell'ambito dell'Organizzazione mondiale del commercio. La Commissione è convinta che la cooperazione internazionale sulle questioni riguardanti l'IA debba basarsi su un approccio che promuova il rispetto dei diritti fondamentali, tra cui la dignità umana, il pluralismo, l'inclusione, la non discriminazione e la protezione della privacy e dei dati personali²⁶, e si adopererà per esportare i suoi valori nel mondo²⁷. È inoltre chiaro che lo sviluppo e l'uso responsabili dell'IA possono essere una forza trainante per conseguire gli obiettivi di sviluppo sostenibile e portare avanti l'Agenda 2030.

5. UN ECOSISTEMA DI FIDUCIA: QUADRO NORMATIVO PER L'IA

L'uso dell'IA, come l'uso di qualunque nuova tecnologia, comporta sia opportunità sia rischi. I cittadini temono di essere privati dei mezzi per difendere i loro diritti e la loro sicurezza di fronte alle asimmetrie informative del processo decisionale algoritmico, mentre le imprese sono preoccupate per l'incertezza giuridica. L'IA può contribuire a proteggere la sicurezza dei cittadini e consentire loro di godere dei diritti fondamentali, tuttavia i cittadini temono anche che l'intelligenza artificiale possa avere effetti indesiderati o essere addirittura utilizzata per scopi dolosi. A queste preoccupazioni occorre dare una risposta. Oltre alla mancanza di investimenti e di competenze, la mancanza di fiducia è infatti uno dei fattori principali che frenano una più ampia adozione dell'IA.

Per questo motivo il 25 aprile 2018 la Commissione ha definito una strategia per l'IA²⁸ che affronta gli aspetti socioeconomici parallelamente a un aumento degli investimenti nella ricerca, nell'innovazione e nelle capacità di IA in tutta l'UE, e ha concordato con gli Stati membri un piano coordinato²⁹ per l'allineamento delle strategie. La Commissione ha inoltre istituito un gruppo di esperti ad alto livello che, nell'aprile 2019, ha pubblicato orientamenti per un'IA affidabile³⁰.

La Commissione ha pubblicato una comunicazione³¹ in cui accoglie con favore i sette requisiti fondamentali individuati negli orientamenti del gruppo di esperti ad alto livello:

- intervento e sorveglianza umani,
- robustezza tecnica e sicurezza,
- riservatezza e governance dei dati,
- trasparenza,
- diversità, non discriminazione ed equità,
- benessere sociale e ambientale, e

²⁶Nell'ambito dello strumento di partenariato, la Commissione finanzierà un progetto di 2,5 milioni di EUR che ageverrà la cooperazione con i partner che condividono gli stessi principi, al fine di promuovere gli orientamenti etici dell'UE in materia di IA e di adottare principi comuni e conclusioni operative.

²⁷ Presidente Von der Leyen, Un'unione più ambiziosa – Il mio programma per l'Europa, pag. 17.

²⁸ COM(2018) 237 final.

²⁹ COM(2018) 795 final.

³⁰ <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>.

³¹ COM(2019) 168 final.

- accountability.

Negli orientamenti è compresa inoltre una lista di controllo per l'uso pratico da parte delle imprese. Nella seconda metà del 2019, oltre 350 organizzazioni hanno testato tale lista di controllo e hanno inviato un feedback che il gruppo ad alto livello sta utilizzando per rivedere i propri orientamenti; la conclusione di tale revisione è prevista per giugno 2020. Un risultato fondamentale emerso durante tale processo di feedback è che, sebbene i regimi giuridici o normativi esistenti prevedano già numerose prescrizioni, quelle relative alla trasparenza, alla tracciabilità e alla sorveglianza umana non sono contemplate dalla legislazione vigente in molti settori economici.

In aggiunta a questa serie di orientamenti non vincolanti del gruppo di esperti ad alto livello, e in linea con gli orientamenti politici della presidente, un quadro normativo europeo chiaro rafforzerebbe la fiducia dei consumatori e delle imprese nell'IA e accelererebbe quindi l'adozione della tecnologia. Tale quadro normativo dovrebbe essere coerente con altre azioni volte a promuovere la capacità di innovazione e la competitività dell'Europa in questo settore. Deve inoltre garantire risultati ottimali sul piano sociale, ambientale ed economico nonché il rispetto della legislazione, dei principi e dei valori dell'UE. Ciò è particolarmente importante negli ambiti che interessano direttamente i diritti dei cittadini, ad esempio nel caso delle applicazioni di IA per le forze dell'ordine e la magistratura.

Coloro che si occupano di sviluppare e applicare l'IA sono già soggetti alla legislazione europea in materia di diritti fondamentali (ad esempio per quanto riguarda la protezione dei dati, la privacy, la non discriminazione) e di protezione dei consumatori e alle norme in materia di responsabilità e di sicurezza dei prodotti. I consumatori si attendono lo stesso livello di sicurezza e di rispetto dei loro diritti, indipendentemente dal fatto che un prodotto o un sistema si basi sull'IA. Tuttavia determinate caratteristiche specifiche dell'IA (ad esempio l'opacità) possono rendere più difficile l'applicazione e il rispetto di tale legislazione. Per questo motivo è necessario esaminare se la legislazione attuale sia in grado di affrontare i rischi connessi all'IA e se possa essere applicata in modo efficace, se siano necessarie modifiche della legislazione o se sia necessaria una nuova legislazione.

Considerata la rapida evoluzione dell'IA, il quadro normativo deve lasciare spazio a ulteriori sviluppi. Tutte le modifiche dovrebbe essere limitate a problemi chiaramente individuati per i quali esistono soluzioni praticabili.

Gli Stati membri hanno rilevato l'attuale assenza di un quadro europeo comune. La commissione tedesca per l'etica dei dati ha chiesto un sistema normativo su cinque livelli basato sul rischio che spazi dall'assenza di regolamentazione per i sistemi di IA più innocui a un divieto totale per i più pericolosi. La Danimarca ha appena avviato il prototipo di un "marchio per l'etica dei dati". Malta ha introdotto un sistema di certificazione volontaria per l'IA. Se l'UE non riesce a fornire un approccio comune a livello di Unione, esiste un rischio reale di frammentazione del mercato interno, che comprometterebbe gli obiettivi di fiducia, certezza del diritto e adozione da parte del mercato.

Un solido quadro normativo europeo per un'IA affidabile proteggerà tutti i cittadini europei e contribuirà a creare un mercato interno senza attriti che favorirà l'ulteriore sviluppo e l'adozione dell'IA rafforzando la base industriale dell'Europa nel campo dell'IA.

A. DEFINIZIONE DEL PROBLEMA

L'IA può essere estremamente utile, ad esempio in quanto può rendere prodotti e processi più sicuri, ma può anche risultare dannosa. Tale danno può essere di natura sia materiale (quando incide sulla salute e sulla sicurezza delle persone, provocando perdite di vite umane o danni patrimoniali) sia immateriale (quando causa una perdita della privacy, restrizioni alla libertà di espressione, pregiudizi alla dignità umana o discriminazioni, ad esempio nell'accesso all'occupazione), e può riguardare

un'ampia gamma di rischi. Il quadro normativo dovrebbe concentrarsi su come ridurre al minimo i diversi rischi di danno potenziale, soprattutto quelli più significativi.

I rischi principali connessi all'uso dell'IA riguardano l'applicazione di norme intese a tutelare i diritti fondamentali (comprese la protezione dei dati personali e della privacy e la non discriminazione), nonché le questioni legate alla sicurezza³² e alla responsabilità.

Rischi per i diritti fondamentali, comprese la protezione dei dati personali e della privacy e la non discriminazione

L'uso dell'IA può pregiudicare i valori su cui si fonda l'Unione e causare violazioni dei diritti fondamentali³³, compresi i diritti alle libertà di espressione e di riunione, la dignità umana, la non discriminazione fondata sul sesso, sulla razza, sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale (ove applicabili in determinati settori), la protezione dei dati personali e della vita privata³⁴ o il diritto a un ricorso giurisdizionale effettivo e a un giudice imparziale, nonché la tutela dei consumatori. Tali rischi potrebbero derivare da difetti nella progettazione complessiva dei sistemi di IA (anche per quanto riguarda la sorveglianza umana) o dall'uso di dati senza che ne siano state corrette le eventuali distorsioni (ad esempio se un sistema è addestrato utilizzando solo o principalmente dati riguardanti gli uomini, il che comporta risultati non ottimali per quanto concerne le donne).

L'IA può svolgere molte funzioni che in precedenza potevano essere esercitate solo dagli esseri umani. I cittadini e le persone giuridiche saranno pertanto sempre più soggette ad azioni realizzate e a decisioni prese da sistemi di IA o con la loro assistenza; si tratta di un risultato non sempre facile da comprendere e cui è difficile opporsi in modo efficace ove necessario. L'IA aumenta inoltre le possibilità di seguire e analizzare le abitudini quotidiane delle persone. Vi è ad esempio il rischio potenziale che l'IA venga utilizzata, in violazione della normativa dell'UE sulla protezione dei dati e di altre norme, dalle autorità statali o da altri soggetti a fini di sorveglianza di massa, oppure dai datori di lavoro per osservare il comportamento dei loro dipendenti. Poiché permette di analizzare grandi quantità di dati e di individuare collegamenti tra di essi, l'IA può essere usata anche per ricostruire e deanonymizzare dati riguardanti le persone, il che implica nuovi rischi per la protezione dei dati personali anche in relazione a set di dati che di per sé non contengono dati personali. L'IA è utilizzata anche dagli intermediari online per stabilire priorità riguardo alle informazioni da fornire ai loro utenti oppure a fini di moderazione dei contenuti. I dati trattati, le modalità con cui vengono progettate le applicazioni e il margine di intervento umano possono incidere sui diritti alla libertà di espressione, alla protezione dei dati personali e alla privacy nonché sulle libertà politiche.

³² Ivi comprese le questioni legate alla cibersicurezza, alle applicazioni dell'IA nelle infrastrutture critiche o all'uso illecito dell'IA.

³³ Una ricerca del Consiglio d'Europa dimostra che l'uso dell'IA potrebbe avere ripercussioni su numerosi diritti fondamentali, <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>.

³⁴ Il regolamento generale sulla protezione dei dati (*General Data Protection Regulation*, GDPR) e la direttiva relativa alla vita privata e alle comunicazioni elettroniche (il nuovo regolamento sull'e-Privacy è attualmente in fase di negoziazione) affrontano tali rischi, ma potrebbe esservi la necessità di valutare se i sistemi di IA comportino rischi ulteriori. La Commissione monitorerà e valuterà l'applicazione del GDPR in modo costante.

Alcuni algoritmi dell'IA, se usati per prevedere il rischio di recidiva di atti delittuosi, possono riflettere distorsioni legate alla razza e al genere, prevedendo probabilità di rischio di recidiva diverse per le donne rispetto agli uomini, oppure per i cittadini di un determinato paese rispetto agli stranieri. Fonte: Tolan S., Miron M., Gomez E. e Castillo C. "Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia" (Perché l'apprendimento automatico può portare a risultati iniqui: risultanze della valutazione dei rischi per la giustizia minorile in Catalogna), Best Paper Award, International Conference on AI and Law, 2019.

Alcuni programmi di IA per l'analisi facciale riflettono distorsioni legate al genere e alla razza, in quanto identificano con maggiore facilità il genere degli uomini di carnagione chiara mentre commettono più errori nel determinare il genere delle donne di pelle più scura. Fonte: Joy Buolamwini, Timnit Gebru; *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (Atti della 1^a conferenza sull'equità, sulla responsabilità e sulla trasparenza), PMLR 81:77-91, 2018.

Le distorsioni e le discriminazioni rappresentano un rischio intrinseco di qualunque attività sociale od economica. Il processo decisionale umano non è immune da errori e distorsioni. Queste stesse distorsioni, se presenti nell'IA, potrebbero tuttavia avere effetti molto maggiori e colpire o discriminare numerose persone in assenza dei meccanismi di controllo sociale che disciplinano il comportamento umano³⁵. Ciò può accadere anche quando il sistema di IA "apprende" nel corso del suo funzionamento. In tali casi, in cui i risultati non potevano essere evitati o anticipati in fase di progettazione, i rischi deriveranno non da difetti nella progettazione originale del sistema, bensì dagli effetti pratici delle correlazioni o dei modelli che il sistema individua all'interno di un ampio set di dati.

Le caratteristiche specifiche di molte tecnologie di IA, tra cui l'opacità (effetto "scatola nera"), la complessità, l'imprevedibilità e un comportamento parzialmente autonomo, possono rendere difficile verificare il rispetto delle normative dell'UE in vigore volte a proteggere i diritti fondamentali e possono ostacolarne l'applicazione effettiva. Le autorità preposte all'applicazione della legge e le persone interessate potrebbero non disporre dei mezzi per verificare come sia stata presa una determinata decisione con il coinvolgimento di sistemi di IA e, di conseguenza, se sia stata rispettata la normativa pertinente. Le persone fisiche e giuridiche possono incontrare difficoltà nell'accesso effettivo alla giustizia in situazioni in cui tali decisioni possono avere ripercussioni negative su di loro.

Rischi per la sicurezza e per il funzionamento efficace del regime di responsabilità

Le tecnologie di IA incorporate in prodotti e servizi possono presentare nuovi rischi per la sicurezza degli utenti. Ad esempio, a causa di un difetto della tecnologia di riconoscimento degli oggetti, un'auto a guida autonoma può erroneamente identificare un oggetto sulla strada e provocare un incidente causando lesioni e danni materiali. Analogamente ai rischi per i diritti fondamentali, questi rischi

³⁵ Il Comitato consultivo per le pari opportunità tra uomini e donne della Commissione sta attualmente preparando un parere sull'intelligenza artificiale, che dovrebbe essere adottato all'inizio del 2020, in cui si analizza tra l'altro l'impatto dell'intelligenza artificiale sulla parità di genere. Anche la strategia dell'UE per la parità di genere 2020-2024 affronta il rapporto tra IA e parità di genere. La rete europea di enti nazionali per le pari opportunità (Equinet) pubblicherà una relazione (elaborata da Robin Allen e Dee Masters) intitolata: "Regulating AI: the new role for Equality Bodies – Meeting the new challenges to equality and non-discrimination from increased digitalisation and the use of AI" (Disciplinare l'IA: il nuovo ruolo degli enti per le pari opportunità – Affrontare le nuove sfide che l'aumento della digitalizzazione e l'uso dell'IA comportano per l'uguaglianza e la non discriminazione), pubblicazione attesa per l'inizio del 2020.

possono derivare da difetti nella progettazione delle tecnologie di IA, da problemi riguardanti la disponibilità e la qualità dei dati o da altri problemi inerenti all'apprendimento automatico. Sebbene alcuni di questi rischi non riguardino unicamente prodotti e servizi basati sull'IA, l'uso di quest'ultima può aumentare o aggravare i rischi.

La mancanza di disposizioni chiare in materia di sicurezza che affrontino tali rischi può creare, oltre a rischi per le persone interessate, incertezza giuridica per le imprese che commercializzano nell'UE prodotti che integrano sistemi di IA. È possibile che le autorità preposte alla vigilanza del mercato e all'applicazione della legge si trovino in situazioni in cui non sanno se possono intervenire, in quanto potrebbero non avere il potere di farlo oppure non disporre delle adeguate capacità tecniche per l'ispezione dei sistemi³⁶. L'incertezza giuridica può quindi ridurre i livelli complessivi di sicurezza e pregiudicare la competitività delle imprese europee.

Qualora si materializzino i rischi per la sicurezza, la mancanza di prescrizioni chiare e le caratteristiche delle tecnologie di IA sopra citate rendono difficile risalire alle decisioni potenzialmente problematiche adottate con il coinvolgimento di sistemi di IA. Ciò a sua volta può creare problemi per le persone che intendano ottenere il risarcimento dei danni subiti in forza della legislazione UE e nazionale vigente in materia di responsabilità³⁷.

A norma della direttiva sulla responsabilità per danno da prodotti difettosi, il produttore è responsabile dei danni causati da un prodotto difettoso. Tuttavia, nel caso di sistemi basati sull'IA, come quelli delle auto a guida autonoma, può rivelarsi difficile provare che il prodotto è difettoso e dimostrare il danno cagionato e il nesso di causalità tra difetto e danno. In aggiunta non è chiaro come e in che misura si applichi la direttiva sulla responsabilità per danno da prodotti difettosi nel caso di alcuni tipi di difetti, ad esempio per quelli risultanti da carenze della cibersicurezza del prodotto.

Di conseguenza la difficoltà di risalire alle decisioni potenzialmente problematiche adottate da sistemi di IA, di cui si è trattato anteriormente in relazione ai diritti fondamentali, è pertinente anche alle questioni legate alla sicurezza e alla responsabilità. Ad esempio coloro che hanno sofferto danni potrebbero non avere accesso effettivo agli elementi probatori necessari per giustificare un'azione in giudizio, per cui le loro possibilità di ottenere un'effettiva riparazione del danno potrebbero essere inferiori rispetto alle situazioni in cui il pregiudizio è causato da tecnologie tradizionali. Tali rischi aumenteranno man mano che l'uso dell'IA diverrà più diffuso.

B. POSSIBILI ADEGUAMENTI DEL QUADRO LEGISLATIVO VIGENTE DELL'UE PER QUANTO CONCERNE L'IA

Esiste un vasto corpus di norme vigenti dell'UE in materia di sicurezza dei prodotti e di responsabilità per danno da prodotti difettosi³⁸, comprendente norme settoriali ed integrato dalle legislazioni

³⁶ Un esempio può essere dato dagli smartwatch per bambini. Anche qualora non causino alcun danno diretto ai minori che li indossano, tali prodotti, in assenza di un livello minimo di sicurezza, possono facilmente essere utilizzati per avere accesso al minore. Può essere difficile per le autorità preposte alla vigilanza del mercato intervenire nei casi in cui i rischi non siano legati al prodotto in quanto tale.

³⁷ Le implicazioni dell'IA, dell'Internet delle cose e di altre tecnologie digitali per la legislazione in materia di sicurezza e responsabilità sono analizzate nella relazione della Commissione che accompagna il presente libro bianco.

³⁸ Il quadro giuridico dell'UE in materia di sicurezza dei prodotti è costituito dalla direttiva relativa alla sicurezza generale dei prodotti (direttiva 2001/95/CE), che funge da rete di sicurezza, e da una serie di normative settoriali che disciplinano diverse categorie di prodotti, dai macchinari agli aerei, dalle automobili ai giocattoli e ai dispositivi medici, con l'obiettivo di assicurare un elevato livello di salute e sicurezza. La disciplina della responsabilità per danno da prodotti difettosi è integrata da diversi sistemi di responsabilità civile per danni causati da prodotti o servizi.

nazionali; tale corpus di norme è pertinente e potenzialmente applicabile a una serie di applicazioni di IA emergenti.

Per quanto riguarda la protezione dei diritti fondamentali e dei diritti dei consumatori, il quadro legislativo dell'UE comprende atti normativi come la direttiva sull'uguaglianza razziale³⁹, la direttiva sulla parità di trattamento in materia di occupazione e di condizioni di lavoro⁴⁰, le direttive sulla parità di trattamento tra uomini e donne per quanto riguarda l'accesso a beni e servizi e in materia di occupazione⁴¹, una serie di norme sulla tutela dei consumatori⁴², sulla protezione dei dati personali e sulla privacy, in particolare il regolamento generale sulla protezione dei dati, nonché altre normative settoriali riguardanti la protezione dei dati personali, come la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie⁴³. Inoltre, a partire dal 2025 si applicheranno le norme sui requisiti di accessibilità dei beni e dei servizi previste dall'atto europeo sull'accessibilità⁴⁴. I diritti fondamentali devono inoltre essere rispettati in sede di attuazione di altre normative dell'UE, anche nel settore dei servizi finanziari, della migrazione o della responsabilità degli intermediari online.

Se da un lato la legislazione dell'UE rimane in linea di principio pienamente applicabile, indipendentemente dal coinvolgimento dell'IA, dall'altro è importante valutare se tale normativa possa essere adeguatamente applicata per far fronte ai rischi derivanti dai sistemi di IA o se sia necessario apportare adeguamenti a determinati strumenti giuridici.

Ad esempio, gli operatori economici rimangono pienamente responsabili della conformità dell'IA alle norme vigenti a tutela dei consumatori: è vietato utilizzare algoritmi che sfruttano il comportamento dei consumatori in violazione delle norme vigenti, e qualunque infrazione a tale divieto è punita di conseguenza.

La Commissione ritiene che il quadro legislativo possa essere migliorato per affrontare le situazioni e i rischi descritti di seguito.

- *Effettiva applicazione e rispetto della normativa nazionale e dell'UE in vigore:* le caratteristiche principali dell'IA rendono difficile garantire la corretta applicazione e il rispetto della normativa nazionale e dell'UE. A causa della mancanza di trasparenza (opacità dell'IA) è difficile individuare e dimostrare eventuali violazioni delle disposizioni normative (comprese quelle che tutelano i diritti fondamentali), attribuire la responsabilità e soddisfare le condizioni per chiedere un risarcimento. Pertanto, al fine di garantire l'effettiva applicazione e il rispetto delle norme, può essere necessario adeguare o chiarire la legislazione in vigore in determinati settori, ad esempio in materia di responsabilità, come ulteriormente specificato nella relazione che accompagna il presente libro bianco.
- *Limiti dell'ambito di applicazione della legislazione dell'UE vigente:* un aspetto essenziale su cui si concentra la legislazione dell'UE in materia di sicurezza dei prodotti è l'immissione degli stessi sul mercato. Anche se, conformemente alla legislazione dell'UE in materia di sicurezza dei prodotti, il software, quando è parte del prodotto finale, deve rispettare le norme pertinenti

³⁹ Direttiva 2000/43/CE.

⁴⁰ Direttiva 2000/78/CE.

⁴¹ Direttiva 2004/113/CE; direttiva 2006/54/CE.

⁴² Come la direttiva sulle pratiche commerciali sleali (direttiva 2005/29/CE) e la direttiva sui diritti dei consumatori (direttiva 2011/83/CE).

⁴³ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

⁴⁴ Direttiva (UE) 2019/882 sui requisiti di accessibilità dei prodotti e dei servizi.

in materia di sicurezza dei prodotti, rimane da stabilire se il software indipendente (*stand-alone*) rientri nell'ambito di applicazione della normativa dell'UE in materia di sicurezza dei prodotti, al di là di alcuni settori in cui esistono norme esplicite al riguardo⁴⁵. La normativa generale dell'UE in materia di sicurezza attualmente in vigore si applica ai prodotti ma non ai servizi, per cui in linea di principio non si applica nemmeno ai servizi basati sulla tecnologia di IA (ad esempio servizi sanitari, finanziari e di trasporto).

- *Funzionalità mutevole dei sistemi di IA:* l'integrazione del software, compresa l'IA, nei prodotti può modificare il funzionamento di tali prodotti e sistemi durante il loro ciclo di vita. Ciò vale in particolare per i sistemi che richiedono frequenti aggiornamenti del software o che si basano sull'apprendimento automatico. Tali caratteristiche possono dar luogo a nuovi rischi che non erano presenti quando il sistema è stato immesso sul mercato. Tali rischi non sono adeguatamente disciplinati dalla legislazione esistente, che si concentra prevalentemente sui rischi per la sicurezza presenti al momento dell'immissione sul mercato.
- *Incertezza in merito all'attribuzione delle responsabilità tra i diversi operatori economici lungo la catena di approvvigionamento:* in linea generale, la legislazione dell'UE in materia di sicurezza dei prodotti attribuisce al fabbricante la responsabilità del prodotto immesso sul mercato e di tutti i suoi componenti, ad esempio i sistemi di IA. In alcuni casi le norme possono però divenire poco chiare, ad esempio se l'IA è integrata nel prodotto dopo che quest'ultimo è stato immesso sul mercato da un soggetto diverso dal produttore. Inoltre la legislazione dell'UE in materia di responsabilità per danno da prodotti difettosi prevede la responsabilità dei produttori e lascia alle disposizioni nazionali in materia il compito di disciplinare la responsabilità di altri soggetti nella catena di approvvigionamento.
- *Evoluzione del concetto di sicurezza:* l'uso dell'IA nei prodotti e nei servizi può dar luogo a rischi che la legislazione dell'UE attualmente non affronta in modo esplicito. Tali rischi possono essere collegati alle minacce informatiche, possono riguardare la sicurezza personale (ad esempio i rischi collegati a nuove applicazioni dell'IA, come nel caso dell'IA applicata agli elettrodomestici), o ancora possono derivare dalla perdita di connettività, ecc. Tali rischi possono essere presenti al momento dell'immissione dei prodotti sul mercato, o derivare da aggiornamenti del software o dall'apprendimento automatico durante l'uso del prodotto. L'UE dovrebbe avvalersi appieno degli strumenti a sua disposizione per rafforzare la base di conoscenze scientifiche di cui dispone sui potenziali rischi connessi alle applicazioni di IA, sfruttando anche l'esperienza dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) al fine di valutare il panorama delle minacce dell'IA.

⁴⁵ Ad esempio, il software destinato dal fabbricante a essere impiegato per fini medici è considerato un dispositivo medico a norma del regolamento sui dispositivi medici [regolamento (UE) 2017/745].

Come indicato in precedenza, vari Stati membri stanno già valutando diverse opzioni per affrontare attraverso la legislazione nazionale le sfide poste dall'IA. Ciò comporta un rischio di frammentazione del mercato unico. Norme nazionali divergenti possono creare ostacoli per le imprese che intendono

Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità

La relazione che accompagna il presente libro bianco analizza il quadro giuridico pertinente, individuando le incertezze riguardanti l'applicazione di tale quadro giuridico in relazione ai rischi specifici derivanti dai sistemi di IA e da altre tecnologie digitali.

La conclusione è che la legislazione vigente in materia di sicurezza dei prodotti sostiene già un concetto ampio di sicurezza, con l'obiettivo di proteggere da tutti i tipi di rischi derivanti dal prodotto in funzione dell'uso dello stesso. Per garantire una maggiore certezza del diritto si potrebbero tuttavia introdurre disposizioni che contemplino esplicitamente i nuovi rischi derivanti dalle tecnologie digitali emergenti.

- Il comportamento autonomo che mostrano alcuni sistemi di IA durante il loro ciclo di vita può comportare modifiche significative dei prodotti, che a loro volta hanno ripercussioni sulla sicurezza e possono rendere necessaria una nuova valutazione dei rischi. Potrebbe inoltre rendersi necessaria, come misura di salvaguardia, la sorveglianza umana dalla fase di progettazione e durante tutto il ciclo di vita dei prodotti e dei sistemi di IA.
- Ove opportuno potrebbero essere presi in considerazione obblighi esplicativi per i produttori anche in relazione ai rischi per la sicurezza mentale degli utenti (ad esempio dovuti alla collaborazione con robot umanoidi).
- La legislazione dell'Unione in materia di sicurezza dei prodotti potrebbe prevedere prescrizioni specifiche che affrontino i rischi per la sicurezza derivanti dall'uso di dati errati in fase di progettazione, nonché meccanismi per garantire che sia mantenuta la qualità dei dati durante l'intero periodo di utilizzo dei prodotti e dei sistemi di IA.
- Il problema dell'opacità dei sistemi basati su algoritmi potrebbe essere affrontato mediante prescrizioni in materia di trasparenza.
- Potrebbe essere necessario adeguare e chiarire le norme vigenti in relazione ai casi di software indipendente immesso sul mercato senza altri componenti, oppure integrato in un prodotto dopo che quest'ultimo è stato immesso sul mercato, qualora ciò abbia un impatto sulla sicurezza.
- Data la crescente complessità delle catene di approvvigionamento in relazione alle nuove tecnologie, disposizioni che richiedano specificamente una collaborazione tra gli utenti e gli operatori economici attivi lungo la catena di approvvigionamento potrebbero garantire la certezza del diritto.

Le caratteristiche delle tecnologie digitali emergenti, come l'IA, l'Internet delle cose e la robotica, possono mettere in discussione alcuni aspetti dei quadri giuridici relativi alla responsabilità e renderli meno efficaci. Alcune di queste caratteristiche potrebbero rendere difficile far risalire il danno alla condotta di una persona, condizione indispensabile per invocare la responsabilità per colpa conformemente alla maggior parte delle norme nazionali in materia. Ne deriva la possibilità che i costi per le vittime aumentino in maniera significativa, e la potenziale difficoltà di avviare azioni per responsabilità nei confronti di soggetti diversi dal produttore e di ottenere elementi di prova a sostegno di tali azioni.

- Le persone che hanno subito un danno provocato con il coinvolgimento di sistemi di IA devono godere dello stesso livello di protezione delle persone che hanno subito danni causati da altre tecnologie; nel contempo occorre che l'innovazione tecnologica possa continuare a svilupparsi.
- È opportuno valutare attentamente tutte le opzioni che consentano di raggiungere tale obiettivo, compresa la possibilità di modificare la direttiva sulla responsabilità per danno da prodotti difettosi e ulteriori possibili interventi mirati di armonizzazione delle norme nazionali in materia di responsabilità. Ad esempio, la Commissione sta valutando se e in quale misura sia necessario mitigare le conseguenze della complessità adeguando l'onere della prova richiesto dalle norme nazionali in materia di responsabilità in relazione ai danni provocati dal funzionamento delle applicazioni di IA.

vendere e gestire sistemi di IA nel mercato unico. Garantire un approccio comune a livello di UE consentirebbe alle imprese europee di beneficiare di un accesso agevole al mercato unico e favorirebbe la loro competitività sui mercati mondiali.

In base a quanto esposto in precedenza la Commissione conclude che, oltre agli eventuali adeguamenti della legislazione esistente, potrebbe essere necessaria una nuova normativa specifica sull'IA al fine di adeguare il quadro giuridico dell'UE agli sviluppi tecnologici e commerciali attuali e futuri.

C. AMBITO DI APPLICAZIONE DI UN FUTURO QUADRO NORMATIVO DELL'UE

La determinazione dell'ambito di applicazione del futuro quadro normativo specifico sull'IA rappresenta una questione essenziale. L'ipotesi di lavoro è che il quadro normativo si applichi a prodotti e servizi basati sull'IA. Ai fini del presente libro bianco e di qualsiasi eventuale iniziativa futura di elaborazione delle politiche dovrebbe essere stabilita una definizione chiara di IA.

Nella sua comunicazione dal titolo "L'intelligenza artificiale per l'Europa" la Commissione ha fornito una prima definizione di IA⁴⁶, che poi è stata ulteriormente perfezionata dal gruppo di esperti ad alto livello⁴⁷.

Qualunque nuovo strumento giuridico dovrà comprendere una definizione di IA abbastanza flessibile da accogliere il progresso tecnico, ma anche sufficientemente precisa da garantire la necessaria certezza del diritto.

Ai fini del presente libro bianco e di eventuali future discussioni su iniziative strategiche, sembra importante chiarire gli elementi principali da cui è composta l'IA, vale a dire i "dati" e gli "algoritmi". L'IA può essere integrata nell'hardware. Nel caso delle tecniche di apprendimento automatico, che costituiscono un sottoinsieme dell'IA, gli algoritmi vengono addestrati per dedurre determinati modelli partendo da un set di dati al fine di stabilire le azioni necessarie al conseguimento di un determinato obiettivo.

Nel caso della guida autonoma, ad esempio, l'algoritmo utilizza in tempo reale dati forniti dall'automobile (velocità, consumo del motore, dati relativi agli ammortizzatori, ecc.) e dai sensori che rilevano tutti i dati dell'ambiente in cui si trova l'automobile (strada, segnali, altri veicoli, pedoni, ecc.) per stabilire quale direzione dovrebbe prendere l'automobile e con quale accelerazione e velocità al fine di raggiungere una determinata destinazione. L'algoritmo si basa sui dati rilevati e si adegua alla situazione della strada ed alle condizioni esterne, compreso il comportamento degli altri conducenti, al fine di ottenere la guida più sicura e più comoda.

Gli algoritmi possono continuare a imparare mentre vengono utilizzati. Sebbene i prodotti basati sull'IA possano agire in modo autonomo percependo il proprio ambiente senza seguire un insieme di istruzioni predeterminate, il loro comportamento è in larga misura definito e limitato dai loro

⁴⁶ COM(2018) 237 final, pag. 1: "Intelligenza artificiale (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (ad esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale), oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)."

⁴⁷ Gruppo di esperti ad alto livello, Una definizione di IA, pag. 8: "I sistemi di intelligenza artificiale (IA) sono sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulle conoscenze, o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti."

sviluppatori. Gli esseri umani determinano e programmano gli obiettivi che un sistema di IA dovrebbe raggiungere nel modo più efficace.

L'UE ha istituito un quadro giuridico rigoroso i cui obiettivi sono, tra gli altri, garantire la tutela dei consumatori, far fronte alle pratiche commerciali sleali e proteggere i dati personali e la privacy. L'acquis prevede inoltre norme settoriali specifiche (ad esempio per il settore dell'assistenza sanitaria o dei trasporti). Tali disposizioni vigenti del diritto dell'UE continueranno ad applicarsi in relazione all'IA, ma potrebbero rendersi necessari determinati adeguamenti di tale quadro giuridico per tenere conto della trasformazione digitale e dell'uso dell'IA (cfr. sezione B). Di conseguenza, gli aspetti già trattati dalla legislazione orizzontale o settoriale in vigore (ad esempio per quanto riguarda i dispositivi medici⁴⁸ o i sistemi di trasporto) continueranno ad essere disciplinati da tale legislazione.

In linea di principio il nuovo quadro normativo per l'IA dovrebbe essere efficace nel raggiungimento dei propri obiettivi, senza tuttavia essere talmente prescrittivo da creare oneri sproporzionali, in particolare per le PMI. Per raggiungere tale equilibrio la Commissione ritiene opportuno seguire un approccio basato sul rischio.

Tale approccio basato sul rischio è importante per garantire la proporzionalità dell'intervento normativo, ma richiede che siano definiti criteri chiari per distinguere tra le diverse applicazioni di IA, in particolare per stabilire se tali applicazioni siano o meno "ad alto rischio"⁴⁹. I criteri per stabilire che cosa sia un'applicazione di IA ad alto rischio dovrebbero essere chiari, facilmente comprensibili e applicabili a tutte le parti interessate. Le applicazioni di IA rimangono comunque interamente soggette al diritto vigente dell'UE, anche qualora non siano considerate ad alto rischio.

La Commissione ritiene che, per stabilire in generale se una determinata applicazione di IA debba essere ritenuta ad alto rischio, occorra valutare gli interessi in gioco e considerare se il settore interessato e l'uso previsto per tale applicazione implichino rischi significativi, in particolare per quanto concerne la protezione della sicurezza, dei diritti dei consumatori e dei diritti fondamentali. Più specificamente, un'applicazione di IA dovrebbe essere considerata ad alto rischio se soddisfa i due criteri cumulativi descritti di seguito.

- In primo luogo, l'applicazione di IA è utilizzata in un settore in cui, date le caratteristiche delle attività abitualmente svolte, si possono prevedere rischi significativi. Questo primo criterio garantisce che l'intervento normativo sia mirato ai settori in cui i rischi sono generalmente ritenuti più probabili. I settori interessati dovranno essere elencati in maniera specifica ed esaustiva nel nuovo quadro normativo. Ad esempio, settori dell'assistenza sanitaria, dei trasporti; dell'energia e parti del settore pubblico⁵⁰. L'elenco dovrrebbe essere periodicamente rivisto e modificato, ove necessario, in funzione dei pertinenti sviluppi nella pratica.
- In secondo luogo, l'applicazione dell'IA nel settore in questione è inoltre utilizzata in modo tale da poter generare rischi significativi. Questo secondo criterio riconosce il fatto che non tutti gli usi dell'IA nei settori selezionati comportano necessariamente rischi significativi. Ad esempio, per quanto l'assistenza sanitaria in genere possa essere certamente un settore

⁴⁸ Ad esempio vi sono diverse considerazioni in materia di sicurezza e varie implicazioni giuridiche riguardanti i sistemi di IA che forniscono ai medici informazioni sanitarie specializzate, i sistemi di IA che forniscono informazioni mediche direttamente al paziente e i sistemi di IA che svolgono essi stessi funzioni di carattere medico su un paziente. La Commissione sta esaminando queste sfide in materia di sicurezza e responsabilità, che caratterizzano il settore dell'assistenza sanitaria.

⁴⁹ La legislazione dell'UE può classificare i "rischi" in modo diverso da quanto qui descritto, in funzione del settore, come ad esempio per la sicurezza dei prodotti.

⁵⁰ Il settore pubblico potrebbe includere ambiti quali il diritto di asilo, la migrazione, i controlli alle frontiere e il potere giudiziario, la sicurezza sociale e i servizi per l'impiego.

rilevante, un eventuale difetto del sistema di prenotazione degli appuntamenti in un ospedale non presenta, in linea di massima, rischi tali da giustificare un intervento legislativo. La valutazione del livello di rischio derivante da un determinato uso potrebbe basarsi sull'impatto per i soggetti interessati. Ad esempio, usi delle applicazioni di IA che producono effetti giuridici, o effetti altrettanto rilevanti, sui diritti di una persona o di una società; usi che presentano il rischio di lesioni, morte o danni materiali o immateriali significativi; usi che producono effetti non ragionevolmente evitabili dalle persone fisiche o giuridiche.

L'applicazione dei due criteri cumulativi garantirebbe un ambito di applicazione del quadro normativo mirato e atto a garantire la certezza del diritto. Le prescrizioni obbligatorie contenute nel nuovo quadro normativo sull'IA (cfr. sezione D) si applicherebbero in linea di principio unicamente a quelle che siano state identificate come applicazioni ad alto rischio utilizzando i due criteri cumulativi sopra descritti.

Fatto salvo quanto precede, possono esistere anche casi eccezionali in cui, a causa dei rischi in gioco, l'uso di applicazioni di IA per determinati scopi deve essere considerato ad alto rischio di per sé, ossia indipendentemente dal settore interessato, per cui si applicherebbero comunque le prescrizioni di seguito indicate⁵¹. A titolo illustrativo si possono citare in particolare i seguenti usi:

- Alla luce dell'importanza che riveste per le persone, e tenendo conto dell'acquis dell'UE sulla parità in materia di occupazione, l'uso delle applicazioni di IA nei processi di selezione del personale e nelle situazioni che incidono sui diritti dei lavoratori sarebbe sempre considerato "ad alto rischio" e quindi si applicherebbero sempre le prescrizioni sotto indicate. Potrebbero essere prese in considerazione ulteriori applicazioni specifiche che incidono sui diritti dei consumatori.
- L'uso delle applicazioni di IA a fini di identificazione biometrica remota⁵² e l'impiego di altre tecnologie di sorveglianza intrusive sarebbero sempre considerati "ad alto rischio", per cui si applicherebbero sempre le prescrizioni sotto indicate.

D. TIPI DI PRESCRIZIONI

In fase di elaborazione del futuro quadro normativo in materia di IA sarà necessario decidere quali tipi di prescrizioni giuridiche obbligatorie imporre ai soggetti interessati. Tali prescrizioni possono essere ulteriormente specificate mediante il ricorso a norme. Come osservato nella sezione C, e in aggiunta alla legislazione già in vigore, tali prescrizioni si applicherebbero soltanto alle applicazioni di IA ad alto rischio, in modo da garantire che qualsiasi intervento normativo sia mirato e proporzionato.

Tenendo conto degli orientamenti del gruppo di esperti ad alto livello e di quanto esposto in precedenza, le prescrizioni per le applicazioni di IA ad alto rischio potrebbero riguardare i seguenti elementi essenziali, ulteriormente discussi nelle sottosezioni che seguono:

- i dati di addestramento;
- la tenuta dei dati e dei registri;

⁵¹ È importante sottolineare che potrebbero applicarsi anche altre normative dell'UE. Ad esempio, se le applicazioni di IA sono incorporate in un prodotto di consumo, la sicurezza di tali applicazioni può essere disciplinata dalla direttiva sulla sicurezza generale dei prodotti.

⁵² L'identificazione biometrica remota dovrebbe essere distinta dall'autenticazione biometrica (quest'ultima è un processo di sicurezza basato sulle caratteristiche biologiche uniche di un individuo, utilizzato per verificare che quest'ultimo sia chi afferma di essere). L'identificazione biometrica remota serve a determinare l'identità di più persone utilizzando identificatori biometrici (impronte digitali, immagine del volto, iride, schema delle vene, ecc.) a distanza, in uno spazio pubblico e in modo continuo o permanente confrontandoli con i dati contenuti in una banca dati.

- le informazioni da fornire;
- la robustezza e la precisione;
- la sorveglianza umana;
- prescrizioni specifiche per determinate applicazioni particolari dell'IA, come quelle utilizzate a fini di identificazione biometrica remota.

Al fine di garantire la certezza del diritto, tali prescrizioni saranno ulteriormente precise per fornire un chiaro punto di riferimento a tutti i soggetti chiamati a rispettarle.

a) Dati di addestramento

È più importante che mai promuovere, rafforzare e difendere i valori e le regole dell'UE, in particolare i diritti di cui i cittadini godono grazie al diritto dell'UE. Questi sforzi vanno senza dubbio estesi anche alle applicazioni di IA ad alto rischio qui in esame, commercializzate e utilizzate nell'UE.

Come discusso in precedenza, l'IA non può esistere senza i dati. Il funzionamento di numerosi sistemi di IA, nonché le azioni e le decisioni che ne possono derivare, dipendono in larga misura dai set di dati utilizzati per addestrarli. Occorre dunque adottare le misure necessarie per garantire che, nell'individuare i dati di addestramento dei sistemi di IA, siano rispettati i valori e le norme dell'UE, in particolare per quanto riguarda la sicurezza e le norme vigenti in materia di tutela dei diritti fondamentali. Si potrebbero prevedere le seguenti prescrizioni per quanto concerne i dati utilizzati per l'addestramento dei sistemi di IA:

- prescrizioni volte a fornire ragionevoli garanzie circa la sicurezza dell'uso successivo dei prodotti e dei servizi basati sull'IA; tale sicurezza è intesa come conformità agli standard stabiliti dalle norme dell'UE applicabili in materia di sicurezza (sia quelle vigenti, sia eventuali norme complementari). Si tratta ad esempio di prescrizioni volte a garantire che i sistemi di IA siano addestrati utilizzando set di dati sufficientemente ampi e che contemplino tutti gli scenari pertinenti, in modo da evitare situazioni pericolose;
- prescrizioni che impongano di adottare misure ragionevoli per garantire che tale uso successivo dei sistemi di IA non porti a risultati che implichino discriminazioni vietate. Tali prescrizioni potrebbero comportare, in particolare, l'obbligo di utilizzare set di dati sufficientemente rappresentativi, in particolare per garantire che rispecchino adeguatamente tutte le pertinenti dimensioni di genere, etnia e altri possibili motivi di discriminazione vietata;
- prescrizioni volte a garantire un'adeguata protezione della privacy e dei dati personali durante l'uso dei prodotti e dei servizi basati sull'IA. Tali questioni sono disciplinate dal regolamento generale sulla protezione dei dati e dalla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie per la parte che rientra nel loro rispettivo ambito di applicazione.

b) Tenuta dei dati e dei registri

Tenuto conto di elementi quali la complessità e l'opacità di molti sistemi di IA, nonché delle conseguenti difficoltà che possono sorgere nel garantire l'effettiva applicazione e il rispetto delle norme pertinenti, sono necessarie prescrizioni per la tenuta di registri relativi alla programmazione dell'algoritmo, ai dati utilizzati per addestrare sistemi di IA ad alto rischio e, in alcuni casi, per la tenuta dei dati stessi. Tali prescrizioni consentono essenzialmente di risalire alle azioni o decisioni potenzialmente problematiche dei sistemi di IA e di verificarle. Ciò dovrebbe non solo agevolare la vigilanza e l'applicazione delle norme, ma anche aumentare gli incentivi affinché gli operatori economici interessati tengano conto sin dall'inizio dell'esigenza di rispettare tali norme.

A tal fine il quadro normativo potrebbe prescrivere l'obbligo di tenere:

- registri accurati dei set di dati utilizzati per addestrare e sottoporre a prova i sistemi di IA, compresa una descrizione delle principali caratteristiche e delle modalità di selezione di tali insiemi;
- in taluni casi giustificati, gli stessi set di dati;
- la documentazione relativa alle metodologie, alle procedure e alle tecniche di programmazione⁵³ e di addestramento utilizzate per costruire, sottoporre a prova e convalidare i sistemi di IA, ove opportuno anche in materia di sicurezza, evitando distorsioni che potrebbero dar luogo a discriminazioni vietate.

I registri, la documentazione e, se del caso, i set di dati dovrebbero essere conservati per un periodo di tempo limitato e ragionevole al fine di garantire l'effettiva applicazione della legislazione pertinente. È opportuno adottare misure per garantire che tali elementi siano messi a disposizione su richiesta, in particolare per essere sottoposti a prove o ispezioni da parte delle autorità competenti. Ove necessario, è opportuno prevedere modalità per garantire la tutela delle informazioni riservate, come i segreti commerciali.

c) *Obblighi di informazione*

La trasparenza è necessaria anche al di là degli obblighi di tenuta dei registri di cui al punto c). Al fine di conseguire gli obiettivi perseguiti, in particolare promuovere un uso responsabile dell'IA, rafforzare la fiducia e agevolare la riparazione del danno ove necessario, è importante che vengano fornite in maniera proattiva informazioni adeguate sull'uso dei sistemi di IA ad alto rischio.

Potrebbero pertanto essere prese in considerazione le seguenti prescrizioni volte a:

- garantire che vengano fornite informazioni chiare sulle capacità e sulle limitazioni dei sistemi di IA, in particolare per quanto riguarda l'obiettivo per il quale i sistemi sono stati concepiti, le condizioni alle quali ci si può attendere che funzionino come previsto e il livello di precisione previsto nel raggiungimento dell'obiettivo specificato. Tali informazioni sono importanti soprattutto per coloro che applicano i sistemi, ma possono essere rilevanti anche per le autorità competenti e le parti interessate;
- informare i cittadini separatamente e con chiarezza quando questi interagiscono con un sistema di IA e non con un essere umano. Anche se la normativa dell'UE in materia di protezione dei dati contiene già alcune disposizioni analoghe⁵⁴, potrebbero essere necessarie ulteriori prescrizioni per raggiungere gli obiettivi sopra indicati. In tal caso occorre evitare oneri inutili. Non è quindi necessario fornire tali informazioni, ad esempio, quando ai cittadini sia immediatamente evidente che interagiscono con sistemi di IA. È inoltre importante che le informazioni fornite siano obiettive, concise e di facile comprensione. Le modalità di presentazione delle informazioni dovrebbero essere adeguate al contesto specifico.

⁵³ Si tratta ad esempio della documentazione riguardante l'algoritmo, compresi l'obiettivo di ottimizzazione perseguito dal modello, le ponderazioni inizialmente concepite per determinati parametri, ecc.

⁵⁴ In particolare, a norma dell'articolo 13, paragrafo 2, lettera f), del GDPR, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento è tenuto a fornire agli interessati ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente in relazione all'esistenza di un processo decisionale automatizzato, oltre a determinate informazioni aggiuntive.

d) Robustezza e precisione

Per essere affidabili, i sistemi di IA (ed in particolare le applicazioni di IA ad alto rischio) devono essere tecnicamente robusti e precisi. Ciò significa che tali sistemi devono essere sviluppati in modo responsabile e con la debita e adeguata valutazione ex ante dei rischi che possono generare. Il loro sviluppo e funzionamento devono essere tali da garantire che tali sistemi si comportino in modo affidabile secondo le previsioni. Dovrebbero essere adottate tutte le misure ragionevoli per ridurre al minimo il rischio di danni.

Potrebbero pertanto essere presi in considerazione i seguenti elementi:

- prescrizioni che garantiscano la robustezza e la precisione dei sistemi di IA, o che almeno riflettano correttamente il loro livello di precisione, durante tutte le fasi del ciclo di vita;
- prescrizioni atte a garantire la riproducibilità dei risultati;
- prescrizioni atte a garantire che i sistemi di IA possano gestire adeguatamente gli errori o le incongruenze in tutte le fasi del ciclo di vita;
- prescrizioni volte a assicurare la resilienza dei sistemi di IA sia agli attacchi palesi sia ai tentativi meno evidenti di manipolare i dati o gli stessi algoritmi, e a garantire che in tali casi siano adottate misure di attenuazione.

e) Sorveglianza umana

La sorveglianza umana aiuta a garantire che un sistema di IA non comprometta l'autonomia umana o provochi altri effetti negativi. L'obiettivo di un'IA affidabile, etica e antropocentrica può essere raggiunto solo garantendo un adeguato coinvolgimento degli esseri umani in relazione alle applicazioni di IA ad alto rischio.

Sebbene tutte le applicazioni di IA prese in considerazione nel presente libro bianco per un regime giuridico specifico siano ritenute ad alto rischio, il tipo e il livello adeguati di sorveglianza umana possono variare da un caso all'altro. Dipende in particolare dall'uso previsto dei sistemi e dagli effetti che potrebbero derivarne per le persone giuridiche e i cittadini interessati, senza pregiudizio per i diritti stabiliti dal GDPR in relazione al trattamento di dati personali da parte di sistemi di IA. La sorveglianza umana potrebbe ad esempio essere esercitata nei modi descritti di seguito a titolo meramente indicativo:

- il risultato del sistema di IA non diviene effettivo prima di essere stato rivisto e convalidato da un essere umano (ad esempio, la decisione di respingere una richiesta di prestazioni di sicurezza sociale può essere presa unicamente da un essere umano);
- il risultato del sistema di IA diviene immediatamente effettivo, ma successivamente è garantito l'intervento di un essere umano (ad esempio, la decisione di respingere la richiesta di una carta di credito può essere adottata da un sistema di IA, ma successivamente deve essere possibile il riesame da parte di un essere umano);
- il sistema di IA può essere monitorato durante il suo funzionamento da un essere umano che può intervenire in tempo reale e disattivarlo (ad esempio, prevedendo su un'auto a guida autonoma un pulsante o una procedura di arresto che un essere umano può attivare qualora decida che il funzionamento dell'auto non è sicuro);

- in fase di progettazione, imponendo vincoli operativi al sistema di IA (ad esempio, in determinate condizioni di scarsa visibilità in cui i sensori divengono meno affidabili, un'auto a guida autonoma deve cessare di funzionare, oppure in qualunque condizione tale veicolo deve mantenere una determinata distanza rispetto al veicolo che lo precede).

f) Prescrizioni specifiche per l'identificazione biometrica remota

La raccolta e l'uso di dati biometrici⁵⁵ a fini di identificazione⁵⁶ remota, ad esempio mediante la diffusione di sistemi di riconoscimento facciale in luoghi pubblici, comporta rischi specifici per i diritti fondamentali⁵⁷. L'uso di sistemi di IA per l'identificazione biometrica remota ha implicazioni sui diritti fondamentali che variano notevolmente a seconda dello scopo, del contesto e della portata del loro uso.

Le norme dell'UE in materia di protezione dei dati vietano in linea di principio il trattamento di dati biometrici allo scopo di identificare in modo univoco una persona fisica, salvo a determinate condizioni⁵⁸. In particolare, ai sensi del GDPR, tale trattamento può essere effettuato solo per un numero limitato di motivi, principalmente per motivi di interesse pubblico rilevante. In tal caso, il trattamento deve essere effettuato sulla base del diritto dell'Unione o degli Stati membri, rispettare il requisito di proporzionalità e l'essenza del diritto alla protezione dei dati e prevedere appropriate misure di tutela. A norma della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, un simile trattamento deve essere strettamente necessario, autorizzato in linea di principio dal diritto dell'UE o degli Stati membri e soggetto a garanzie adeguate. Qualunque trattamento di dati biometrici finalizzato all'identificazione univoca di una persona fisica sarebbe soggetto alla Carta dei diritti fondamentali dell'Unione europea, in quanto rappresenterebbe un'eccezione a un divieto stabilito dal diritto dell'UE.

Ne consegue che, conformemente alle vigenti norme dell'UE in materia di protezione dei dati e alla Carta dei diritti fondamentali, l'IA può essere utilizzata a fini di identificazione biometrica remota unicamente ove tale uso sia debitamente giustificato, proporzionato e soggetto a garanzie adeguate.

Per affrontare eventuali preoccupazioni sociali relative all'uso dell'IA per tali fini in luoghi pubblici, e per evitare la frammentazione del mercato interno, la Commissione avvierà un ampio dibattito europeo

⁵⁵ Per dati biometrici si intendono "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione o l'autenticazione univoca, quali l'immagine facciale o i dati dattiloskopici [impronte digitali]." [Articolo 3, paragrafo 13, della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie; articolo 4, paragrafo 14, del GDPR; articolo 3, paragrafo 18, del regolamento (UE) 2018/1725].

⁵⁶ In relazione al riconoscimento facciale, per identificazione si intende il confronto tra il modello (*template*) dell'immagine del volto di una persona e i numerosi altri modelli contenuti in una banca dati al fine di stabilire una corrispondenza. D'altro canto l'autenticazione (o verifica) è spesso definita verifica uno a uno e consente il confronto tra due modelli biometrici, di solito ritenuti appartenenti alla stessa persona. Il confronto tra i due modelli biometrici permette di stabilire se la persona che figura in entrambe le immagini sia la medesima. Tale procedura è usata, ad esempio, alle porte di controllo automatizzate alla frontiera utilizzate per i controlli alle frontiere presso gli aeroporti.

⁵⁷ Ad esempio per la dignità delle persone. Analogamente, i diritti al rispetto della vita privata e alla protezione dei dati personali sono al centro delle preoccupazioni riguardanti i diritti fondamentali connesse all'uso della tecnologia di riconoscimento facciale. Vi è anche un impatto potenziale per quanto concerne la non discriminazione e i diritti dei gruppi speciali, come i bambini, gli anziani e le persone con disabilità. L'uso della tecnologia non deve inoltre compromettere i diritti alla libertà di espressione, di associazione e di riunione. Cfr. Facial recognition technology: fundamental rights considerations in the context of law enforcement (Tecnologia di riconoscimento facciale: considerazioni sui diritti fondamentali nell'ambito delle attività di polizia e giudiziarie), <https://fra.europa.eu/en/publication/2019/facial-recognition>.

⁵⁸ Articolo 9 del GDPR; articolo 10 della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie. Cfr. anche l'articolo 10 del regolamento (UE) 2018/1725 (applicabile alle istituzioni e agli organi dell'UE).

sulle circostanze specifiche che possano eventualmente giustificare tali usi, nonché sulle garanzie comuni.

E. DESTINATARI

Per quanto riguarda i destinatari delle prescrizioni giuridiche sopra descritte relative alle applicazioni di IA ad alto rischio, si devono considerare due questioni principali.

In primo luogo va affrontata la questione di come ripartire gli obblighi tra gli operatori economici coinvolti. Il ciclo di vita di un sistema di IA coinvolge numerosi operatori, tra cui lo sviluppatore, il soggetto che lo applica (il "deployer", ossia la persona che utilizza un prodotto o servizio dotato di IA) e potenzialmente altri soggetti (il produttore, il distributore o l'importatore, i prestatori di servizi, gli utenti professionali o privati).

La Commissione ritiene che in un futuro quadro normativo ciascun obbligo debba essere stabilito a carico dell'operatore o degli operatori che si trovano nella posizione migliore per affrontare eventuali rischi potenziali. Ad esempio, se da un lato gli sviluppatori dell'IA sono i più qualificati per affrontare i rischi derivanti dalla fase di sviluppo, dall'altro la loro capacità di controllare i rischi durante la fase di utilizzo può essere più limitata. In tal caso il pertinente obbligo dovrebbe essere stabilito a carico del soggetto che applica l'IA. Ciò lascia impregiudicata, ai fini della responsabilità nei confronti degli utenti finali o di altre parti che abbiano subito un danno nonché della garanzia di un accesso effettivo alla giustizia, la questione dell'individuazione del soggetto chiamato a rispondere dei danni eventualmente provocati dal sistema di IA. In base al diritto dell'UE in materia di responsabilità per danno da prodotti difettosi, tale responsabilità è attribuita al produttore, fatta salva la normativa nazionale, che può anche prevedere la possibilità di rivalersi su altri soggetti.

In secondo luogo va affrontata la questione dell'ambito di applicazione geografico dell'intervento legislativo. Secondo la Commissione, è fondamentale che le prescrizioni siano applicabili a tutti gli operatori economici interessati che forniscono prodotti o servizi basati sull'IA nell'UE, indipendentemente dal fatto che siano stabiliti o meno nell'Unione; in caso contrario, gli obiettivi dell'intervento legislativo di cui sopra potrebbero non essere pienamente raggiunti.

F. CONFORMITÀ E APPLICAZIONE DELLE NORME

Per avere un'IA affidabile, sicura e conforme alle norme e ai valori europei le prescrizioni giuridiche devono essere rispettate ed applicate efficacemente nella pratica, sia dalle autorità nazionali ed europee competenti sia dalle parti interessate. Le autorità competenti dovrebbero essere in grado di indagare sui singoli casi, ma anche di valutare l'impatto sulla società.

In considerazione dell'elevato rischio che talune applicazioni di IA presentano per i cittadini e la nostra società (cfr. la sezione A), in questa fase la Commissione ritiene che sia necessaria una valutazione preliminare e obiettiva della conformità per verificare e garantire il rispetto di talune prescrizioni obbligatorie sopra citate che disciplinano le applicazioni ad alto rischio (cfr. sezione D). La valutazione preliminare della conformità potrebbe includere procedure di prova, ispezione o certificazione⁵⁹, oltre a controlli degli algoritmi e dei set di dati utilizzati nella fase di sviluppo.

⁵⁹ Il sistema si baserebbe sulle procedure di valutazione della conformità nell'UE [cfr. la decisione n. 768/2008/CE o il regolamento (UE) 2019/881 (regolamento sulla cibersicurezza)], tenendo conto delle specificità dell'IA. Cfr. la guida blu all'attuazione della normativa UE sui prodotti, del 2014.

Le valutazioni della conformità per le applicazioni di IA ad alto rischio dovrebbero far parte dei meccanismi di valutazione della conformità già esistenti per un gran numero di prodotti immessi sul mercato interno dell'UE. Qualora non sia possibile avvalersi di tali meccanismi, potrebbe essere necessario istituire meccanismi analoghi, avvalendosi delle migliori prassi e di eventuali contributi dei portatori di interessi e delle organizzazioni europee di normazione. Tali nuovi meccanismi dovrebbero essere proporzionali e non discriminatori e utilizzare criteri trasparenti e obiettivi in conformità agli obblighi internazionali.

In fase di progettazione e realizzazione di un sistema sulla base di valutazioni preliminari della conformità, occorre considerare in particolare:

- che non tutti i requisiti sopra indicati possono essere verificati mediante una valutazione preliminare della conformità. Ad esempio, in generale l'adempimento dell'obbligo di fornire informazioni non si presta facilmente ad essere verificato mediante una simile valutazione;
- la possibilità che taluni sistemi di IA si evolvano e apprendano dall'esperienza: tale possibilità può rendere necessarie valutazioni ripetute per tutta la durata dei sistemi di IA in questione;
- la necessità di verificare i dati utilizzati per l'addestramento nonché le pertinenti metodologie, procedure e tecniche di programmazione e di addestramento utilizzate per costruire, sottoporre a prova e convalidare i sistemi di IA;
- che, qualora dalla valutazione della conformità emerga che un sistema di IA non rispetta alcune prescrizioni, ad esempio quelle relative ai dati utilizzati per l'addestramento, sarà necessario porre rimedio alle carenze individuate, ad esempio addestrando nuovamente il sistema nell'UE in modo tale da garantire il rispetto di tutte le prescrizioni applicabili.

Le valutazioni della conformità sarebbero obbligatorie per tutti gli operatori economici destinatari delle prescrizioni, indipendentemente dal loro luogo di stabilimento⁶⁰. Al fine di limitare l'onere a carico delle PMI, potrebbero essere previste strutture di sostegno, anche attraverso i poli dell'innovazione digitale. Norme e strumenti online dedicati potrebbero inoltre agevolare il rispetto degli obblighi.

Lo svolgimento di valutazioni preliminari della conformità non pregiudica il controllo della conformità e l'applicazione ex post della legge da parte delle autorità nazionali competenti. Ciò vale per le applicazioni di IA ad alto rischio, ma anche per altre applicazioni di IA soggette a prescrizioni giuridiche, pur se le autorità nazionali competenti potrebbero prestare particolare attenzione alle prime, dato l'alto rischio che le contraddistingue. Un'adeguata documentazione delle pertinenti applicazioni di IA dovrebbe consentire i controlli ex post (cfr. la sezione E) e, ove opportuno, la possibilità che tali applicazioni siano sottoposte a prova da terzi, ad esempio dalle autorità competenti. Ciò può essere particolarmente importante quando sorgono rischi per i diritti fondamentali che dipendono dal contesto. Tale controllo della conformità dovrebbe essere inquadrato in un sistema di vigilanza continua del mercato. Gli aspetti relativi alla governance sono ulteriormente discussi nella sezione H.

È inoltre opportuno garantire, sia per le applicazioni di IA ad alto rischio sia per il resto delle applicazioni, un ricorso giurisdizionale effettivo per chiunque sia stato danneggiato dai sistemi di IA.

⁶⁰ Per quanto concerne la pertinente struttura di governance, compresi gli organismi incaricati di svolgere le valutazioni della conformità, cfr. la sezione H.

Le questioni relative alla responsabilità sono ulteriormente discusse nella relazione sul quadro di riferimento per la sicurezza e la responsabilità che accompagna il presente libro bianco.

G. ETICHETTATURA SU BASE VOLONTARIA PER LE APPLICAZIONI DI IA NON AD ALTO RISCHIO

Per le applicazioni di IA che non sono considerate "ad alto rischio" (cfr. sezione C) e che pertanto non sono soggette alle prescrizioni obbligatorie di cui sopra (cfr. le sezioni D, E e F), oltre alla legislazione applicabile vi sarebbe la possibilità di istituire un sistema di etichettatura su base volontaria.

Nel quadro di tale sistema, gli operatori economici interessati non soggetti alle prescrizioni obbligatorie potrebbero decidere, su base volontaria, di conformarsi a tali prescrizioni o di impegnarsi al rispetto di una serie specifica di prescrizioni analoghe, stabilite appositamente ai fini del sistema volontario. Agli operatori economici interessati sarebbe allora assegnato un marchio di qualità per le loro applicazioni di IA.

Il marchio volontario consentirebbe agli operatori economici interessati di mettere in evidenza l'affidabilità dei loro prodotti e servizi basati sull'IA, e consentirebbe agli utenti di riconoscere facilmente che i prodotti e i servizi in questione sono conformi a determinati parametri di riferimento obiettivi e standardizzati a livello dell'UE, che vanno oltre gli obblighi giuridici normalmente applicabili. Ciò contribuirebbe a rafforzare la fiducia degli utenti nei sistemi di IA e a promuovere l'adozione generale della tecnologia.

Tale opzione richiederebbe la creazione di un nuovo strumento giuridico che definisca il quadro relativo a un sistema di etichettatura su base volontaria per gli sviluppatori e/o i soggetti che applicano i sistemi di IA non considerati ad alto rischio. Sebbene la partecipazione al sistema di etichettatura sia facoltativo, una volta che gli sviluppatori o i soggetti che applicano l'IA hanno deciso di aderirvi le relative prescrizioni sarebbero vincolanti. La combinazione di attività di applicazione della legge ex ante ed ex post dovrebbe garantire il rispetto di tutte le prescrizioni.

H. GOVERNANCE

Occorre una struttura di governance europea in materia di IA, sotto forma di un quadro di cooperazione delle autorità nazionali competenti, per evitare la frammentazione delle responsabilità, aumentare la capacità degli Stati membri e garantire che l'Europa si doti progressivamente delle capacità necessarie per sottoporre a prova e certificare prodotti e servizi basati sull'IA. In tale contesto sarebbe utile sostenere le autorità nazionali competenti affinché possano adempiere il loro mandato nei casi di utilizzo dell'IA.

Una struttura di governance europea potrebbe essere investita di varie funzioni, tra cui permettere uno scambio regolare di informazioni e migliori prassi, individuare le tendenze emergenti e fornire consulenza sulle attività di normazione e sulla certificazione. Dovrebbe inoltre svolgere un ruolo essenziale nell'agevolare l'attuazione del quadro giuridico, ad esempio fornendo orientamenti, pareri e consulenze. A tal fine dovrebbe basarsi su una rete di autorità nazionali, nonché su reti settoriali e autorità di regolamentazione a livello nazionale e dell'UE. Un comitato di esperti potrebbe inoltre fornire assistenza alla Commissione.

La struttura di governance dovrebbe garantire la massima partecipazione dei portatori di interessi, fra cui organizzazioni dei consumatori e parti sociali, imprese, ricercatori e organizzazioni della società civile, che dovrebbero essere consultati in merito all'attuazione e all'ulteriore sviluppo del quadro di riferimento.

Considerando che vi sono strutture già esistenti, ad esempio nei settori finanziario, farmaceutico, dell'aviazione, dei dispositivi medici, della tutela dei consumatori o della protezione dei dati, la struttura di governance proposta non dovrebbe duplicare le funzioni esistenti, bensì stabilire stretti legami con altre autorità competenti a livello nazionale e dell'UE nei vari settori, al fine di integrare le competenze esistenti e aiutare le autorità nel monitoraggio e nella sorveglianza delle attività svolte dagli operatori economici in cui intervengono sistemi di IA nonché prodotti e servizi basati sull'IA.

Infine, qualora venga scelta questa opzione, lo svolgimento delle valutazioni della conformità potrebbe essere affidato agli organismi notificati designati dagli Stati membri. I centri di prova dovrebbero rendere possibili verifiche e valutazioni indipendenti dei sistemi di IA in conformità alle prescrizioni sopra descritte. Le valutazioni indipendenti rafforzeranno la fiducia, garantiranno l'obiettività e potrebbero anche facilitare il lavoro delle autorità competenti.

L'UE dispone di centri di prova e di valutazione eccellenti e dovrebbe sviluppare le proprie capacità anche nel settore dell'IA. Gli operatori economici stabiliti in paesi terzi che intendono entrare nel mercato interno possono ricorrere a organismi designati stabiliti nell'UE o, in forza di accordi di riconoscimento reciproco con paesi terzi, ricorrere a organismi di paesi terzi designati per effettuare tale valutazione.

La struttura di governance relativa all'IA e le possibili valutazioni della conformità qui discusse non inciderebbero sulle responsabilità e sui poteri riconosciuti dal diritto dell'UE in vigore alle autorità competenti in determinati settori o per questioni specifiche (ad esempio nei settori finanziario, farmaceutico, dell'aviazione, dei dispositivi medici, della tutela dei consumatori, della protezione dei dati, ecc.).

6. CONCLUSIONI

L'IA è una tecnologia strategica che offre molti benefici ai cittadini, alle imprese e alla società nel suo insieme, a condizione che segua un approccio antropocentrico, etico, sostenibile e rispettoso dei valori e dei diritti fondamentali. L'IA offre importanti vantaggi in termini di efficienza e produttività, che possono rafforzare la competitività dell'industria europea e migliorare il benessere dei cittadini. Può inoltre contribuire a individuare soluzioni ad alcune delle sfide sociali più urgenti, tra cui la lotta ai cambiamenti climatici e al degrado ambientale, le sfide legate alla sostenibilità e ai cambiamenti demografici, la protezione delle nostre democrazie e, ove tale uso sia necessario e proporzionato, la lotta alla criminalità.

Se vuole cogliere appieno le opportunità offerte dall'IA, l'Europa deve sviluppare e rafforzare le capacità industriali e tecnologiche necessarie. Come indicato nella strategia europea per i dati, che accompagna il presente libro bianco, ciò richiede anche misure che consentano all'UE di diventare un hub di dati globale.

L'approccio europeo all'IA mira a promuovere la capacità di innovazione dell'Europa nel settore dell'IA, sostenendo nel contempo lo sviluppo e la diffusione di un'IA etica e affidabile in tutta l'economia dell'UE. L'IA dovrebbe apportare vantaggi alle persone ed essere un fattore positivo per la società.

Con il presente libro bianco, accompagnato dalla relazione sul quadro di riferimento per la sicurezza e la responsabilità, la Commissione avvia un'ampia consultazione della società civile, dell'industria e del mondo accademico negli Stati membri in merito a proposte concrete per un approccio europeo all'IA. Tali misure comprendono sia strumenti strategici per promuovere gli investimenti nella ricerca e nell'innovazione, favorire lo sviluppo delle competenze e sostenere l'adozione dell'IA da parte delle PMI, sia proposte relative a elementi essenziali di un futuro quadro normativo. Questa consultazione

consentirà un dialogo globale con tutti i portatori di interessi, che informerà le prossime fasi del lavoro della Commissione.

La Commissione invita a formulare osservazioni sulle proposte presentate nel libro bianco mediante una consultazione pubblica aperta consultabile all'indirizzo: https://ec.europa.eu/info/consultations_en. Sarà possibile formulare osservazioni nel quadro della consultazione fino al 19 maggio 2020.

È prassi abituale della Commissione pubblicare le osservazioni pervenute in risposta a una consultazione pubblica. È tuttavia possibile chiedere che tali osservazioni rimangano in tutto o in parte riservate. In tal caso si prega di indicare tale richiesta sulla prima pagina della risposta e trasmettere alla Commissione anche una versione non riservata della risposta, che sarà pubblicata.