

# dossier

XIX Legislatura

**25 gennaio 2024**

## **Conferenza sull'intelligenza artificiale**

***Bruxelles, 28-29 gennaio 2024***



Senato  
della Repubblica



Camera  
dei deputati





XIX LEGISLATURA

Documentazione per le Commissioni  
RIUNIONI INTERPARLAMENTARI

Conferenza sull'intelligenza artificiale  
*Bruxelles, 28-29 gennaio 2024*

SENATO DELLA REPUBBLICA

CAMERA DEI DEPUTATI

SERVIZIO STUDI

SERVIZIO DEGLI AFFARI INTERNAZIONALI

UFFICIO RAPPORTI CON L'UNIONE

UFFICIO DEI RAPPORTI CON LE ISTITUZIONI  
DELL'UNIONE EUROPEA

EUROPEA

N. 65

N. 39



Servizio Studi

TEL. 06 6706 2451 - [studi1@senato.it](mailto:studi1@senato.it) - ✉@SR\_Studi

Dossier n.65

Servizio degli Affari internazionali -

Ufficio dei rapporti con le istituzioni dell'Unione Europea

TEL. 06 6706 4561 - [affeuropei@senato.it](mailto:affeuropei@senato.it)



Ufficio rapporti con l'Unione europea

Tel. 06 6760 2145 - [cdrue@camera.it](mailto:cdrue@camera.it) - ✉@CD\_europa - [europa.camera.it](http://europa.camera.it).

Dossier n. 39

Servizio Studi

TEL. 06 6760 3410 - [st\\_segreteria@camera.it](mailto:st_segreteria@camera.it)

La documentazione dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. Si declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

# INDICE

## ORDINE DEL GIORNO

### **INTRODUZIONE.....1**

La conferenza interparlamentare .....1

Il contesto .....1

### **IL REGOLAMENTO UE IN MATERIA DI INTELLIGENZA ARTIFICIALE.....3**

I principali elementi del nuovo regolamento (in base all'accordo  
provvisorio tra Parlamento europeo e Consiglio).....3

La posizione negoziale del Governo italiano .....15

Pacchetto per l'innovazione in materia di IA a sostegno delle *start-up*  
e delle PMI nel settore dell'intelligenza artificiale .....16

### **L'ATTIVITÀ DELLA CAMERA DEI DEPUTATI IN TEMA DI INTELLIGENZA ARTIFICIALE.....19**

Giustizia.....19

Difesa.....20

Cultura .....20

Attività produttive.....22

Lavoro.....25

Affari sociali.....28

Affari comunitari .....29

Comitato per la documentazione .....30

**ATTIVITÀ DEL SENATO IN TEMA DI INTELLIGENZA ARTIFICIALE.....33**

Giustizia.....	33
Cultura .....	33
Lavori pubblici .....	33
Attività legislativa.....	33

**SESSIONE 1 - LE INDUSTRIE CREATIVE E CULTURALI DI FRONTE  
ALL'INTELLIGENZA ARTIFICIALE E IL SUO IMPATTO SULLA VITA  
QUOTIDIANA DEI CITTADINI EUROPEI.....35**

La promozione delle imprese culturali e creative.....	35
I creatori digitali .....	36
Attività parlamentari in corso: l'indagine conoscitiva sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano .....	38
Profili normativi: gli incentivi .....	39
Le questioni legate alla tutela dei consumatori .....	41

**SESSIONE 2 - LA DIDATTICA NELL'ERA DELL'INTELLIGENZA  
ARTIFICIALE: PROBLEMATICHE E IMPATTI.....43**

1. Le iniziative parlamentari in corso .....	43
2. Approcci regolatori e politiche pubbliche in materia di AI nei settori dell'istruzione, dell'università e della ricerca di base .....	45
3. Approcci regolatori e politiche pubbliche in materia di AI nei settori della cultura .....	50
4. Approcci regolatori e politiche pubbliche in materia di editoria e diritto d'autore .....	52

**SESSIONE 3 - IL SETTORE SANITARIO DI FRONTE  
ALL'INTELLIGENZA ARTIFICIALE: PROSPETTIVE E SFIDE .....57**

Attività parlamentari in corso .....	61
--------------------------------------	----

**SESSIONE 4 - LE SFIDE DELL'INTELLIGENZA ARTIFICIALE PER  
LA GOVERNANCE PUBBLICA.....63**

Trasformazione della vita delle persone attraverso le piattaforme digitali pubbliche .....	63
---	----

Le sfide dell'implementazione dell'intelligenza artificiale nel settore pubblico .....	64
---	----

Approcci regolatori e politiche pubbliche in materia di AI nei settori dell'amministrazione pubblica, delle istituzioni e dei processi democratici e dei diritti fondamentali.....	65
--	----

Le attività in corso presso la Camera dei deputati.....	68
---	----

Accordo tra Camera e Agenzia per la Cybersicurezza Nazionale sulla protezione dalle minacce informatiche.....	69
--	----

**FOCUS: L'EXECUTIVE ORDER DEL PRESIDENTE BIDEN IN  
MATERIA DI AI .....**

Premessa .....	77
----------------	----

Le 8 finalità.....	77
--------------------	----

Le definizioni.....	79
---------------------	----

Il cronoprogramma di attuazione delle singole politiche .....	81
---	----

**FOCUS: INTELLIGENZA ARTIFICIALE E ANALISI DEL RISCHIO  
FISCALE .....**

.....	85
-------	----



## **ARTIFICIAL INTELLIGENCE AND ITS FUTURE IMPACTS**

*Brussels, 28-29 January 2024*

### **Sunday, 28 January 2024**

*Venue: Parliament of the Brussels-Capital Region - Salle des Glaces and Grand Salon*

- |       |  |
|-------|--|
| 18:30 | Reception of participants  |
| 19:00 | Welcome speech by the President of the Parliament of the Brussels-Capital Region, Mr Rachid MADRANE and the President of the Parliament of Wallonia, Mr André FRÉDÉRIC |
| 19:15 | Dinner at the invitation of the Parliament of the Wallonia-Brussels Federation, of the Parliament of Wallonia and of the Parliament of the Brussels-Capital Region     |
| 22:00 | Return transport to the hotels   |

### **Monday, 29 January 2024**

*Venue: Parliament of the Wallonia-Brussels Federation - Hemicycle - 3rd floor*

- |       |   |
|-------|---|
| 08:15 | Reception of participants   |
| 09:00 | Welcoming words by the President of the Wallonia-Brussels Federation, Mr Rudy DEMOTTE                         |
|       | Intervention by the Vice-President of the Government of the Wallonia-Brussels Federation, Mr Frédéric DAERDEN |

09:10

**Session 1 "The creative and cultural industries faced with artificial intelligence and its impacts on the daily lives of European citizens"**

- Mr Thierry DUTOIT, President of the Numédiart Institute at the University of Mons (UMons)
- Ms Marie DU CHASTEL, Artistic Director of KIKK, curator specialising in digital art and new media
- Mr Antonin DESCAMPE, Professor at the Louvain School of Journalism, researcher at the Media Innovation & Intelligibility Lab (MiiL)

Moderation: Mr Gilles QUOISTIAUX

Exchange with the participants

10:30

*Coffee break*

10:40

**Session 2 "Teaching in the age of artificial intelligence: issues and impacts"**

- Mr Nathanaël ACKERMAN, Director General of the AI4Belgium coalition
- Ms Karen BOERS, Managing Director FARI - AI For The Common Good Institute - Brussels
- Mr Bruno DE LIEVRE, Professor at the University of Mons (UMons), adviser to the Rector on digital strategies for education

Moderation: Mr Gilles QUOISTIAUX

Exchange with the participants

12:10

Official photo in the Hemicycle

12:15

*Lunch (Atrium - ground floor)*

13:30

**Session 3 “The healthcare sector faced with artificial intelligence: prospects and challenges”**

Intervention by the President of the Parliament of Wallonia, Mr André FRÉDÉRIC

Presentations:

- Ms Christie MORREALE, Vice-President of the Government of Wallonia
- Mr Giovanni BRIGANTI, Holder of the Chair in Artificial Intelligence and Digital Medicine at UMONS
- Mr Stéphane LEFEBVRE, CEO of ZORGI

Moderation: Mr Gilles QUOISTIAUX

Exchange with the participants

15:00

**Session 4 "The challenges of artificial intelligence for public governance”**

Chaired by the President of the Brussels Parliament, Mr Rachid MADRANE

Intervention by the Minister of the Government of the Brussels-Capital Region responsible for Employment and Vocational Training, Digital Transition, Local Authorities, and Animal Welfare, Mr Bernard CLERFAYT

Presentations:

- Ms Lucie CLUZEL-MÉTAYER, Professor of Public Digital Law at the University of Paris-Nanterre
- Mr Hugues BERSINI, co-director of the laboratory IRIDIA, Université libre de Bruxelles
- Mrs Lucia Russo, representative of the OECD's Global Parliamentary Network on Artificial Intelligence

Exchange with the participants

16:30

*Closing ceremony and reception (Atrium - ground floor)*



Parliamentary  
Dimension

Wi-Fi access



Username:

Europe2024

Password:

Europe2024

#EU2024BE

[www.parleu2024.be](http://www.parleu2024.be)

## INTRODUZIONE

### **La conferenza interparlamentare**

La conferenza interparlamentare sul tema "L'intelligenza artificiale e i suoi impatti futuri", che si svolgerà a Bruxelles il 28 e 29 gennaio 2024, è organizzata dal **Parlamento della regione di Bruxelles Capitale**, dal **Parlamento della Federazione Vallonia - Bruxelles** e dal **Parlamento della Vallonia**.

La riunione rientra fra gli incontri organizzati nell'ambito della dimensione parlamentare della Presidenza belga del Consiglio dell'Unione europea nel primo semestre del 2024.

Il Parlamento belga ha deciso, in coerenza con la natura federale del rispettivo sistema costituzionale, di organizzare le riunioni interparlamentari nel corso del proprio semestre di Presidenza in collaborazione con i parlamenti regionali.

Sulla base del programma (cfr. allegato), la riunione prevede, dopo gli interventi di apertura, quattro sessioni:

- le industrie creative e culturali di fronte all'intelligenza artificiale e il suo impatto sulla vita quotidiana dei cittadini europei;
- la didattica nell'era dell'intelligenza artificiale: problematiche e impatti;
- il settore sanitario di fronte all'intelligenza artificiale: prospettive e sfide;
- le sfide dell'intelligenza artificiale per la governance pubblica.

Alla riunione sono invitati a partecipare fino a due parlamentari per ciascuna Camera.

### **Il contesto**

Negli ultimi anni si è assistito a un **rapido sviluppo tecnologico dell'intelligenza artificiale (IA)**, ossia dell'uso della tecnologia digitale per creare sistemi in grado di svolgere compiti per i quali è comunemente ritenuta necessaria l'intelligenza umana.

L'IA è **già usata in molte applicazioni quotidiane**, quali, tra le altre, l'assistenza virtuale, le diagnosi mediche, le traduzioni automatiche, gli strumenti di navigazione, il controllo della qualità nella fabbricazione e la previsione delle catastrofi naturali.

I **progressi più recenti** hanno anche favorito **l'emergere di IA generative sempre più potenti**, che stanno assumendo un ruolo centrale e strategico nell'economia e nella società.

I **benefici** dell'intelligenza artificiale possono essere **molteplici**, da un'assistenza medica più efficace a una migliore istruzione a trasporti più sicuri. L'IA può contribuire a sviluppare un'economia più innovativa, sostenibile e competitiva e alla lotta contro i cambiamenti climatici.

Allo stesso tempo, l'intelligenza artificiale può essere fonte di **diversi rischi**, ad esempio per la salute, la sicurezza e la tutela dei diritti fondamentali. Alcuni modelli particolarmente potenti di IA, il cui utilizzo è assai diffuso, possono comportare addirittura **rischi sistemici**.

Anche e soprattutto per questi motivi, **l'Unione europea ha deciso di definire una normativa sull'intelligenza artificiale** (cfr. l'apposito capitolo del presente dossier). Essa intende garantire migliori condizioni per lo sviluppo e l'uso dell'IA e rappresentare anche **un modello globale** per la regolamentazione dell'IA in altre giurisdizioni, promuovendo in tal modo a livello mondiale l'approccio europeo alla regolamentazione dell'IA.

## IL REGOLAMENTO UE IN MATERIA DI INTELLIGENZA ARTIFICIALE

È in via di definitiva adozione da parte del Parlamento europeo e del Consiglio, secondo la **procedura legislativa ordinaria**, la [proposta di regolamento](#), presentata dalla Commissione europea il 21 aprile 2021, recante un **quadro giuridico** in materia di **intelligenza artificiale** (esplicitamente denominato “**legge sull’intelligenza artificiale**”).

In esito ai **triloghi** (negoziati interistituzionali tra i rappresentanti di Parlamento europeo, Consiglio e Commissione per concordare il testo da sottoporre all’approvazione dei due colegislatori), il **9 dicembre 2023** è stato infatti raggiunto un **accordo politico provvisorio**, con l’obiettivo di approvare in via definitiva la nuova normativa **entro la fine dell’anno** o, al massimo, **entro la conclusione dell’attuale legislatura europea**.

L’accordo dovrà ora essere **formalmente approvato** dal Consiglio (a maggioranza qualificata), probabilmente nel corso del mese di **febbraio**, e dal Parlamento europeo (a maggioranza dei suoi componenti), al più tardi nella sessione del **prossimo aprile**.

Prima dell’avvio dei negoziati, il **Consiglio dell’UE**, con un [orientamento generale](#) adottato all’unanimità il **6 dicembre 2022** e il **Parlamento europeo** con [emendamenti approvati](#) in plenaria (con 499 voti a favore, 28 contrari e 93 astensioni) il **14 giugno 2023** avevano definito le proprie posizioni.

### **I principali elementi del nuovo regolamento (in base all’accordo provvisorio tra Parlamento europeo e Consiglio)**

Il testo dell’accordo provvisorio, diffuso presso i gruppi di lavoro del Consiglio, prevede i seguenti punti qualificanti.

#### ***Definizione e ambito di applicazione***

Il regolamento ha l’**obiettivo** di migliorare il funzionamento del mercato interno e promuovere l’**adozione di un’intelligenza artificiale affidabile e incentrata sull’uomo**, garantendo, nel contempo, un elevato livello di **protezione** della **salute**, della **sicurezza** e dei **diritti fondamentali**, compresa la **democrazia**, lo **Stato di diritto** e la tutela dell’ambiente dagli effetti dannosi dei sistemi di intelligenza artificiale nell’Unione, e sostenendo l’innovazione.

Il regolamento **definisce un sistema di IA** come un sistema basato su una macchina progettato per funzionare con diversi livelli di autonomia e che può mostrare adattività dopo l'implementazione e che, per obiettivi espliciti o impliciti, deduce, dall'input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

La nuova disciplina non intende introdurre una normazione esaustiva e dettagliata di ogni aspetto connesso all'IA, così definita. Tiene conto che diversi profili della materia sono già riconducibili ad **atti legislativi vigenti o in corso di adozione** a livello UE (v. infra). In particolare, il nuovo regolamento introduce:

- a) regole armonizzate per **l'immissione sul mercato**, la messa in servizio e l'uso dei sistemi di intelligenza artificiale nell'Unione;
- b) il **divieto** di determinate pratiche di intelligenza artificiale;
- c) requisiti specifici per i **sistemi di IA ad alto rischio** e obblighi per gli operatori di tali sistemi;
- d) regole di **trasparenza** armonizzate per alcuni sistemi di IA;
- e) regole armonizzate specifiche per l'immissione sul mercato di modelli di **IA di uso generale**;
- f) regole sul **monitoraggio** del mercato, sulla governance e sull'applicazione della **vigilanza** del mercato stesso;
- g) misure a sostegno dell'**innovazione**, con particolare attenzione alle PMI, comprese le start-up;

Il regolamento si applicherà ai **sogetti pubblici e privati**, all'interno e all'esterno dell'UE, a condizione che il **sistema di IA** sia **immesso sul mercato dell'Unione** o che il suo uso abbia effetti su persone situate nell'UE.

Riguarderà sia i **fornitori** (ad es. uno sviluppatore di uno strumento di screening dei CV) che gli **operatori di sistemi di IA ad alto rischio** (ad es., una banca che acquista uno strumento di screening dei CV).

Gli **importatori** di sistemi di IA dovranno inoltre garantire che il fornitore straniero abbia già eseguito l'appropriata procedura di valutazione della conformità, che il sistema rechi una marcatura di conformità europea (CE) e sia corredato della documentazione e delle istruzioni per l'uso richieste.

Il regolamento prevede inoltre determinati **obblighi per i fornitori di modelli di IA per finalità generali**, compresi i **modelli di IA generativa** di

grandi dimensioni. Invece, i fornitori di **modelli gratuiti e open source** saranno **esentati** dalla maggior parte di questi obblighi. Esenzione che tuttavia non riguarderà gli obblighi incombenti ai fornitori di modelli di IA per finalità generali che comportano **rischi sistemici**.

Il regolamento non **pregiudicherà le competenze degli Stati membri** in materia di **sicurezza nazionale**. Non si applicherà infatti ai sistemi di IA che sono esclusivamente per **scopi militari, di difesa o di sicurezza nazionale**, indipendentemente dal tipo di entità che svolge tali attività, nonché alle **attività di ricerca, sviluppo e prototipazione** che precedono l'immissione sul mercato o a persone che utilizzano l'IA per motivi non professionali.

### *Classificazione dei sistemi di IA e pratiche di IA vietate*

La nuova disciplina stabilisce obblighi per fornitori e operatori dei sistemi di IA a seconda del livello di rischio che l'IA può generare: i) un **rischio inaccettabile**; ii) un **rischio alto**; iii) un **rischio basso o minimo**; iv) un rischio specifico per la trasparenza.

#### Rischio inaccettabile

Saranno **vietati** i sistemi di IA che determinano un **rischio inaccettabile** per la sicurezza, i mezzi di sussistenza e i diritti delle persone. In questa categoria rientrano i sistemi che possono **manipolare il comportamento umano** come quelli che consentono di attribuire un "**punteggio sociale**" (*social scoring*), per finalità pubbliche e private, classificando le persone in base al loro comportamento sociale o alle loro caratteristiche personali, e **determinate applicazioni di polizia predittiva**.

Saranno **vietati**, in particolare:

- i **sistemi di riconoscimento delle emozioni utilizzati sul luogo di lavoro e negli istituti scolastici**, eccetto per motivi medici o di sicurezza (ad esempio il monitoraggio dei livelli di stanchezza di un pilota); i sistemi di sfruttamento delle vulnerabilità delle persone e di **utilizzo di tecniche subliminali**;
- alcuni sistemi di **categorizzazione biometrica** delle persone fisiche sulla base di dati biometrici per dedurne o desumerne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche o l'orientamento sessuale (sarà ancora possibile filtrare set di dati basandosi su dati biometrici nel settore delle attività di

contrasto) o di **identificazione biometrica in tempo reale in spazi accessibili al pubblico** (ossia il riconoscimento facciale mediante telecamere a circuito chiuso) da parte delle autorità di contrasto (con limitate eccezioni: *vedi oltre*);

- l'**estrazione non mirata** (*scraping*) di immagini facciali da internet o telecamere a circuito chiuso per la creazione o l'espansione di banche dati.

### Sistemi ad alto rischio

Il regolamento considera ad **alto rischio** un **numero limitato di sistemi di IA** che possono potenzialmente avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali (tutelati dalla **Carta dei diritti fondamentali dell'UE**).

Prima di **immettere un sistema di IA ad alto rischio sul mercato dell'UE**, o di farlo entrare in servizio, i fornitori dovranno sottoporlo a una **valutazione della conformità**. Dovranno, quindi, dimostrare che il loro sistema è **conforme ai requisiti obbligatori** per un'IA affidabile (ad esempio: qualità dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, accuratezza, cibersicurezza e robustezza). Anche per i sistemi biometrici è sempre richiesta una valutazione della conformità da parte di terzi. La valutazione dovrà essere ripetuta in caso di modifica sostanziale del sistema o della sua finalità. Si prevede inoltre una **valutazione d'impatto sui diritti fondamentali** prima che un sistema di IA ad alto rischio venga immesso sul mercato.

I sistemi di IA che costituiscono componenti di sicurezza di prodotti disciplinati dalla **legislazione settoriale** dell'Unione saranno sempre considerati ad alto rischio, se soggetti a una valutazione della conformità da parte di terzi ai sensi della legislazione settoriale stessa. I fornitori di tali sistemi dovranno inoltre **attuare sistemi di gestione della qualità e del rischio** per garantire la conformità ai nuovi requisiti e ridurre al minimo i rischi per gli utenti e per le persone interessate, anche dopo l'immissione sul mercato di un prodotto.

I sistemi di IA ad alto rischio implementati da autorità pubbliche o entità che agiscono per loro conto dovranno essere **registrati in una banca dati pubblica dell'UE**. Ove tali sistemi non siano utilizzati per le attività di contrasto e relative al controllo della migrazione, dovranno essere registrati

in una parte non pubblica della banca dati, che sarà accessibile solo alle autorità di controllo competenti.

Le **autorità di vigilanza** del mercato contribuiranno al monitoraggio successivo all'immissione sul mercato mediante audit e offrendo ai fornitori la possibilità di segnalare incidenti o violazioni gravi degli obblighi in materia di diritti fondamentali di cui sono venuti a conoscenza. Qualsiasi autorità di vigilanza del mercato potrà, per motivi eccezionali, autorizzare l'immissione sul mercato di una specifica IA ad alto rischio.

Tra i sistemi ad **alto rischio** rientrano: quelli di **identificazione biometrica**, categorizzazione biometrica e riconoscimento delle emozioni (al di fuori delle categorie vietate) e quelli utilizzati nella **gestione di alcune infrastrutture critiche** nei settori dell'acqua, del gas e dell'elettricità, del traffico stradale e dei **dispositivi medici**; quelli finalizzati a determinare **l'accesso agli istituti di istruzione e formazione professionale** (ad esempio: per valutare i risultati dell'apprendimento e orientare il processo di apprendimento e il monitoraggio dei comportamenti disonesti; quelli relativi alla **valutazione dell'occupazione**, ad ottimizzare la gestione dei lavoratori e l'accesso al lavoro autonomo (ad esempio: per pubblicare annunci di lavoro mirati, analizzare e filtrare le candidature e valutare i candidati), nonché per determinare **l'accesso a servizi e a prestazioni pubblici e privati essenziali** (come, ad esempio, l'assistenza sanitaria); quelli finalizzati alla **valutazione dell'affidabilità creditizia** delle persone fisiche, alla valutazione dei rischi finanziari, nonché alla determinazione dei prezzi in relazione ad assicurazioni sulla vita e assicurazioni sanitarie; quelli utilizzati nelle attività di **contrasto, controllo delle frontiere, amministrazione della giustizia, svolgimento dei processi democratici** e per la valutazione e classificazione delle chiamate di emergenza.

Non sono invece inclusi i **sistemi di raccomandazione delle piattaforme online di dimensioni molto grandi** (utilizzati dalle aziende online per suggerire agli utenti prodotti, servizi o contenuti che potrebbero essere di loro interesse) in quanto sono **già disciplinati** da altre normative (regolamento sui mercati digitali e regolamento sui servizi digitali).

L'**elenco** dei sistemi di IA ad alto rischio, che può essere **modificato** per allineare la normativa **all'evoluzione tecnologica**, è **allegato** al regolamento.

### Sistemi a rischio minimo

I sistemi di **IA a rischio minimo** (come **videogiochi o filtri spam**) saranno **esenti da obblighi**, ferma restando l'adesione volontaria a codici di condotta, da parte dei fornitori di tali sistemi, ad esempio laddove esista un evidente rischio di manipolazione. Gli utenti dovrebbero essere consapevoli del fatto che stanno interagendo con una macchina.

La **grande maggioranza dei sistemi di IA** attualmente utilizzati o il cui utilizzo è probabile nell'UE rientra in questa categoria.

### Rischio specifico per la trasparenza

A determinati sistemi di IA sono imposti **specifici obblighi di trasparenza**, ad esempio laddove esista un evidente rischio di manipolazione (come attraverso l'uso di **chatbot**); gli utenti dovranno essere consapevoli del fatto che stanno interagendo con una macchina.

Anche i **deep fake dovranno essere etichettati come tali** e gli utenti dovranno essere informati quando vengono utilizzati sistemi di categorizzazione biometrica o di riconoscimento delle emozioni.

Inoltre il regolamento prende in considerazione i **rischi sistemici** che potrebbero derivare dai **modelli di IA per finalità generali** (*General purpose AI*), compresi i **modelli di IA generativa di grandi dimensioni** (*vedi oltre*), che possono essere utilizzati per un'ampia serie di compiti e stanno diventando la base di molti sistemi di IA nell'UE. Alcuni di questi modelli potrebbero comportare rischi sistemici se risultano particolarmente efficaci o molto utilizzati. Modelli potenti potrebbero, ad esempio, causare incidenti gravi o essere utilizzati impropriamente per attacchi informatici di vasta portata.

Il “**rischio sistemico** a livello di Unione” si riferisce alla possibilità che l'uso dell'IA possa avere un **impatto significativo sul mercato** interno a causa della sua portata e con **effetti negativi reali o ragionevolmente prevedibili** su **salute pubblica, sicurezza, diritti fondamentali** o sulla **società nel suo insieme**, che possono essere propagati su larga scala lungo tutta la catena del valore. Ad esempio, se un'applicazione di guida autonoma mal funzionasse su larga scala, potrebbe causare incidenti stradali su vasta scala, influenzando quindi l'intero sistema di mobilità urbana.

Quanto al concetto di “**incidente grave**”, ci si riferisce a qualsiasi incidente o malfunzionamento di un sistema di IA che porti direttamente o indirettamente a uno dei seguenti effetti: (a) la morte di una persona o un

grave danno alla salute di una persona; b) un'interruzione grave e irreversibile della gestione e del funzionamento delle infrastrutture critiche; c) violazione degli obblighi derivanti dal diritto dell'Unione volti a tutelare i diritti fondamentali; d) danni gravi alla proprietà o all'ambiente.

Ad esempio, si pensi ad un errore in un sistema diagnostico medico basato sull'IA che porta a diagnosi errate e danni significativi ai pazienti.

### ***Eccezioni previste per le autorità di contrasto***

L'uso dell'AI da parte delle forze dell'ordine ha rappresentato **uno dei punti più delicati e controversi del negoziato**. Il compromesso raggiunto consente il **riconoscimento biometrico da remoto** in tempo reale negli **spazi accessibili al pubblico** solo in alcuni casi quali:

- 1) **attività di contrasto** relative a **16 reati specifici**: terrorismo; tratta di esseri umani; sfruttamento sessuale di minori e materiale pedopornografico; traffico illecito di stupefacenti e sostanze psicotrope; traffico illecito di armi, munizioni ed esplosivi; omicidio volontario; lesioni personali gravi; traffico illecito di organi e tessuti umani; traffico illecito di materie nucleari e radioattive, rapimento, sequestro e presa di ostaggi; reati che rientrano nella competenza giurisdizionale della Corte penale internazionale; dirottamento di un aeromobile o una nave; stupro; reati ambientali; furto organizzato o rapina a mano armata; sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra;
- 2) **ricerca mirata** di specifiche vittime, rapimento, tratta e sfruttamento sessuale di esseri umani e persone scomparse;
- 3) **prevenzione di minacce** per la vita o l'incolumità fisica delle persone o risposta da una minaccia attuale o prevedibile di **attacco terroristico**.

Si specifica che **l'identificazione biometrica può assumere varie forme**. Può essere utilizzata per l'autenticazione degli utenti, ad esempio per sbloccare uno *smartphone* o per le verifiche e l'autenticazione presso i valichi di frontiera nei controlli dell'identità e dei documenti di viaggio di una persona (corrispondenza "uno a uno"). L'identificazione biometrica remota potrebbe anche essere utilizzata per identificare persone nella folla, ad esempio confrontando l'immagine di una persona con quelle contenute in una banca dati (corrispondenza "uno a molti").

L'accuratezza dei sistemi per il **riconoscimento facciale** può variare in modo significativo in base a un'ampia gamma di fattori, quali la qualità della fotocamera, la luce, la distanza, la banca dati, l'algoritmo e l'etnia, l'età o il sesso del soggetto. Lo stesso vale per il riconoscimento vocale e dell'andatura e per altri sistemi biometrici. Il tasso di falsi positivi dei sistemi altamente avanzati è in continua diminuzione. Un tasso di accuratezza del 99% può sembrare adeguato, mentre è notevolmente rischioso quando può condurre a sospettare di una persona innocente. D'altra parte, anche un tasso di errore dello 0,1% è molto elevato se riguarda decine di migliaia di persone.

L'identificazione biometrica remota in tempo reale da parte delle autorità di contrasto sarà subordinata a un'**autorizzazione preventiva rilasciata da un'autorità giudiziaria o amministrativa indipendente**. In caso di **urgenza** debitamente giustificata, tuttavia, si potrà procedere **senza un'autorizzazione**, purché quest'ultima sia richiesta senza indebito ritardo, al più tardi entro 24 ore; se l'autorizzazione **non è concessa**, è necessario che tutti i dati e gli output siano soppressi. L'autorizzazione dovrà essere preceduta da una **valutazione preventiva d'impatto sui diritti fondamentali** e dovrà essere **notificata all'autorità di vigilanza e all'autorità per la protezione dei dati interessate**.

L'uso di sistemi di IA per l'**identificazione biometrica remota a posteriori** delle persone oggetto di indagine (identificazione di persone in materiale video raccolto in precedenza) richiederà l'autorizzazione preventiva di un'autorità giudiziaria o di un'autorità amministrativa indipendente e la notifica all'autorità per la protezione dei dati e all'autorità di vigilanza del mercato.

### ***Sistemi di IA per finalità generali e modelli fondativi o di base***

La nuova disciplina, introdotta nell'accordo di compromesso finale, su richiesta del PE, reca disposizioni dettagliate applicabili alle situazioni in cui i sistemi di IA per finalità generali (*general purpose AI*) sono utilizzati per scopi per i quali non sono stati **intenzionalmente e specificamente progettati** e in cui la tecnologia viene successivamente integrata in un altro sistema ad alto rischio. I modelli di IA per finalità generali **comprendono i modelli di IA generativa di grandi dimensioni**.

È considerato importante che un fornitore che intenda basarsi su un modello di IA per finalità generali disponga di tutte le informazioni

necessarie per far sì che il suo sistema sia sicuro e conforme al regolamento. Il regolamento obbliga i fornitori di tali modelli a **comunicare determinate informazioni ai fornitori di sistemi a valle**. I fornitori dovranno inoltre disporre di politiche in essere atte a garantire il **rispetto del diritto d'autore** nel corso della formazione dei loro modelli.

Alcuni di questi modelli potrebbero comportare **rischi sistemici** dato che sono particolarmente efficaci o molto utilizzati.

La Commissione europea ritiene che, allo stato attuale della tecnologia, i modelli di IA per finalità generali che sono stati addestrati utilizzando **una potenza di calcolo totale superiore a  $10^{25}$  FLOPS** comportino **rischi sistemici**. L'Ufficio per l'IA (istituito all'interno della Commissione) potrà **aggiornare tale soglia alla luce dell'evoluzione tecnologica** ovvero integrare il criterio della potenza di calcolo con altri criteri (ad esempio, il numero di utenti o il grado di autonomia del modello).

I fornitori di modelli che comportano rischi sistemici saranno pertanto tenuti a **valutare e attenuare i rischi**, a **segnalare incidenti gravi**, a **condurre prove e valutazioni dei modelli all'avanguardia**, a garantire la **cibersicurezza** e a fornire **informazioni sul consumo energetico** dei loro modelli. A tal fine potranno **collaborare con l'Ufficio europeo per l'IA** per elaborare codici di condotta. Un **gruppo di esperti scientifici** svolgerà un ruolo centrale nella supervisione dei modelli di IA per finalità generali.

**La Commissione spiega per quale motivo  $10^{25}$  FLOPS è una soglia adeguata per ritenere che un'IA per finalità generali possa comportare rischi sistemici.** La soglia, infatti, riflette i modelli di IA per finalità generali attualmente più avanzati, ossia **GPT-4 di OpenAI** e probabilmente **Gemini di Google DeepMind**. Non essendo ancora sufficientemente comprese le capacità dei modelli al di sopra di tale soglia, si ritiene che essi possano comportare rischi sistemici e che sia ragionevole, pertanto, imporre ai fornitori obblighi aggiuntivi.

Sono state inoltre concordate **regole specifiche per i modelli fondativi o di base** (la cui regolamentazione non era presente nella proposta originaria e che ha rappresentato una **tematica particolarmente divisiva nel negoziato**): i grandi sistemi in grado di svolgere con competenza un'ampia gamma di compiti distintivi, quali la generazione di video, testi, immagini, il calcolo di dati o la generazione di codici informatici. I modelli di base debbano **rispettare specifici obblighi di trasparenza** prima di essere immessi sul mercato. È stato introdotto un regime più rigoroso per i modelli di base "ad

**alto impatto"**, come **GPT-4**, per i quali occorre una verifica prima dell'immissione nel mercato con riguardo alla sicurezza informatica e alla trasparenza, nonché una condivisione della documentazione tecnica. Si tratta di modelli di base addestrati con grandi quantità di dati e di complessità, capacità e prestazioni avanzate ben al di sopra della media, che possono diffondere i rischi sistemici lungo la catena del valore.

### ***Misure a sostegno dell'innovazione***

Il regolamento contiene diverse **misure a sostegno dell'innovazione**. In particolare, consente la creazione di **spazi di sperimentazione normativa per l'IA** (*sandbox* normativi) e di **prova in condizioni reali**, che forniscono un ambiente controllato per testare tecnologie innovative per un periodo di tempo limitato, promuovendo in tal modo l'innovazione da parte delle imprese, delle PMI e delle *start-up*.

Gli Stati membri dovranno istituire **almeno un sandbox normativo sull'IA a livello nazionale**. Potrà anche essere istituito **congiuntamente** tra più Stati membri.

Le prove in condizioni reali dei sistemi di IA ad alto rischio potranno essere effettuate per un massimo di 6 mesi (prorogabili di altri 6 mesi). Prima delle prove dovrà essere elaborato un piano da presentare all'autorità di vigilanza del mercato, la quale dovrà approvare il piano e le condizioni di prova specifiche; in caso di mancata risposta entro 30 giorni, il piano si considererà tacitamente approvato. Le prove potranno essere oggetto di ispezioni senza preavviso da parte dell'Autorità.

Le prove in condizioni reali potranno essere effettuate solo se sono presenti garanzie specifiche: ad esempio, gli utenti dei sistemi sottoposti a prova in condizioni reali dovranno fornire un consenso informato, le prove non dovranno avere alcun effetto negativo sugli utenti, gli esiti delle prove dovranno essere reversibili o poter essere ignorati, i relativi dati dovranno essere cancellati dopo la conclusione delle prove. Una protezione speciale dovrà essere riservata ai gruppi vulnerabili, ad esempio a causa della loro età o della disabilità fisica o mentale.

### ***Architettura di governance***

Le **autorità nazionali competenti per la vigilanza del mercato** sorveglieranno l'attuazione delle nuove norme a livello nazionale, mentre un **Ufficio europeo per l'IA**, costituito presso la Commissione europea, garantirà il coordinamento a livello europeo.

Un **comitato scientifico di esperti indipendenti** avrà il compito di segnalare i rischi sistemici e contribuire alla classificazione e alla sperimentazione dei modelli. Un **comitato europeo per l'IA**, composto dai rappresentanti degli Stati membri, svolgerà il ruolo di **piattaforma di coordinamento e di organo consultivo** per la Commissione europea. Si prevede infine l'istituzione di un **forum consultivo** per i portatori di interessi, come i rappresentanti dell'industria, le PMI, le *start-up*, la società civile e il mondo accademico.

Più nello specifico, la missione dell'Ufficio per l'IA sarà quella di sviluppare le competenze e le capacità dell'Unione nel settore dell'IA e contribuire all'attuazione della legislazione dell'Unione in materia di intelligenza artificiale in una struttura centralizzata. In particolare, l'Ufficio avrà il compito di **applicare e supervisionare le nuove regole per i modelli di IA per finalità generali**, con il potere di richiedere documentazione, condurre valutazioni dei modelli, indagare sulle segnalazioni e chiedere ai fornitori di adottare misure correttive.

L'Ufficio garantirà inoltre il **coordinamento** per quanto riguarda la politica in materia di IA e la collaborazione tra le istituzioni, gli organi e le agenzie dell'Unione coinvolti, nonché con gli esperti e i portatori di interessi. In particolare, dovrà provvedere a creare un forte legame con la comunità scientifica per sostenere l'applicazione delle regole, fungerà da punto di riferimento internazionale per gli esperti e le organizzazioni di esperti indipendenti e faciliterà gli scambi e la collaborazione con istituzioni analoghe in tutto il mondo.

### ***Sanzioni***

Le **sanzioni** per le violazioni del nuovo regolamento sono state fissate in una **percentuale del fatturato annuo globale** nell'anno finanziario precedente della società incriminata **o in un importo predeterminato**, a seconda di quale sia il più elevato.

Più nello specifico, per i sistemi di IA che sono immessi sul mercato o messi in servizio e che non rispettano i requisiti del regolamento, gli Stati membri dovranno stabilire **sanzioni** effettive, proporzionate e dissuasive, comprese sanzioni amministrative pecuniarie, in relazione alle violazioni, e comunicarle alla Commissione. Il regolamento stabilisce le **soglie** da tenere in considerazione:

- fino a **35 milioni di euro o al 7% del fatturato** mondiale totale annuo dell'esercizio precedente (se superiore) per violazioni relative a pratiche vietate o per l'inosservanza di requisiti in materia di dati;

- fino a **15 milioni di euro o al 3% del fatturato mondiale** totale annuo dell'esercizio precedente, per l'inosservanza di qualsiasi altro requisito o obbligo del regolamento, compresa la violazione delle regole relative ai modelli di IA per finalità generali;
- fino a **7,5 milioni di euro o all'1,5% del fatturato mondiale** totale annuo dell'esercizio precedente, per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti in risposta a una richiesta;
- per ciascuna categoria di violazione, la **soglia per le PMI** sarebbe l'importo più basso tra i due previsti, mentre per le altre imprese sarebbe l'importo più elevato.

La Commissione, sulla base del parere del comitato, elaborerà orientamenti al fine di armonizzare le regole e le prassi nazionali in materia di calcolo delle sanzioni amministrative pecuniarie.

### ***Entrata in vigore***

Il regolamento sull'IA sarà pienamente applicabile **due anni** dopo la sua entrata in vigore, secondo il seguente approccio graduale:

- 6 mesi dopo l'entrata in vigore, gli Stati membri devono eliminare gradualmente i sistemi vietati;
- 12 mesi dopo: diventano applicabili gli obblighi relativi alla *governance* dell'IA per finalità generali;
- 24 mesi dopo: tutte le regole della legge sull'IA diventano applicabili, compresi gli obblighi per i sistemi ad alto rischio definiti nell'allegato III (elenco dei casi d'uso ad alto rischio);
- 36 mesi dopo: si applicano gli obblighi per i sistemi ad alto rischio definiti nell'allegato II (elenco della normativa di armonizzazione dell'Unione).

Il regolamento potrà essere modificato mediante **atti delegati e di esecuzione**, anche per aggiornare la soglia FLOPS (atto delegato), aggiungere criteri per classificare i modelli di IA per finalità generali come modelli che presentano rischi sistemici (atto delegato), modificare le modalità per istituire spazi di sperimentazione normativa ed elementi del piano di prova in condizioni reali (atti di esecuzione).

## **La posizione negoziale del Governo italiano**

Nel corso del complesso negoziato in seno al Consiglio, il **Governo italiano** si è sempre dichiarato a **favore** dell'introduzione di un quadro comune di regole sull'intelligenza artificiale, sottolineando l'importanza che il nuovo regolamento tutelasse i **diritti fondamentali**, imponesse **obblighi e sanzioni commisurati al rischio** e allo stesso tempo permettesse di **mantenere il passo tecnologico e lo slancio verso l'innovazione** di altri competitor globali, come Stati Uniti e Cina.

La **posizione negoziale italiana**, inoltre, si è basata su una **visione "umano-centrica"**, volta a promuovere pertanto la **semplificazione** e la **chiarezza delle definizioni** a partire da quelle di **IA, sistemi generativi, foundation model**.

Sulla base di questa impostazione, il Governo italiano ha insistito per la **compartmentazione di alcuni perimetri e settori esclusi** dall'ambito di applicazione della originaria proposta di regolamento, oltre che sulla maggior chiarezza rispetto al coordinamento con le normative di settore, in particolare **bancario e assicurativo**.

Si è espresso inoltre a favore di un sistema di **self-assessment da parte delle aziende dei sistemi di IA**, attraverso linee guida o un archivio di esempi. Quanto agli **obblighi**, ha supportato la definizione di oneri e obblighi lungo la catena del valore dei sistemi IA e insistito affinché quest'ultimi non risultino **troppo gravosi soprattutto per le PMI**.

Sempre per quanto concerne le **definizioni**, l'Italia ha chiesto chiarezza relativamente ai **sistemi a finalità generale** in quanto vi è il **rischio di rapida obsolescenza di definizioni troppo ristrette**.

Ha altresì espresso apertura rispetto alla possibilità per gli Stati membri di integrarsi attraverso **sandbox a livello unionale**. Ha chiesto pertanto di estendere la **presunzione di conformità** con la normativa UE anche ai **risultati** delle sandbox, per accelerare il processo di integrazione dei medesimi risultati nel contesto normativo.

L'Italia ha manifestato anche **apertura con riferimento alle valutazioni di impatto sui diritti fondamentali**, in linea con le richieste del Parlamento europeo e nazionale di maggiore attenzione ai profili etici.

Infine, il nostro Paese ha chiesto di includere tra i sistemi ad alto rischio i sistemi di ausilio e supporto al giudice nella ricerca e nell'interpretazione dei fatti e della

legge, nonché i sistemi di ADR (metodi alternativi di risoluzione delle controversie).

Per definire la convergenza su alcuni dei punti più complessi del negoziato, **Italia, Francia e Germania** il 30 ottobre scorso avevano tenuto un incontro trilaterale a Roma ([comunicato stampa](#)) durante il quale sono state discusse soprattutto le tematiche relative alla regolamentazione dei modelli fondativi, l'esclusione delle forze dell'ordine e della sicurezza nazionale e la classificazione dei sistemi ad alto rischio.

In esito all'incontro, i tre Paesi avevano sottoscritto un **documento di posizione** congiunto che si opponeva, con riferimento ai **modelli di fondazione**, all'**approccio graduale** della Presidenza spagnola basato su criteri e regole più rigorosi per i modelli ad alto impatto. I tre paesi avevano invece **chiesto** che nella prima fase i modelli in questione siano disciplinati da un **codice di condotta** e che le future sanzioni europee non vengano imposte in prima istanza.

In sostanza, i tre paesi hanno chiesto di **non applicare regole troppo stringenti ai sistemi di intelligenza artificiale generativa**, ma che le imprese possano sviluppare i modelli di fondazione, ossia i sistemi alla base dei prodotti di IA, come ChatGPT, semplicemente autocertificandone le caratteristiche e adeguandosi alle migliori pratiche.

### **Pacchetto per l'innovazione in materia di IA a sostegno delle *start-up* e delle PMI nel settore dell'intelligenza artificiale**

Facendo seguito all'accordo politico raggiunto a dicembre 2023, il **24 gennaio 2024** la Commissione europea ha varato un **pacchetto di misure** volto a **sostenere le *start-up* e le PMI europee nello sviluppo dell'intelligenza artificiale**. Il pacchetto:

- la [proposta di regolamento](#) che modifica il [regolamento \(UE\) 2021/1173](#) relativo all'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo (**EuroHPC**) per istituire **fabbriche di IA**, ([impresa comune](#) dei supercomputer dell'UE);
- la [decisione](#) istitutiva del richiamato Ufficio per l'IA in seno alla Commissione;
- la [comunicazione](#) sulle **start-up e l'innovazione in materia di IA** che delinea ulteriori **attività chiave**, tra cui:

- a) il sostegno finanziario attraverso [Orizzonte Europa](#) e il [programma Europa digitale](#) dedicato all'IA generativa (che dovrebbe generare un ulteriore investimento pubblico e privato complessivo di circa **4 miliardi di euro fino al 2027**);
- b) alcune iniziative volte a **rafforzare il bacino generativo di talenti** dell'UE in materia di IA attraverso attività di istruzione, formazione, qualificazione e riqualificazione;
- c) la promozione di investimenti pubblici e privati nelle start-up e nelle scale-up nel settore dell'IA, anche attraverso **il capitale di rischio o il sostegno al capitale** (ad es. nuove iniziative del [programma di accelerazione del CEI](#) e di [InvestEU](#));
- d) l'accelerazione dello **sviluppo e della diffusione di spazi [comuni europei di dati](#)**, messi a disposizione della comunità dell'IA, per i quali i dati sono una risorsa fondamentale per formare e migliorare i loro modelli;
- e) l'iniziativa "**GenAI4EU**", che mira a sostenere lo sviluppo di nuovi casi d'uso e applicazioni emergenti nei 14 ecosistemi industriali europei, nonché nel settore pubblico. I settori di applicazione comprendono la robotica, la salute, le biotecnologie, l'industria manifatturiera, la mobilità, il clima e i mondi virtuali.

La Commissione ha annunciato inoltre che sta istituendo, con diversi Stati membri, **due consorzi per l'infrastruttura digitale europea (EDIC)**, ovvero l'"**Alleanza per le tecnologie linguistiche**" (**ALT-EDIC**), che mira a sviluppare un'infrastruttura europea comune nelle tecnologie del linguaggio, volta anche a sostenere lo sviluppo di grandi modelli linguistici europei, e l'**EDIC "CitiVERSE"**, che tra l'altro aiuterà le città a simulare e ottimizzare i processi, dalla gestione del traffico alla gestione dei rifiuti. Gli Stati membri istituiranno ora i consorzi per l'infrastruttura digitale europea ALT-EDIC e CitiVERSE EDIC con il sostegno della Commissione.

La Commissione ha adottato anche una [comunicazione](#) che delinea **l'approccio strategico sull'uso dell'intelligenza artificiale**, anticipando e preparandosi all'attuazione del regolamento sull'IA. Comprende azioni concrete per garantire lo sviluppo e l'uso di un'IA affidabile, sicura ed etica. La Commissione annuncia altresì che si sta preparando a sostenere le PA dell'UE nell'adozione e nell'utilizzo dell'intelligenza artificiale.



## L'ATTIVITÀ DELLA CAMERA DEI DEPUTATI IN TEMA DI INTELLIGENZA ARTIFICIALE

### Giustizia

Per quanto riguarda il tema dell'intelligenza artificiale applicata alla giustizia nell'ambito dei lavori della Camera, si segnala, in primo luogo, la recente approvazione da parte dell'Assemblea, nella seduta del 28 settembre 2023, in sede di esame del disegno di legge di conversione del DL 105/2023 (A.C. 1373-A), dell'**ordine del giorno 9/1373-A/56 Enrico Costa**, con il quale la Camera impegna il Governo, nell'ambito della più ampia dimensione del **riconoscimento della prova «vocale»**, ad introdurre le opportune modifiche delle norme processuali al fine di istituire una specifica procedura, anche attraverso una puntuale forma di incidente probatorio, in fase di indagine o di udienza preliminare e su richiesta di parte, al fine di **garantire l'effettuazione di una perizia in caso di sospetti sull'alterazione di file audio o video per mezzo di sistemi di intelligenza artificiale**, attesa la facile reperibilità di sistemi e applicazioni basati sull'intelligenza artificiale in grado di replicare la voce di chiunque a sua insaputa.

Si segnala, inoltre, l'**interrogazione a risposta immediata in Commissione al Ministro dell'interno 5-01444 Magi** sulle direttive del Ministero in materia di riservatezza dei dati relativi ai partecipanti alle manifestazioni pubbliche, svolta nella seduta della Commissione Affari costituzionali dell'11 ottobre 2023, nella quale l'interrogante ha chiesto cosa prevedano nel dettaglio le *policies* delle Forze dell'ordine, e quali siano le direttive del Ministero, in materia di **riservatezza dei dati relativi a soggetti presenti a manifestazioni e ripresi in operazioni di ordine pubblico**, anche al fine di evitare, tra l'altro, che i dati, e in particolare le immagini, possano essere utilizzati in *software* e sistemi di intelligenza artificiale in violazione della normativa vigente.

Nella risposta il Governo ha assicurato che il trattamento dei dati avviene in conformità a quanto stabilito dal D.M. 24 maggio 2017 e dal D.P.R. 15/2018 e che sulla conformità di tali disposizioni alla normativa vigente si è pronunciato il Garante per la *privacy*. Nella risposta, inoltre, il Governo ha precisato che "le immagini video raccolte dalla Polizia di Stato non sono sottoposte a elaborazioni informatiche a fini identificativi".

Si segnala, infine, che presso la Commissione Giustizia del Senato, il 23 novembre 2023, è stata deliberata un'indagine conoscitiva sull'**impatto**

**dell'intelligenza artificiale nel settore della giustizia.** Una proposta analoga è stata avanzata presso la Commissione giustizia della Camera.

## **Difesa**

Nell'ambito della Difesa, la Commissione IV della Camera dei deputati ha deliberato, nella seduta dell'[8 novembre 2023](#), lo svolgimento di un'**indagine conoscitiva** su nuovi profili e criticità relativamente alla **difesa cibernetica**.

La difesa cibernetica si sostanzia in uno spettro di competenze dello Stato di natura prettamente militare, da inquadrare in una più ampia strategia nazionale per la **sicurezza cibernetica**, che a sua volta è intensamente integrata con l'Intelligenza Artificiale, tramite l'adozione sempre più frequente di strumenti e tecniche basati sull'Intelligenza Artificiale.

Proprio nella consapevolezza della rapida evoluzione e obsolescenza dello stato dell'arte nella materia, la Commissione Difesa, nel predisporre il programma dell'Indagine conoscitiva, ha previsto un campo di indagine quanto più ampio e flessibile possibile, in modo da coprire ogni eventuale esigenza informativa che si presentasse in corso d'opera.

Si ricorda infine che il dominio cibernetico e quello aero-spaziale sono stati inseriti, a livello normativo (articolo 88 del Codice dell'ordinamento militare), tra gli **ambiti tutelati dalla difesa nazionale**, insieme ai domini tradizionali (terrestre, marittimo e aereo).

## **Cultura**

Innanzitutto alla **Commissione VII (Cultura, scienza e istruzione)** è in corso di svolgimento una **indagine conoscitiva sull'impatto della digitalizzazione e dell'innovazione tecnologica sui settori di competenza dell'organo**.

Come evidenziato all'atto di deliberare l'avvio dell'iniziativa, lo sviluppo e la diffusione delle tecnologie digitali e di internet, che hanno conosciuto un impetuoso sviluppo a partire dagli anni '80 del secolo scorso, con il nuovo millennio sono venute ad assumere dimensioni quantitative e qualitative tali da investire ogni ambito della vita umana, ridefinendo modelli e paradigmi in campo sociale, economico, culturale e politico (c.d. *digital disruption*). L'impatto trasformativo della digitalizzazione è stato tale da spingere gli studiosi di diversi ambiti disciplinari a indicare come "era digitale" l'epoca presente, ascrivendo a tali sviluppi una valenza paragonabile a quella dei progressi e delle innovazioni che segnarono la rivoluzione industriale. Lo

scenario appena delineato - all'evidenza – rientra sotto molteplici profili nei settori di competenza o, comunque, d'interesse della VII Commissione: ciò sia per gli specifici e distinti temi di cui essa si occupa (cultura, istruzione, università, ricerca di base, sport, editoria); sia, in una logica più complessiva, per l'attenzione da essa tradizionalmente prestata alla dimensione antropologica e umanistica dei fenomeni, la quale, nel caso della digitalizzazione, è assai rilevante, se non addirittura prevalente, attesa la sua capacità d'imprimere mutamenti profondi negli schemi culturali e relazionali degli individui e delle collettività. L'indagine conoscitiva ha due obiettivi, fra loro sinergici. Il primo è quello di aprire una sede di confronto istituzionale con i soggetti pubblici e privati, le realtà nazionali e internazionali, gli operatori di settore, gli accademici e gli esperti per guidare un processo condiviso di emersione, perimetrazione e definizione dei temi, dei problemi e degli interessi in campo. Il secondo è quello di procurare alla Commissione dati, materiali istruttori e contenuti indispensabili per valutare, promuovere e adottare le conseguenti iniziative politiche e legislative, che, in un clima di aperto e costruttivo confronto fra tutte le Istituzioni, possano massimizzare per il nostro Paese i benefici della digitalizzazione, preservandone al contempo le peculiarità legate ai valori e al patrimonio che rendono l'Italia unica sul piano mondiale.

Nell'ambito dell'indagine, ad oggi il **tema dell'intelligenza artificiale**, sotto diverse angolazioni, è stato toccato principalmente, in ordine cronologico, nelle audizioni di [Roberto Sergio](#) (amministratore delegato della RAI), di [Giampaolo Rossi](#) (direttore generale della RAI), di [Carlo Bartoli](#) (presidente del Consiglio nazionale dell'Ordine dei giornalisti), di [Eduardo Montefusco](#) (presidente di Radio Dimensione Suono SpA), di [Massimo Pellegrino](#) (partner responsabile dei processi di innovazione digitale di Intellera Consulting), di [Francesco Angelo Siddi](#) (presidente di Confindustria Radio Televisioni), di [Salvatore Giordano](#) (legale del gruppo SIMAR), di [Mirko Tavosanis](#) (professore associato di linguistica italiana e presidente dei corsi di studio in informatica umanistica dell'Università di Pisa), di [Federico Ferrazza](#) (direttore di Wired Italia), di [Enzo Mazza](#) (presidente e amministratore delegato della Federazione industria musicale italiana), di [Stefano Da Empoli](#) (presidente dell'Istituto per la competitività - I-COM), di [Paolo Marzano](#) (professore di Diritto della proprietà intellettuale e di Tutela della proprietà intellettuale presso la Facoltà di Giurisprudenza della Luiss Guido Carli di Roma), di [Alessandro Giuli](#) (presidente della Fondazione MAXXI - Museo Nazionale delle Arti del XXI secolo), di [Padre Paolo](#)

[Benanti](#) (professore di teologia morale presso la Pontificia Università Gregoriana) e di [Roberto Sommella](#) (direttore di Milano Finanza).

L'indagine conoscitiva è in corso di svolgimento e non è dunque ancora stato approvato un documento conclusivo.

Si ricorda poi che presso la VII Commissione è stato avviato il dibattito connesso alla [risoluzione 7-00185](#) presentata da Alessandro Amorese (FdI) che **impegna il Governo**, anche alla luce del quadro normativo europeo in corso di definizione, **ad assumere iniziative per garantire il rispetto del diritto d'autore, la tutela dei dati personali, la trasparenza e la tracciabilità dei contenuti generati mediante intelligenza artificiale.**

Infine, risulta depositata la **proposta di legge [A.C. 1514](#) (Ascani e altri, PD)**, recante **"Disposizioni per assicurare la trasparenza nella pubblicazione e diffusione di contenuti prodotti mediante sistemi di intelligenza artificiale"**. Il testo, di cui non è stato ancora avviato l'esame, consta di 3 articoli.

Per quanto qui interessa, l'art. 2 prevede che tutti i contenuti prodotti mediante sistemi di IA devono essere chiaramente identificati come tali e resi riconoscibili agli utenti attraverso l'apposizione di etichette e di filigrana. I soggetti responsabili della pubblicazione e della diffusione dei contenuti prodotti mediante sistemi di IA, in ogni mezzo trasmissivo, devono fornire, all'inizio e alla fine del contenuto, un'etichetta e un avviso visibili e facilmente comprensibili agli utenti che indichino che il contenuto è stato creato, in tutto o in parte, da un sistema di intelligenza artificiale. L'Autorità per le garanzie nelle comunicazioni, con proprio regolamento, da adottare entro sessanta giorni dalla data di entrata in vigore della legge, stabilisce le modalità attraverso le quali i soggetti responsabili della pubblicazione e della diffusione dei contenuti prodotti mediante sistemi di IA, in ogni mezzo trasmissivo, devono rendere riconoscibile agli utenti che il contenuto è stato creato, in tutto o in parte, da un sistema di intelligenza artificiale.

### **Attività produttive**

Innanzi alla **Commissione X (Attività produttive, commercio e turismo)** è in corso di svolgimento una **indagine conoscitiva dal titolo: "sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano"**.

L'indagine conoscitiva, come chiarito nel programma approvato il 3 agosto 2023, è volta a restituire un quadro organico dello stato dell'arte

nell'applicazione dell'IA nel sistema industriale italiano e della regolamentazione vigente, con l'intento di proporre soluzioni normative adeguate, a descrivere le opportunità, le criticità e i rischi che l'implementazione dell'IA nei processi produttivi comporta, a rilevare in che modo l'IA possa diventare strategica per lo sviluppo delle attività imprenditoriali, a valutare i principali ostacoli alla competitività delle imprese italiane in rapporto al *digital-gap* che ancora interessa il nostro sistema produttivo, in particolare il sistema delle PMI, a individuare le metodologie di impiego dell'IA che possano supportare il commercio, l'artigianato e il turismo, a valutare l'impiego dei fondi PNRR per investimenti nell'innovazione, compresa l'intelligenza artificiale, nonché a valutare l'incidenza dei nuovi fenomeni globali per quanto riguarda l'impiego dell'IA nelle realtà imprenditoriali.

Il programma dell'indagine conoscitiva, tuttora in corso, prevede che intervengano in audizione rappresentanti istituzionali, associazioni di categoria e realtà rappresentative del settore, esperti provenienti da atenei e istituti di ricerca, nonché le associazioni dei consumatori.

Nel corso delle audizioni sin qui tenute, è emerso come l'intelligenza artificiale possa contribuire ad aumentare la produttività delle imprese operanti nei diversi settori e trovare applicazione lungo tutta la catena del valore, ottimizzando l'utilizzo delle materie prime, i processi di trasformazione, così come le attività di *marketing* e nei rapporti commerciali con i clienti, soprattutto nell'ambito dell'*e-commerce* ma non solo. Sono stati riportati anche esempi che dimostrano come l'IA possa utilmente essere utilizzata per migliorare la sicurezza sul lavoro e degli asset aziendali, così come per meglio garantire la conformità di operazioni e contratti tra privati ai diversi ordinamenti giuridici. È stato inoltre evidenziato come l'intelligenza artificiale, soprattutto generativa, possa – a differenza delle tecnologie dell'automazione tradizionale - migliorare i servizi prestati dalle professioni intellettuali.

Per cogliere tali opportunità, occorre però investire in formazione permanente sia per rafforzare le competenze utili allo sviluppo di tali tecnologie, sia per consentirne la diffusione e un uso consapevole da parte delle imprese, in particolare le PMI, che spesso non hanno le risorse finanziarie, manageriali e umane per investire e impiegare al meglio i sistemi di intelligenza artificiale. Un aspetto affrontato è anche quello della opportunità di adottare a livello europeo e nazionale un approccio strategico

allo sviluppo di banche dati e sistemi di intelligenza artificiale, così da ridurre la dipendenza da tecnologie importate dai grandi attori globali.

I soggetti auditi hanno poi rilevato come alcuni rischi connessi al ricorso all'intelligenza artificiale debbano essere valutati dal legislatore e dalle amministrazioni pubbliche competenti per assicurare un quadro normativo adeguato. In particolare, è stato posto l'accento sulla necessità di garantire la trasparenza e l'affidabilità dei sistemi di intelligenza artificiale attraverso attività di certificazione e regole che consentano di spiegare le modalità di funzionamento dei sistemi di intelligenza artificiale, così da evitare i *bias* e i pregiudizi che possono incidere sulle decisioni assunte avvalendosi di tali tecnologie, avere piena consapevolezza dei limiti e della qualità dei dati processati dai sistemi di IA e salvaguardare la *privacy* e i diritti dei consumatori. Altro compito della regolamentazione, che pur non deve tradursi in un ostacolo allo sviluppo e alla diffusione dell'intelligenza artificiale, inerisce alla corretta ripartizione delle responsabilità tra l'impresa che sviluppa il sistema di intelligenza artificiale e l'impresa che se ne avvale.

Infine, risultano depositate e assegnate alle commissioni X e IX le **proposte di legge**:

- [A.C. 1084](#) (Centemero ed altri, Lega), recante "**Disposizioni concernenti l'adozione di una disciplina temporanea per la sperimentazione dell'impiego di sistemi di intelligenza artificiale**". La proposta di legge, che consta di due articoli, disciplina la creazione di uno **spazio tecnico-normativo sperimentale e temporaneo per le attività che impiegano sistemi di intelligenza artificiale**, al fine di promuovere l'innovazione e di consentire lo sviluppo dell'intelligenza artificiale e dei suoi possibili usi nel territorio nazionale (art. 1). A tal fine, l'articolo 2 prevede l'adozione di uno o più **regolamenti**, con decreto del Presidente del Consiglio dei ministri, per definire le condizioni e le modalità di svolgimento di una sperimentazione, che ha una durata massima di diciotto mesi, prorogabili per un massimo di ulteriori dodici mesi, relativa all'impiego di sistemi di intelligenza artificiale volti al perseguimento dell'innovazione di servizi e di prodotti nei diversi settori. Istituisce, infine, presso la Presidenza del Consiglio, un **Comitato permanente per l'intelligenza artificiale**;
- [A.C. 1444](#) (Cannata e altri, FdI), recante "**Disposizioni concernenti la fornitura e l'impiego dei sistemi di intelligenza artificiale**". La

proposta di legge, composta da 14 articoli, reca disposizioni in materia di:

- a) **immissione nel mercato**, messa in servizio e **uso** dei sistemi di IA nel territorio nazionale;
- b) **trasparenza** dei sistemi di IA destinati a interagire con le persone fisiche, dei sistemi biometrici e dei sistemi di IA utilizzati per generare o manipolare immagini nonché contenuti audio o video;
- c) non conformità o **divieto di determinate pratiche** dei sistemi di IA;
- d) creazione di uno **spazio tecnico-normativo sperimentale e temporaneo** per le attività che sviluppano i sistemi di IA, al fine di verificarne e valutarne l'impatto nel territorio nazionale;
- e) istituzione del **Comitato nazionale** per i sistemi di IA presso la Presidenza del Consiglio.

## **Lavoro**

Lo scorso 28 settembre 2023, la XI Commissione Lavoro ha deliberato di svolgere un'**indagine conoscitiva sul rapporto tra intelligenza artificiale e mondo del lavoro, con particolare riferimento agli impatti che l'intelligenza artificiale generativa può avere sul mercato del lavoro.**

Nel programma dell'indagine si sottolinea che tali impatti possono dare luogo ad un primo effetto integrativo a carattere positivo, nel quale si teorizza che i sistemi di intelligenza artificiale generativa saranno in grado di integrare le mansioni ed i compiti delle persone incrementandone la produttività e causando una riduzione di posti di lavoro limitata, e ad un secondo effetto sostitutivo a carattere negativo, nel quale si teorizza una massiva sostituzione di lavoratori i cui compiti, in special modo quelli routinari e quelli ad alta connotazione intellettuale, saranno progressivamente sostituiti da un massiccio ricorso alla tecnologia, con effetti dirompenti non verificati sui livelli occupazionali in seno alle economie più moderne.

Dati raccolti a livello nazionale e sovranazionale confermano la necessità di indagare e governare con urgenza questo cambiamento per evitare *in primis* l'acuirsi di disuguaglianze produttive e competitive all'interno del sistema Paese, anche in termini di valore aggiunto per ora lavorata, ed in una seconda fase individuare i potenziali rischi del sistema Paese connessi ad eventuali processi di massiva ristrutturazione.

Tale indagine conoscitiva è quindi finalizzata alla comprensione e alla verifica delle proposte, delle prospettive e dei risultati dell'impatto dell'intelligenza artificiale e delle nuove tecnologie all'interno del lavoro, nel breve e nel medio termine, nonché all'approfondimento di ogni aspetto relativo al rapporto tra tecnologia e lavoro, con lo scopo di tracciare un punto di fatto e sollecitare una produzione normativa, che sappia incrementare la produttività delle aziende, rilanciando l'economia, nonché proteggere il mercato del lavoro nella direzione di una crescita economica socialmente responsabile.

La Commissione ha deliberato di svolgere, in seno a tale indagine conoscitiva, un ciclo di audizioni - che ha avuto inizio con l'audizione del Ministro del lavoro e delle politiche sociali, Marina Elvira Calderone (26 ottobre 2023) - particolarmente ampio ed articolato, che prevede il coinvolgimento di diversi soggetti interessati dalla tematica.

Di seguito un riepilogo delle audizioni finora svolte nell'ambito dell'indagine conoscitiva in oggetto:

- Prof. Guerino Nuccio Bovalino, Chercheur associé presso il LEIRIS - Laboratoire d'Études Interdisciplinaires sur le Réel et les;
- Imaginaires Sociaux de l'Université Paul Valéry-Montpellier, Francia (9 novembre 2023);
- Igor Bailo, Executive Director Data & Analytics di Engineering ingegneria informatica Spa (9 novembre 2023);
- Francesca Bitondo, Direttrice rapporti istituzionali, Microsoft Italia (9 novembre 2023);
- Prof. Francesco Fabrizio Delzio, Direttore del Master in Relazioni Istituzionali, Lobby e Human Capital della Luiss Business School (9 novembre 2023);
- Claudia Trivilino, Public Policy Manager, Italy and Greece di META (9 novembre 2023);
- Mauro Macchi, CEO di Accenture Italia (14 novembre 2023);
- Lelio Borgherese, Presidente di Assocontact (14 novembre 2023);
- Prof. Daniele Nardi, Direttore del Laboratorio Nazionale Artificial Intelligence and Intelligent Systems del CINI (15 novembre 2023);

- Andrea Orlandini, organizzatore della 22esima Conferenza internazionale dell'associazione italiana per l'intelligenza artificiale, e di Chiara Ghidini, vicepresidente dell'associazione italiana per l'intelligenza artificiale (15 novembre 2023);
- Emanuela Girardi, Board member di Adra - AI, Data and Robotics Association (15 novembre 2023);
- Alessandra Santacroce, Direttore Relazioni Istituzionali di IBM Italia S.p.A. (16 novembre 2023);
- Avv. Chiara Ciccia Romito, dottoranda di ricerca in «Lavoro, Sviluppo e Innovazione», Università degli Studi di Modena e Reggio Emilia - Fondazione Marco Biagi (16 novembre 2023);
- Roberto De Ioris, programmatore e docente di programmazione presso l'Accademia Italiana Videogiochi (16 novembre 2023);
- Rita Cucchiara, professore ordinario di «Computer vision and Cognitive systems» presso il Dipartimento di ingegneria «Enzo Ferrari»;
- dell'Università degli studi di Modena e Reggio Emilia (16 novembre 2023);
- Giovanni Paolino, presidente di Avedisco, e Giuliano Sciortino, Segretario generale di Avedisco (22 novembre 2023);
- Giorgio Metta, direttore scientifico dell'Istituto Italiano di Tecnologia (22 novembre 2023);
- Marco Trombetti, cofondatore e CEO Translated - Pi Campus (22 novembre 2023);
- Prof. Stefano Crisci, avvocato esperto di IA e professore di Market Regulation e Diritto del turismo e del governo del territorio presso l'Università La Sapienza di Roma (22 novembre 2023);
- Carlo Cosolo, consigliere di ADID (Associazione direttori italiani doppiaggio), e di Daniele Giuliani, presidente di ANAD (Associazione nazionale attori doppiatori) (6 dicembre 2023);
- Francesco Verbaro, Senior Advisor di AdEPP (6 dicembre 2023);
- Fosca Giannotti, professore ordinario di informatica presso la Scuola Normale Superiore (6 dicembre 2023);

- Stefano da Empoli, presidente di I-Com (6 dicembre 2023);
- Aldo Forte, responsabile Personale ed organizzazione di ENEL Spa. (13 dicembre 2023);
- Francesco Rutelli, Presidente di ANICA (13 dicembre 2023);
- Francesca Boccia, Coordinatrice Commissione nazionale sull'Intelligenza Artificiale di Federmanager (13 dicembre 2023);
- Chiara Trifino, addetta alle relazioni industriali di Conflavoro PMI (13 dicembre 2023);
- Cesare Damiano, presidente dell'Associazione Lavoro & Welfare (20 dicembre 2023);
- rappresentanti di Confprofessioni: Carlo Girella, relazioni istituzionali dell'ufficio studi (20 dicembre 2023);
- Marco Carlomagno, Segretario generale di FLP - Federazione Lavoratori Pubblici e Funzioni Pubbliche, e di Roberto Cefalo, responsabile area politiche contrattuali di FLP (20 dicembre 2023);
- Alberto Lucarelli, professore ordinario di diritto costituzionale presso l'Università degli studi di Napoli Federico II (20 dicembre 2023) rappresentanti dell'Associazione EG AIR (10 gennaio 2024);
- Armando Tursi, professore ordinario di diritto del lavoro presso l'Università degli studi di Milano (10 gennaio 2024);
- Matteo Flora, professore a contratto in Corporate reputation presso l'Università degli studi di Pavia (10 gennaio 2024);
- Giuseppe Attardi, professore ordinario di Informatica presso l'Università degli studi di Pisa (10 gennaio 2024).

Il termine per la conclusione dell'indagine conoscitiva è il 31 marzo 2024.

### **Affari sociali**

Presso la Commissione XII (Affari sociali) i temi dell'Intelligenza artificiale sono stati affrontati in primo luogo, sia pure in maniera indiretta, con riferimento alla **digitalizzazione in ambito sanitario, obiettivo della Missione 6 (Salute)** cui sono destinate risorse del Piano nazionale di ripresa e resilienza - PNRR, in termini di **nuovo Fascicolo sanitario elettronico** (circa 1,67 miliardi di euro): da un lato, per il trattamento, condivisione ed interoperabilità di **grandi dati** acquisiti grazie all'accesso garantito a tutti i

cittadini alle piattaforme dei servizi, e dall'altro. di **Telemedicina e cure domiciliari** (circa 4 miliardi) per assicurare un'assistenza sanitaria personalizzata, in particolar modo per i pazienti fragili.

Sul tema della Telemedicina è stata poi discussa nella seduta del 5 dicembre 2023 l'interrogazione a risposta immediata in Commissione [5-01699 \(MORGANTE Maddalena\)](#), in particolare sugli aspetti della televisita di pazienti affetti da malattie croniche come la sclerosi multipla, a cui il Governo ha risposto confermando l'intenzione, in accordo con gli obiettivi del PNRR, di implementare una rete infrastrutturale per connettere le strutture mediche tra loro e con i pazienti nelle loro unità remote.

Va infine ricordato che è attualmente all'esame della Commissione XII, la risoluzione in Commissione [7-00183 \(LOIZZO Simona\)](#), diretta ad impegnare il Governo a definire una normativa in grado di sfruttare pienamente il potenziale dei dati sanitari, tutelando il consenso, la privacy e la sicurezza dei cittadini, e individuando tra le finalità della proposta di regolamento comunitario sullo "spazio europeo dei dati sanitari" (cd. EHDS – *European Health Data Space*), quella di garantire l'accesso delle persone ai propri dati sanitari elettronici ed un maggiore controllo di tali dati, a livello nazionale e transfrontaliero, per assicurare l'omogeneità dei dati nell'ambito del mercato unico dei sistemi di cartelle cliniche elettroniche, dei dispositivi medici e dei sistemi di intelligenza artificiale (IA) ad alto rischio (cd. "uso primario dei dati").

Sul tema l'Ufficio di Presidenza della Commissione ha deliberato di audire la direzione generale del Ministero della salute, l'Istituto superiore di sanità, l'Agenas, l'Istat, il Garante per la protezione dei dati personali e le associazioni dei pazienti: le audizioni si svolgeranno nel corso delle prossime settimane.

### **Affari comunitari**

La XIV Commissione Politiche dell'UE non ha trattato espressamente degli sviluppi dell'intelligenza artificiale nelle sue attività ma tali tematiche sono comunque emerse nell'ambito dell'articolato **ciclo di audizioni informali** svolto in relazione all'esame, ai sensi dell'art. 127 Reg. Camera, della Comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo e al Consiglio - **La politica di ciberdifesa dell'UE** (Join (2022) 49 def) (assegnata, in sede primaria alle Commissioni riunite IV e IX), tuttora in via di svolgimento.

In particolare tra i soggetti che hanno fatto riferimento alle questioni legate all'IA nel corso delle audizioni si segnalano:

- i rappresentanti di Google Italia e di Apple Italia (12 aprile 2023);
- i rappresentanti di IBM Italia (3 maggio 2023);
- i rappresentanti di Hewlett Packard Enterprise – HPE Italia (3 maggio 2023);
- i rappresentanti di CISCO (31 maggio 2023);
- i rappresentanti di Samsung Electronics Italia (21 giugno 2023);
- i rappresentanti di DELL Technologies (21 giugno 2023);
- il prof. Federico Faggin (6 luglio 2023).

Si rappresenta, inoltre, che nelle prossime settimane, la XIV Commissione inizierà a trattare del tema dell'Intelligenza Artificiale, nell'ambito dell'esame, della Relazione della Commissione europea sul **controllo dell'applicazione del diritto dell'UE nel 2022** (COM(2023)453 *final*), nella quale una sezione è intitolata "*Un'Europa pronta per l'era digitale*".

### **Comitato per la documentazione**

Il Comitato di vigilanza per l'attività di documentazione, già nella scorsa Legislatura, ha iniziato a lavorare sul tema dell'intelligenza artificiale ritenendo che l'uso delle nuove tecnologie nel campo della conoscenza possa fornire un utile apporto anche allo sviluppo della documentazione parlamentare.

Durante la Legislatura in corso, il Comitato ha ripreso il lavoro su tale tematica con l'avvio di un'indagine conoscitiva, sviluppatasi a oggi nell'arco di dodici sedute, nell'ambito della quale sono stati auditi:

- Prof. Paolo BENANTI della Pontificia Università Gregoriana; Prof.ssa Rita CUCCHIARA dell'Università degli Studi di Modena e Reggio Emilia;
- Prof. Maurizio FERRARIS dell'Università di Torino; Prof. Gianluca MISURACA dell'Università politecnica di Madrid;
- Dott. Pier Luigi Dal Pino, Senior Regional Director Government Affairs Western Europe, Microsoft;
- Dott. Mattia De Rosa, Direttore dell'unità specialistica Data & AI, Microsoft;

- Dott. Alessio DEL BUE della Fondazione Istituto Italiano di Tecnologia; Nestor MASLEJ AI Index Research Manager dell'Università di Stanford;
- Anna MAKANJU, Head of Public Policy, OpenAI; Boris POWER, Head of Partnerships Research, OpenAI;
- Prof. Gianfranco BASTI, professore ordinario di Filosofia della Natura e della Scienza presso la Pontificia Università Lateranense;
- Naila MURRAY, Head of FAIR (Fundamental AI Research) Emea Lab META; Angelo MAZZETTI, Head of Public Policy Italy and Greece META;
- Michael Sellitto, Head of Global Affairs, Anthropic; Orowa SIKDER, Technical Lead on Applied Research, Anthropic.

Il 14 febbraio 2024 il Comitato presenterà il documento conclusivo dell'indagine conoscitiva. Nell'occasione, verrà attivato un *hackathon*, aperto a centri di ricerca e operatori del settore, per lo studio e lo sviluppo di sistemi da impiegare nell'ambito dell'attività di documentazione.



## ATTIVITÀ DEL SENATO IN TEMA DI INTELLIGENZA ARTIFICIALE

### Giustizia

La 2a Commissione (giustizia e affari interni) lo scorso [23 novembre](#) ha deliberato lo svolgimento di un'**indagine conoscitiva** “sull'impatto dell'intelligenza artificiale nel settore della giustizia”, che, attraverso una serie mirata di audizioni, dovrebbe approfondire in particolare i temi della giustizia predittiva e della formazione della prova.

### Cultura

Presso la 7a Commissione (Cultura e patrimonio culturale, istruzione pubblica, ricerca scientifica, spettacolo e sport) è in corso un'**indagine conoscitiva** “[sull'impatto dell'intelligenza artificiale nei settori di competenza della 7a Commissione, anche con riferimento al servizio ChatGPT](#)”, nell'ambito della quale sono stati già state svolte alcune audizioni.

### Lavori pubblici

L'8a Commissione (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) sta svolgendo un'**indagine conoscitiva** “[sull'utilizzo delle tecnologie digitali e dell'intelligenza artificiale nella pianificazione, nella costruzione e nel monitoraggio delle infrastrutture stradali, autostradali, ferroviarie, portuali, aeroportuali e logistiche](#)”, nell'ambito della quale sono in corso una serie di audizioni di rappresentanti di settore (per dettagli sulle audizioni svolte si veda [qui](#)).

### Attività legislativa

Lo scorso 19 ottobre è stato presentato il disegno di legge “Misure sulla trasparenza dei contenuti generati da intelligenza artificiale” ([A.S. 917](#)) a firma del sen. Antonio Nicita (PD-IdP) e altri. Il disegno di legge, assegnato all'8a Commissione in sede redigente, mira ad introdurre l'obbligo per i soggetti responsabili della pubblicazione e della diffusione dei contenuti

generati da IA, in ogni mezzo trasmissivo, di assicurare immediata riconoscibilità di questi agli utenti, nelle modalità definite dall'Autorità per le garanzie nelle comunicazioni (AGCOM) con proprio regolamento.

## **SESSIONE 1 - LE INDUSTRIE CREATIVE E CULTURALI DI FRONTE ALL'INTELLIGENZA ARTIFICIALE E IL SUO IMPATTO SULLA VITA QUOTIDIANA DEI CITTADINI EUROPEI**

L'intelligenza artificiale costituisce una delle modalità con cui l'industria culturale può:

- produrre nuovi prodotti e opere culturali;
- migliorare la fruizione delle opere culturali già esistenti.

Si pone, a tal proposito, il tema di come estendere alle nuove opere talune forme di tutela già riconosciute a favore delle opere artistiche e, più latamente culturali, di come promuoverne lo sviluppo.

Al contempo, anche quello di garantire la tutela delle opere "tradizionali" nella loro versione originale.

Ad alcuni di questi aspetti sono dedicate le disposizioni contenute agli articoli da 25 a 30 della legge 27 dicembre 2023, n. 206 (Disposizioni organiche per la valorizzazione, la promozione e la tutela del made in Italy).

### **La promozione delle imprese culturali e creative**

Gli articoli 25, 26, 29 e 30 della legge n. 206/2023 prevedono norme per la **promozione dell'innovazione da parte delle imprese culturali e creative** (artt. da 25 a 30).

In particolare, la legge qualifica:

- come **imprese culturali e creative** quegli enti e quei lavoratori autonomi che svolgono, in Italia o in uno degli Stati membri dell'Unione europea o in uno degli Stati aderenti all'Accordo sullo Spazio economico europeo, in via esclusiva o prevalente, una o più delle seguenti attività: ideazione, creazione, produzione, sviluppo, diffusione, promozione, conservazione, ricerca, valorizzazione e gestione di beni, attività e prodotti culturali. Sono altresì qualificati imprese culturali e creative i soggetti privati che svolgono, in via esclusiva o prevalente, attività economiche di supporto, ausiliarie o comunque strettamente funzionali all'ideazione, creazione, produzione, sviluppo, diffusione, promozione, conservazione, ricerca, valorizzazione o gestione di beni, attività e prodotti culturali (art. 25, commi 2 e 3);

- come **start up innovative culturali e creative** le società di capitali di recente costituzione che svolgono le suddette attività. La definizione di *start up* innovative prevede, ai sensi dell'articolo 25 del D.L. n. 179/2012) che tali soggetti abbiano un fatturato fino a 5 milioni di euro, investano in ricerca e sviluppo, impieghino ricercatori o laureati magistrali o siano titolari o depositari o licenziatari di almeno una privativa industriale (art. 25, comma 7).

Le imprese culturali e creative possono introdurre nella propria denominazione sociale la **dicitura di «impresa culturale e creativa» o «ICC»** e utilizzare tale denominazione nella documentazione e nelle comunicazioni sociali (art. 25, comma 9).

La legge, inoltre:

- istituisce **l'albo delle imprese culturali e creative di interesse nazionale**. L'iscrizione nell'albo importa anche la registrazione nel portale del Sistema archivistico nazionale del Ministero della cultura (art. 26);
- stanZIA **3 milioni di euro per ciascuno degli anni dal 2024 al 2033 per promuovere e sostenere gli investimenti effettuati nel territorio nazionale dalle imprese culturali e creative**, rinviando ad un decreto del Ministro della cultura, di concerto con il Ministro delle imprese e del made in Italy e con il Ministro dell'economia e delle finanze, previa intesa in sede di Conferenza unificata, la individuazione delle condizioni, dei termini e delle modalità per la concessione dei contributi in favore di dette imprese (art. 29);
- prevede l'adozione ogni tre anni, da parte del Ministro della cultura, di concerto con il Ministro delle imprese e del made in Italy e con il Ministro degli affari esteri e della cooperazione internazionale, sentita la Conferenza Stato-Regioni, di un **Piano nazionale strategico per la promozione e lo sviluppo delle imprese culturali e creative**. Tra le finalità, si segnala quella di favorire lo sviluppo del settore, con particolare riguardo agli aspetti innovativi e di sperimentazione tecnologica, nonché lo sviluppo delle opere dell'ingegno e la tutela della proprietà intellettuale (art. 30).

### **I creatori digitali**

La legge n. 206/2023, inoltre, qualifica come **creatori digitali** gli artisti che sviluppano opere originali ad alto contenuto digitale (art. 27, comma 1)

e prevede l'istituzione di un **repertorio delle opere dei creatori digitali** nel registro pubblico generale delle opere protette, di cui all'articolo 103 della legge 22 aprile 1941, n. 633 (art. 27, comma 2).

Si ricorda che, secondo l'articolo 1, comma 1, lett. *p*), del regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70 (adottato dall'AGCOM con la delibera n. 680/13/CONS del 12 dicembre 2013), e più volte modificato, per "opera digitale" s'intende un'opera, o parti di essa, di carattere sonoro, audiovisivo, fotografico, videoludico, editoriale e letterario, inclusi i programmi applicativi e i sistemi operativi per elaboratore, tutelata dalla Legge sul diritto d'autore e diffusa su reti di comunicazione elettronica.

Riguardo all'istituzione di un repertorio delle opere dei creatori digitali nel registro pubblico generale delle opere protette, si rammenta che il richiamato articolo 103 della L. n. 633/1941 ha istituito presso la Presidenza del consiglio dei ministri un registro pubblico generale delle opere protette – RPG ai sensi della stessa legge. Nel registro sono registrate le opere soggette all'obbligo del deposito con la indicazione del nome dell'autore, del produttore, della data della pubblicazione e con le altre indicazioni stabilite dal regolamento. Alla Società italiana degli autori ed editori è affidata, altresì, la tenuta di un registro pubblico speciale per i programmi per elaboratore. In tale registro viene registrato il nome del titolare dei diritti esclusivi di utilizzazione economica e la data di pubblicazione del programma, intendendosi per pubblicazione il primo atto di esercizio dei diritti esclusivi. La registrazione fa fede, sino a prova contraria, della esistenza dell'opera e del fatto della sua pubblicazione. Gli autori e i produttori indicati nel registro sono reputati, sino a prova contraria, autori o produttori delle opere che sono loro attribuite. La tenuta dei registri di pubblicità è disciplinata nel regolamento. I registri di cui al presente articolo possono essere tenuti utilizzando mezzi e strumenti informatici. Nel capo III, il R.D. n. 1369/1942, recante il regolamento per l'esecuzione della L. 22 aprile 1941, n. 633, per la protezione del diritto di autore e di altri diritti connessi al suo esercizio, detta le disposizioni di attuazione della disciplina relativa ai registri di pubblicità e deposito di esemplari delle opere.

## **Attività parlamentari in corso: l'indagine conoscitiva sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano**

Il tema della regolamentazione dell'AI risulta fondamentale anche in relazione alle sue applicazioni nei diversi settori dell'industria e dei servizi. In riferimento al sistema produttivo italiano, caratterizzato soprattutto da PMI (talvolta ancora sprovviste delle necessarie competenze per gestire l'Intelligenza artificiale), va rilevato come il nostro Paese sia sostanzialmente caratterizzato da una visione e una percezione non omogenee del tema, sebbene il comparto abbia già conosciuto un ampio sviluppo in termini di valore del mercato.

Sulla base di tali premesse, **la Commissione X** (Attività produttive, commercio e turismo), in data 3 agosto 2023, ha deliberato lo **svolgimento dell'indagine conoscitiva sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano**. Il termine, inizialmente fissato al 30 novembre 2023, è stato prorogato fino al 1° marzo 2024.

L'indagine conoscitiva, come chiarito nel [programma](#) approvato il 3 agosto 2023, è volta a restituire un quadro organico dello **stato dell'arte nell'applicazione dell'AI nel sistema industriale italiano e della regolamentazione vigente, con l'intento di proporre soluzioni normative adeguate**, a descrivere le **opportunità**, le **criticità** e i **rischi** che l'implementazione dell'AI nei processi produttivi comporta, a rilevare in che modo l'AI possa diventare strategica per lo sviluppo delle attività imprenditoriali, a valutare i principali **ostacoli alla competitività** delle imprese italiane in rapporto al **digital-gap** che ancora interessa il nostro sistema produttivo, in particolare il sistema delle **PMI**, a individuare le metodologie di impiego dell'AI che possano supportare il commercio, l'artigianato e il turismo, a valutare l'impiego dei **fondi PNRR** per investimenti nell'innovazione, compresa l'intelligenza artificiale, nonché a valutare l'incidenza dei nuovi **fenomeni globali** per quanto riguarda l'impiego dell'AI nelle realtà imprenditoriali.

Il programma dell'indagine conoscitiva, tuttora in corso, prevede che intervengano in audizione rappresentanti istituzionali, associazioni di categoria e realtà rappresentative del settore, esperti provenienti da atenei e istituti di ricerca, nonché le associazioni dei consumatori.

Nel corso delle audizioni sin qui tenute, è emerso come l'intelligenza artificiale possa contribuire ad aumentare la produttività delle imprese operanti nei diversi settori e trovare applicazione lungo tutta la catena del

valore, ottimizzando l'utilizzo delle materie prime, i processi di trasformazione, così come le attività di marketing e nei rapporti commerciali con i clienti, soprattutto nell'ambito *dell'e-commerce* ma non solo. Sono stati riportati anche esempi che dimostrano come l'IA possa utilmente essere utilizzata per migliorare la sicurezza sul lavoro e degli asset aziendali, così come per meglio garantire la conformità di operazioni e contratti tra privati ai diversi ordinamenti giuridici. È stato inoltre evidenziato come l'intelligenza artificiale, soprattutto generativa, possa – a differenza delle tecnologie dell'automazione tradizionale - migliorare i servizi prestati dalle professioni intellettuali.

Per cogliere tali opportunità, occorre però investire in formazione permanente sia per rafforzare le competenze utili allo sviluppo di tali tecnologie, sia per consentirne la diffusione e un uso consapevole da parte delle imprese, in particolare le PMI, che spesso non hanno le risorse finanziarie, manageriali e umane per investire e impiegare al meglio i sistemi di intelligenza artificiale. Un aspetto affrontato è anche quello della opportunità di adottare a livello europeo e nazionale un approccio strategico allo sviluppo di banche dati e sistemi di intelligenza artificiale, così da ridurre la dipendenza da tecnologie importate dai grandi attori globali.

I soggetti auditi hanno poi rilevato come alcuni rischi connessi al ricorso all'intelligenza artificiale debbano essere valutati dal legislatore e dalle amministrazioni pubbliche competenti per assicurare un quadro normativo adeguato. In particolare, è stato posto l'accento sulla necessità di garantire la trasparenza e l'affidabilità dei sistemi di intelligenza artificiale attraverso attività di certificazione e regole che consentano di spiegare le modalità di funzionamento dei sistemi di intelligenza artificiale, così da evitare i bias e i pregiudizi che possono incidere sulle decisioni assunte avvalendosi di tali tecnologie, avere piena consapevolezza dei limiti e della qualità dei dati processati dai sistemi di IA e salvaguardare la privacy e i diritti dei consumatori. Altro compito della regolamentazione, che pur non deve tradursi in un ostacolo allo sviluppo e alla diffusione dell'intelligenza artificiale, inerisce alla corretta ripartizione delle responsabilità tra l'impresa che sviluppa il sistema di intelligenza artificiale e l'impresa che se ne avvale.

### **Profili normativi: gli incentivi**

L'articolo 1, comma 226 della legge 30 dicembre 2018, n. 145 (Legge di bilancio 2019) ha istituito, nello stato di previsione del Ministero dello sviluppo economico (ora Ministero delle imprese e del made in Italy), un

Fondo per interventi volti a favorire lo sviluppo delle tecnologie e delle applicazioni di intelligenza artificiale, blockchain e internet of things, con una dotazione di 15 milioni di euro per ciascuno degli anni 2019, 2020 e 2021.

Le iniziative che il Fondo è destinato a finanziare comprendono i progetti di ricerca e innovazione da realizzare in Italia ad opera di soggetti pubblici e privati, anche esteri, nelle aree strategiche per lo sviluppo dell'intelligenza artificiale, della blockchain e dell'internet of things, funzionali alla competitività del Paese. Per l'attuazione dell'intervento il Ministero si è avvalso della società Infratel Italia S.p.a. mediante apposita convenzione.

I criteri e modalità di utilizzo delle risorse del Fondo sono stati definiti con D.M. 6 dicembre 2021.

Con [decreto direttoriale 24 giugno 2022](#) sono stati stabiliti i termini e le modalità per la [presentazione delle domande](#) di agevolazione, nonché i criteri per la concessione e l'erogazione delle agevolazioni.

I soggetti ammissibili sono stati individuati nelle **imprese di qualsiasi dimensione**, costituite in forma societaria e che esercitano attività industriali di produzione di beni e servizi, agro-industriali, artigiane, di trasporto, di servizi alle imprese che esercitano le predette attività, nonché i centri di ricerca con personalità giuridica.

Le grandi imprese sono ammissibili alle agevolazioni soltanto nell'ambito di un progetto che preveda una collaborazione effettiva con le piccole e medie imprese (PMI) beneficiarie.

Il [decreto direttoriale 24 giugno](#) ha disposto l'apertura dell'intervento agevolativo il 21 settembre 2022, con la possibilità di precaricare la documentazione prevista dal bando, a partire dal 14 settembre 2022. Il decreto ha stabilito in 25 milioni di euro la somma a valere sul fondo destinata a progetti volti a favorire lo sviluppo dell'intelligenza artificiale. Per essere ammessi, i progetti presentati dovevano prevedere spese e costi ammissibili non inferiori a 500 mila euro e non superiori a 2 milioni di euro. Le agevolazioni sono state concesse, nei limiti stabiliti dagli articoli 25 e 29 del Regolamento GBER ovvero dal Regolamento *de minimis*, in misura pari ad una percentuale tra il 50 e il 70 per cento delle spese sostenute per le attività di ricerca industriale, tra il 25 e il 45 per cento per le attività di sviluppo sperimentale e tra il 15 e il 50 per cento per i progetti relativi all'innovazione dei processi e all'innovazione dell'organizzazione. Le percentuali più alte sono state applicate alle imprese di micro e piccola dimensione. Le

percentuali più basse alle imprese di grande dimensione e agli organismi di ricerca. Maggiorazioni sono state previste per i progetti di ricerca industriale e sviluppo sperimentale che prevedessero una collaborazione effettiva tra imprese di cui almeno una PMI e una collaborazione effettiva tra imprese e organismi di ricerca.

A seguito dell'**esaurimento delle risorse** disponibili, con [decreto direttoriale 21 settembre 2022](#) è disposta, a partire dal 22 settembre 2022, la chiusura dello sportello per la presentazione delle domande di agevolazione.

La misura persegue gli obiettivi connessi al **programma Industria 4.0 – Transizione 4.0** (per un approfondimento, si veda il [tema](#) ad esso dedicato), che comprende una serie di interventi volti a promuovere l'innovazione delle imprese, alcuni dei quali rifinanziati a valere sulle risorse del PNRR (M1C2, investimento 1). Seppur non specificatamente finalizzati allo sviluppo e all'applicazione dell'intelligenza artificiale, gli investimenti promossi da alcuni di tali interventi possono comprendere l'introduzione dell'intelligenza artificiale nei processi produttivi.

In particolare, il **credito di imposta**, riconosciuto alle imprese dalla legge di bilancio 2021 (art. 1, commi 1051-1063, legge n. 178/2020), come modificata da ultimo con la legge di bilancio 2022 (art. 1, comma 44, legge n. 234/2021) che effettuano fino al 30 giugno 2026 **investimenti in beni strumentali nuovi**, è volto a promuovere l'acquisto di beni strumentali materiali tecnologicamente avanzati e connessi beni immateriali a vocazione tecnologica, quali *software*, sistemi, piattaforme e applicazioni di *artificial intelligence*, nonché tecnologie di *machine learning* che consentano alle macchine di mostrare un'abilità e/o attività intelligente in campi specifici a garanzia della qualità del processo produttivo e del funzionamento affidabile del macchinario e/o dell'impianto.

Si ricorda poi che un distinto **credito di imposta** è riconosciuto dalla legge di bilancio 2020 (art. 1, commi 198-209, legge n. 160/2019), come da ultimo modificata dalla legge di bilancio 2022 (articolo 1, comma 45, Legge n. 234/2022) fino al 2031 per gli **investimenti in ricerca e sviluppo** e fino al 2025 per gli investimenti in **innovazione tecnologica**.

### **Le questioni legate alla tutela dei consumatori**

Benché non sia stata adottata una disciplina specifica per la tutela dei consumatori nei confronti delle applicazioni dell'intelligenza artificiale, si segnala che, con D.Lgs. n. 26/2023, in recepimento della direttiva (UE)

2019/2161, sono state introdotte alcune disposizioni volte aggiornare la disciplina consumeristica alla luce dello sviluppo del commercio elettronico e della pubblicità *on line* e del ricorso da parte dei gestori dei mercati *on line* di algoritmi per la presentazione di offerte al pubblico (per un approfondimento, si veda il tema in materia di [concorrenza e tutela dei consumatori](#)). In particolare, è stato introdotto l'obbligo per il fornitore del mercato *on line*, prima che un consumatore sia vincolato da un contratto a distanza o da una corrispondente offerta, di indicare al consumatore (art. 49-*bis* del D.Lgs. n. 206/2005, inserito con D.Lgs. n. 26/2023), tra le altre, informazioni generali, attraverso un'apposita sezione dell'interfaccia online direttamente e facilmente accessibile, sui principali parametri che determinano la classificazione (ossia l'ordine e la modalità di esposizione) delle offerte presentate al consumatore in esito alla sua ricerca.

Inoltre, in base all'articolo 23 del Codice del consumo, come integrato dal D.Lgs. n. 26/2023, sono considerate pratiche commerciali ingannevoli:

- fornire risultati in risposta a una ricerca *on line* del consumatore senza indicare ogni eventuale annuncio pubblicitario a pagamento o pagamento specifico per ottenere una classificazione migliore;
- rivendere biglietti per eventi acquistati utilizzando strumenti automatizzati per eludere qualsiasi limite imposto riguardo al numero di biglietti acquistabili.

## SESSIONE 2 - LA DIDATTICA NELL'ERA DELL'INTELLIGENZA ARTIFICIALE: PROBLEMATICHE E IMPATTI

### 1. Le iniziative parlamentari in corso

Innanzi alla **Commissione VII (Cultura, scienza e istruzione)** della **Camera dei deputati** è in corso di svolgimento una **indagine conoscitiva sull'impatto della digitalizzazione e dell'innovazione tecnologica sui settori di competenza dell'organo**.

Come evidenziato all'atto di deliberare l'avvio dell'iniziativa, lo sviluppo e la diffusione delle tecnologie digitali e di internet, che hanno conosciuto un impetuoso sviluppo a partire dagli anni '80 del secolo scorso, con il nuovo millennio sono venute ad assumere dimensioni quantitative e qualitative tali da investire ogni ambito della vita umana, ridefinendo modelli e paradigmi in campo sociale, economico, culturale e politico (c.d. *digital disruption*). L'impatto trasformativo della digitalizzazione è stato tale da spingere gli studiosi di diversi ambiti disciplinari a indicare come "era digitale" l'epoca presente, ascrivendo a tali sviluppi una valenza paragonabile a quella dei progressi e delle innovazioni che segnarono la rivoluzione industriale. Lo scenario appena delineato - all'evidenza - rientra sotto molteplici profili nei settori di competenza o, comunque, d'interesse della VII Commissione: ciò sia per gli specifici e distinti temi di cui essa si occupa (cultura, istruzione, università, ricerca di base, sport, editoria); sia, in una logica più complessiva, per l'attenzione da essa tradizionalmente prestata alla dimensione antropologica e umanistica dei fenomeni, la quale, nel caso della digitalizzazione, è assai rilevante, se non addirittura prevalente, attesa la sua capacità d'imprimere mutamenti profondi negli schemi culturali e relazionali degli individui e delle collettività. L'indagine conoscitiva ha due obiettivi, fra loro sinergici. Il primo è quello di aprire una sede di confronto istituzionale con i soggetti pubblici e privati, le realtà nazionali e internazionali, gli operatori di settore, gli accademici e gli esperti per guidare un processo condiviso di emersione, perimetrazione e definizione dei temi, dei problemi e degli interessi in campo. Il secondo è quello di procurare alla Commissione dati, materiali istruttori e contenuti indispensabili per valutare, promuovere e adottare le conseguenti iniziative politiche e legislative, che, in un clima di aperto e costruttivo confronto fra tutte le Istituzioni, possano massimizzare per il nostro Paese i benefici della digitalizzazione, preservandone al contempo le peculiarità legate ai valori e al patrimonio che rendono l'Italia unica sul piano mondiale.

Nell'ambito dell'indagine, ad oggi il tema dell'intelligenza artificiale, sotto diverse angolazioni – fra le altre, editoria e servizio pubblico radiotelevisivo, giornalismo, educazione, cultura, proprietà intellettuale – è stato toccato principalmente, in ordine cronologico, nelle audizioni di [Roberto Sergio](#) (amministratore delegato della RAI), di [Giampaolo Rossi](#) (direttore generale della RAI), di [Carlo Bartoli](#) (presidente del Consiglio nazionale dell'Ordine dei giornalisti), di [Edoardo Montefusco](#) (presidente di Radio Dimensione Suono SpA), di [Massimo Pellegrino](#) (partner responsabile dei processi di innovazione digitale di Intellera Consulting), di [Francesco Angelo Siddi](#) (presidente di Confindustria Radio Televisioni), di [Salvatore Giordano](#) (legale del gruppo SIMAR), di [Mirko Tavano](#) (professore associato di linguistica italiana e presidente dei corsi di studio in informatica umanistica dell'Università di Pisa), di [Federico Ferrazza](#) (direttore di Wired Italia), di [Enzo Mazza](#) (presidente e amministratore delegato della Federazione industria musicale italiana), di [Stefano Da Empoli](#) (presidente dell'Istituto per la competitività - I-COM), di [Paolo Marzano](#) (professore di Diritto della proprietà intellettuale e di Tutela della proprietà intellettuale presso la Facoltà di Giurisprudenza della Luiss Guido Carli di Roma), di [Alessandro Giuli](#) (presidente della Fondazione MAXXI - Museo Nazionale delle Arti del XXI secolo), di [Padre Paolo Benanti](#) (professore di teologia morale presso la Pontificia Università Gregoriana) e di [Roberto Sommella](#) (direttore di Milano Finanza).

L'indagine conoscitiva è tuttora in corso di svolgimento e non è dunque ancora stato approvato un documento conclusivo.

Si ricorda poi che presso la VII Commissione è stato avviato il dibattito connesso alla [risoluzione 7-00185](#) presentata da Alessandro Amorese (FdI) che **impegna il Governo**, anche alla luce del quadro normativo europeo in corso di definizione, **ad assumere iniziative per garantire il rispetto del diritto d'autore, la tutela dei dati personali, la trasparenza e la tracciabilità dei contenuti generati mediante intelligenza artificiale.**

Infine, risulta depositata la **proposta di legge [A.C. 1514](#) (Ascani e altri, PD)**, recante **“Disposizioni per assicurare la trasparenza nella pubblicazione e diffusione di contenuti prodotti mediante sistemi di intelligenza artificiale”**. Il testo, di cui non è stato ancora avviato l'esame, consta di 3 articoli. Per quanto qui interessa, l'art. 2 prevede che tutti i contenuti prodotti mediante sistemi di IA devono essere chiaramente identificati come tali e resi riconoscibili agli utenti attraverso l'apposizione di etichette e di filigrana. I soggetti responsabili della pubblicazione e della

diffusione dei contenuti prodotti mediante sistemi di IA, in ogni mezzo trasmissivo, devono fornire, all'inizio e alla fine del contenuto, un'etichetta e un avviso visibili e facilmente comprensibili agli utenti che indichino che il contenuto è stato creato, in tutto o in parte, da un sistema di intelligenza artificiale. L'Autorità per le garanzie nelle comunicazioni, con proprio regolamento, da adottare entro sessanta giorni dalla data di entrata in vigore della legge, stabilisce le modalità attraverso le quali i soggetti responsabili della pubblicazione e della diffusione dei contenuti prodotti mediante sistemi di IA, in ogni mezzo trasmissivo, devono rendere riconoscibile agli utenti che il contenuto è stato creato, in tutto o in parte, da un sistema di intelligenza artificiale.

## **2. Approcci regolatori e politiche pubbliche in materia di AI nei settori dell'istruzione, dell'università e della ricerca di base**

Il settore dell'educazione (intesa in senso ampio) risulta fra quelli oggetto di maggiore considerazione negli strumenti internazionali ed europei in materia d'intelligenza artificiale.

Si consideri, al riguardo, che il report “[Governing AI for Humanity](#)” dell'AI Advisory Board dell'ONU menziona più volte l'educazione fra i settori più toccati dalle potenzialità e al contempo dai rischi della nuova tecnologia, evidenziando fra l'altro «besides misuse, we also note countervailing worries about missed uses — failing to take advantage of and share the benefits of AI technologies out of an excess of caution. Leveraging AI to improve access to education might raise concerns about young people's data privacy and teacher agency. However, in a world where hundreds of millions of students do not have access to quality education resources, there may be downsides of not using technology to bridge the gap. Agreeing on and addressing such trade-offs will benefit from international governance mechanisms that enable us to share information, pool resources, and adopt common strategies» (par. 38).

L'UNESCO ha attivato il progetto “**The Artificial Intelligence and the Futures of Learning**” nell'ambito del quale sono state adottate diverse iniziative e relazioni: [qui](#) la pagina dedicata.

Sulla esigenza della formazione per governare gli sviluppi dell'AI si concentra il [rapporto OCSE “Employment Outlook 2023 - Artificial Intelligence and the Labour Market”](#). Dedicato alla ricerca scientifica, e a come incrementarne la produttività tramite la nuova tecnologia, è l'altro

rapporto OCSE dal titolo “[Artificial Intelligence in Science: Challenges, Opportunities and the Future of Science](#)”.

Anche il Consiglio d'Europa da alcuni anni è al lavoro sull'intelligenza artificiale – per una sintesi complessiva cfr. il [rapporto The Council of Europe & Artificial Intelligence](#) – e il suo Steering Committee for Education ha prodotto sinora due documenti di rilievo:

- [Report on Artificial Intelligence and Education - A critical view through the lens of human rights, democracy and the rule of law \(2022\)](#);
- [Recommendation on developing and promoting digital citizenship education \(2019\)](#).

Un report apposito che si segnala è stato poi recentemente predisposto negli Stati Uniti dallo U.S. Department of Education con il titolo “[Artificial Intelligence and the Future of Teaching and Learning. Insights and Recommendations](#)”.

Anche all'interno del **regolamento europeo sull'AI** l'educazione riceve specifica attenzione. Anzitutto, l'educazione è espressamente menzionata fra gli ambiti al cui sviluppo l'intelligenza artificiale è chiamata a concorrere (**Considerando 3**).

Trattandosi di un diritto fondamentale, sono poi considerati ad altro rischio i sistemi AI di classificazione che si applichino all'educazione. Nel testo del Regolamento (**Considerando 35**) si evidenzia infatti come l'impiego di sistemi di AI nel settore sia importante per promuovere un'istruzione e una formazione digitale di alta qualità e per consentire a tutti i discenti e agli insegnanti di acquisire e condividere le abilità e le competenze digitali necessarie, compresa l'alfabetizzazione mediatica e il pensiero critico, per partecipare attivamente all'economia, alla società e ai processi democratici. Tuttavia – prosegue il Regolamento – i sistemi di AI utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'ammissione, per assegnare le persone a istituti o programmi di istruzione e formazione professionale a tutti i livelli, per valutare i risultati dell'apprendimento o per valutare le persone, per valutare il livello di istruzione appropriato per un individuo e influenzare materialmente il livello di istruzione e formazione che gli individui riceveranno o a cui potranno accedere o per monitorare e rilevare il comportamento vietato degli studenti durante i test su esami come parte o come condizione per la loro istruzione, sono da considerarsi sistemi di IA ad alto rischio (e dunque, da

assoggettarsi all'apposita disciplina per essi prevista), poiché possono determinare il corso educativo e professionale della vita di una persona e quindi influenzare la sua capacità di assicurarsi il sostentamento. Se progettati e utilizzati in modo improprio, tali sistemi possono essere particolarmente intrusivi e possono violare il diritto all'istruzione e alla formazione, nonché il diritto a non essere discriminati e a perpetuare modelli storici di discriminazione, ad esempio nei confronti delle donne, di determinate fasce d'età, delle persone con disabilità o di determinate origini razziali o etniche.

Con riguardo alla ricerca di base, il testo enuncia fra le sue finalità quelle di sostenere l'innovazione, rispettare la libertà della scienza e non pregiudicare l'attività di ricerca e sviluppo, e pertanto esclude dal proprio campo di applicazione i sistemi e i modelli di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici. Inoltre, il Regolamento afferma che la sua vigenza non debba pregiudicare l'attività di ricerca e sviluppo scientifico su sistemi o modelli di IA prima dell'immissione sul mercato o della messa in servizio (**Considerando 12 c**). Proprio per l'ambito della ricerca il testo riconosce la possibilità di attivare lo strumento della *regulatory sandbox*.

A livello di politiche pubbliche nazionali, l'intelligenza artificiale negli ambiti in questione trova considerazione all'interno del Programma strategico Intelligenza artificiale 2022-2024 del 24 novembre 2021, a cura del Ministero dell'Università e della Ricerca, del Ministero dello Sviluppo Economico e del Ministro per l'Innovazione tecnologica e la Transizione Digitale. Il Programma ricorda, anzitutto, che nel 2020 il mercato privato dell'Intelligenza Artificiale in Italia ha raggiunto un valore di 300 milioni di euro, con un aumento del 15% rispetto al 2019 ma pari a circa solamente il 3% del mercato europeo, nettamente inferiore rispetto al peso italiano sul PIL europeo (ca. 12%). All'interno del mercato italiano, un controvalore di 230 milioni di euro (77%) è fornito ad aziende italiane, mentre i restanti 70 milioni di euro (23%) sono esportati verso aziende estere. Rispetto a questi dati, si evidenzia comunque come, per un verso, la comunità scientifica italiana sia molto attiva nel settore dell'intelligenza artificiale; per altro verso, che accanto alle università e ai centri di ricerca, l'Italia dispone di un'ampia rete di centri di trasferimento tecnologico. Nel Programma si sostiene che il Paese debba investire nel sistema di formazione sull'intelligenza artificiale e nello sviluppo delle relative competenze per i cittadini. Ciò innanzitutto per essere all'avanguardia nella ricerca sull'IA, ampliando e migliorando i

programmi di dottorato e attraendo o trattenendo i migliori ricercatori. Inoltre, l'Italia deve garantire che l'intero tessuto economico sfrutti le opportunità di produttività insite nella diffusione dell'IA, rafforzando più in generale la componente STEM in tutto il sistema dell'istruzione, così da favorire lo sviluppo di una forza lavoro in grado di interagire con l'IA e sfruttarne i benefici.

Con riferimento specifico agli ambiti qui in esame, nel documento si propongono le seguenti misure:

- rafforzare il programma Nazionale di Dottorato: aumentare il numero di dottorati di ricerca;
- attrarre e trattenere i ricercatori: attrarre giovani ricercatori beneficiari di borse di ricerca internazionali di alto profilo come l'ERC;
- Promuovere corsi e carriere in materie STEM: integrare attività, metodologie e contenuti finalizzati allo sviluppo delle materie STEM nei curricula di tutti i cicli scolastici;
- Espandere l'IA negli ITS (“Istituti Tecnici Superiori”): espandere i corsi di programmazione e includere corsi e stage di IA applicata in tutti i curricula ITS;
- Rafforzare l'ecosistema italiano della ricerca sull'IA: creare un'architettura di ricerca su base hub & spoke con competenze territoriali;
- Lanciare la piattaforma italiana di dati e software per la ricerca sull'IA: creare una connessione strutturale di piattaforme nuove ed esistenti, dati e infrastrutture informatiche dedicate all'IA, con librerie open-source;
- Creare cattedre italiane di ricerca sull'IA: allocare fondi specifici per un unico Principal Investigator (PI), già iscritto ad università o centri di ricerca nazionali, per favorire la collaborazione con industrie ed enti pubblici;
- Creare iniziative IA-PRIN per ricerca fondamentale: promuovere bandi dedicati alla ricerca fondamentale sull'IA e sull'IA affidabile;
- Promuovere campioni nazionali IA multidisciplinari: lanciare sfide su temi specifici con concorrenti valutati sulla base di risultati misurabili;

- Lanciare bandi di ricerca-innovazione IA per collaborazioni pubblico-private: promuovere progetti su settori prioritari ma con proposte di libera iniziativa volte a trasferire competenze dalla ricerca alle industrie;
- Finanziare ricerca e applicazioni dell'IA creativa: finanziare progetti che integrano la ricerca accademica nel campo di frontiera dell'IA creativa assieme alle sue applicazioni industriali;
- Promuovere progetti bilaterali per incentivare il rientro in Italia di professionisti: lanciare bandi per progetti incentrati su temi specifici definiti da priorità italiane cofinanziati da un altro Paese con rientro in Italia di almeno un ricercatore.

A livello di sviluppi operativi e di iniziative istituzionali, si segnala fra l'altro che secondo le [Linee guida per le discipline STEM](#) adottate dal MIM con D.M. 184 del 15 settembre 2023 «nell'ambito del coding, del pensiero computazionale e dell'informatica può trovare spazio anche un corretto e consapevole utilizzo dell'intelligenza artificiale (IA) che, in ambito scolastico, può fornire varie opportunità formative, quali la personalizzazione dell'apprendimento e l'ampliamento dell'accesso all'istruzione, soprattutto in contesti in cui le risorse sono limitate. Le risorse digitali, gli strumenti e gli approcci didattici basati sull'IA possono migliorare l'efficacia dell'insegnamento e dell'apprendimento consentendo agli studenti di accedere a contenuti educativi di qualità. L'uso dell'IA in ambito scolastico può favorire negli studenti lo sviluppo di competenze tecniche rilevanti per il mercato del lavoro digitale, preparandoli per le sfide future e le opportunità di carriera legate alla tecnologia. È importante, comunque, affrontare anche i rischi associati all'uso dell'IA che potrebbe portare a una dipendenza eccessiva dalla tecnologia, rischiando di trascurare altre competenze e abilità fondamentali per gli studenti, quali la creatività, il pensiero critico e la risoluzione dei problemi in modo autonomo. Inoltre l'IA potrebbe richiedere la raccolta e l'elaborazione di grandi quantità di dati personali degli studenti, con ricadute sulla sicurezza delle informazioni sensibili. È necessario, pertanto, adottare misure rigorose per proteggere i dati degli studenti e garantire la conformità alle norme sul trattamento dei dati personali».

Sempre il MIM, anche nell'ambito della misura «Scuola di Alta Formazione e formazione obbligatoria per dirigenti scolastici, docenti e personale tecnico-amministrativo» contenuta nel PNRR (M4C1-Riforma

2.2) ha attivato una serie di corsi di formazione per i docenti in materia d'intelligenza artificiale. Cfr. qui il [portale dedicato](#).

Con il [D.M. 203 del 20 ottobre 2023](#) recante «Disposizioni concernenti le aree tecnologiche, le figure professionali nazionali di riferimento degli ITS Academy e gli standard minimi delle competenze tecnologiche e tecnico-professionali», fra l'altro, è stata espressamente prevista la figura del Tecnico superiore per la digitalizzazione dei processi con soluzioni Artificial Intelligence based. Diversi ITS hanno poi attivato corsi in materia.

### **3. Approcci regolatori e politiche pubbliche in materia di AI nei settori della cultura**

Il tema della cultura viene in rilievo nel report “[Governing AI for Humanity](#)” dell'AI Advisory Board dell'ONU soprattutto sotto il profilo della necessità di salvaguardare le diversità e il pluralismo culturale nella regolazione dell'AI.

Lo Steering Committee for Culture, Heritage and Landscape del Consiglio d'Europa in argomento ha adottato:

- [Recommendation on the role of culture, cultural heritage and landscape in helping to address global challenges](#) (2022);
- [E-relevance: The Role of Arts and culture in the Age of Artificial Intelligence](#) (2022);
- [Recommendation on culture's contribution to strengthening the internet as an emancipatory force](#) (2018);
- [Recommendation on Big Data for culture, literacy and democracy](#) (2017);
- [Recommendation on the Internet of citizens](#) (2016);
- [Brochure on Platform Exchanges on Culture and Digitisation](#).

Nel settore dei beni culturali le *digital humanities* o “informatica umanistica” stanno diventando sempre più uno strumento efficace per la gestione, tutela, salvaguardia e conservazione del patrimonio. Questo campo di studi integra le tecniche informatiche con le discipline umanistiche al fine di rendere più efficaci ed efficienti le ricerche, migliorare il processo di digitalizzazione, semplificarne le estrazioni semantiche e supportare le pubbliche amministrazioni, gli enti gestori e i professionisti del settore.

Nell’**AI Act europeo**, la cultura è espressamente menzionata fra gli ambiti al cui sviluppo l’intelligenza artificiale è chiamata a concorrere (**Considerando 3**); la diversità culturale è un fattore che dovrebbe essere preservato nella progettazione e nell’uso dell’AI.

A livello nazionale, nell’ambito delle politiche per la digitalizzazione dei beni culturali, se per un verso si richiamano le potenzialità dell’AI, per altro verso si evidenzia come «digitalizzare beni non metadati e/o descritti è fortemente sconsigliato. Questa eventualità potrebbe essere ammissibile [ad esempio nel caso di] campagne sperimentali orientate a una descrizione del bene eseguita online da una comunità di riferimento adeguatamente identificata (possibili progetti di *crowdsourcing*) o alla descrizione del soggetto con l’uso di algoritmi di intelligenza artificiale» (cfr. [Linee guida per la digitalizzazione del patrimonio culturale](#)). Sempre nell’ambito del processo di digitalizzazione dei beni culturali è stato adottato il [Piano di gestione dei dati \(Data Management Plan, abbreviato DMP\)](#) il quale avverte che «qualora i dati fossero stati elaborati tramite metodi di intelligenza artificiale (es. apprendimento automatico di conoscenza da testi o immagini), occorre considerare i limiti degli attuali sistemi di *machine learning* e valutare attentamente i possibili *bias* che ne derivano».

Sebbene principalmente concepito quale forma di contrasto alla c.d. *cancel culture*, un rilievo assume anche l’art. 28 della legge n. 206 del 2023 («Disposizioni organiche per la valorizzazione, la promozione e la tutela del made in Italy»), rubricato «Linee guida per la salvaguardia dell'autenticità storica delle opere musicali, audiovisive e librerie», ai sensi del quale «il Ministero della cultura adotta linee guida per assicurare che le opere musicali, audiovisive e librerie possedute dalle discoteche, cineteche e biblioteche pubbliche, ancorché oggetto di elaborazioni successive, siano conservate e rese fruibili anche nella loro versione originale, al fine di evitare che operazioni creative di riadattamento delle medesime opere con nuovi linguaggi comunicativi e divulgativi sostituiscano l'originale e ne facciano perdere la memoria». Il tema della “**novità**” dell’opera riadattata con nuovi linguaggi divulgativi e comunicativi rispetto all’originale è adombrato, con specifico riferimento al digitale, anche nel [Piano nazionale di digitalizzazione del patrimonio culturale 2022–2023](#) là dove si evoca il superamento della «funzione ancillare del bene digitale come replica o copia dell’originale fisico e afferma la legittimità di un percorso di conoscenza autonomo, peculiare e connotato da originalità. Originalità che non discende dall’oggetto ma dalla relazione intellettuale da cui il bene digitale prende

forma e da cui attinge nuovi significati trasmissibili e non solo “pensabili”. Il patrimonio culturale digitale è costituito da oggetti, la cui natura può essere definita sulla base delle relazioni informative che sono in grado di generare. Essi, anche quando collegati ai beni culturali fisici, possiedono un’autonomia ontologica, come ormai attestato da un’ampia letteratura». L’esistenza di tale *quid novi* fra opera originale e sue rielaborazioni sembra alla base della disposizione in commento e potrebbe assumere rilievo anche in caso di rielaborazioni operate dall’AI.

#### **4. Approcci regolatori e politiche pubbliche in materia di editoria e diritto d’autore**

Con riferimento all’**editoria e all’informazione**, nell’ambito del Consiglio d’Europa lo Steering Committee on Media and Information Society ha adottato fra gli altri strumenti di rilievo, tutti relativi anche all’impatto dell’AI:

- [Recommendation on the impacts of digital technologies on freedom of expression](#) (2022);
- [Recommendation on combating hate speech](#) (2022);
- [Recommendation on promoting a favourable environment for quality journalism in the digital age](#) (2022);
- [Recommendation on principles for media and communication governance](#) (2022);
- [Recommendation on electoral communication and media coverage of election campaigns](#) (2022);
- [Recommendation on the human rights impacts of algorithmic systems](#) (2020);
- [Guidance note on content moderation](#) (2021);
- [Guidance note on the prioritisation of public interest content online](#) (2021).

Nell’AI Act europeo, per quanto qui interessa si evidenzia come sia opportuno un obbligo di “*disclosure*”, cioè identificazione, in relazione al testo generato o manipolato dall’IA nella misura in cui viene pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico, a meno che il contenuto generato dall’AI non sia stato sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica sia

responsabile editoriale della pubblicazione del contenuto (**Considerando 70b**).

A livello nazionale, anche al fine di valutare l'impatto dell'AI sul settore, è stato istituito il Comitato per l'intelligenza artificiale istituito presso il Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio dei ministri.

Il Presidente del Comitato, Padre Paolo Benanti, è intervenuto in [audizione](#) il giorno 18 gennaio innanzi alla Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi per illustrare i principali filoni di studio e azione negli ambiti dell'editoria, dell'informazione, del giornalismo e della proprietà intellettuale.

Si rappresenta poi che l'art. 1, commi da 315 a 317 e 322 della L. 213/2023 (legge di bilancio 2024), interviene in materia di Fondo per il pluralismo e l'innovazione dell'informazione, contestualmente ridenominato Fondo unico per il pluralismo e l'innovazione digitale dell'informazione e dell'editoria, da un lato novellando direttamente la fonte istitutiva, cioè l'art. 1 della L. 198/2016; dall'altro lato, con una previsione autonoma, autorizzando il Governo ad adottare un regolamento di delegificazione ex art. 17, comma 2, della L. 400/1988, al fine di ridefinire e integrare i criteri per l'erogazione, a valere sul predetto Fondo, dei contributi a sostegno del settore dell'editoria e dell'informazione, individuati dal D.LGS. 70/2017. Fra tali criteri assumono qui rilievo le misure premianti per l'assunzione di giornalisti e di professionisti in possesso di qualifica professionale nel campo della digitalizzazione editoriale, comunicazione e sicurezza informatica finalizzata anche al contrasto del fenomeno delle *fake news*, con una età anagrafica non superiore ai trentacinque anni. Per approfondimenti, cfr. l'apposito [dossier](#) predisposto dal Servizio studi.

Autonoma considerazione merita poi il tema del **diritto d'autore e del copyright**, la cui protezione si è dimostrata esposta a rischi specifici nell'ambito dei procedimenti di addestramento e generazione da parte dell'AI. Esso è espressamente considerato nel report "[Governing AI for Humanity](#)" dell'AI Advisory Board dell'ONU, in relazione ai rischi specifici che la nuova tecnologia può ingenerare rispetto al lavoro, all'espressione artistica, alla protezione della proprietà intellettuale.

L'**AI Act europeo** assoggetta al rispetto della normativa unionale in materia tutti i sistemi di AI commercializzati nel mercato europeo e, fra l'altro, impone ai fornitori di servizi di offrire adeguate informazioni dei

materiali utilizzati per l'addestramento dell'intelligenza artificiale, anche al fine di consentire la tutela del diritto d'autore e del copyright ai soggetti interessati (Considerando 60j e 60 k).

A dimostrazione del rilievo dell'argomento milita la circostanza che attorno ad esso sia scaturita una mole già cospicua di dibattito e di contenzioso, che ha riguardato fundamentalmente, in via di estrema sintesi, due profili:

- nel proprio addestramento, i sistemi d'intelligenza artificiale attingono a una grande massa di dati e contenuti presenti in rete (c.d. webscraping), in alcuni casi protetti da copyright o altri diritti che ne limitano l'accesso o l'utilizzo senza autorizzazione. Al riguardo, fra le vicende dotate di maggior risalto vi è il [giudizio promosso dal New York Times contro Open A.I.](#), non ancora definito, con cui il primo contesta alla seconda di avere copiato illegalmente milioni di articoli del quotidiano per addestrare ChatGPT ed altri servizi con lo scopo di fornire articoli ed informazioni con una tecnologia che ora compete con il Times;
- la configurabilità di un diritto di proprietà intellettuale in caso di opera creata dall'AI. Il problema si è già posto in numerose occasioni. Lo United States Copyright Office ha adottato nel 2023 apposite linee guida ([Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence](#)) al fine di valutare se un'opera realizzata mediante strumenti d'intelligenza artificiale generativa possa o meno essere coperta da diritto d'autore. In questa prospettiva, secondo un giudizio caso per caso, l'ufficio valuta «whether the 'work' is basically one of human authorship, with the computer [or other device] merely being an assisting instrument, or whether the traditional elements of authorship in the work (literary, artistic, or musical expression or elements of selection, arrangement, etc.) were actually conceived and executed not by man but by a machine». Con la conseguenza che «if all of a work's "traditional elements of authorship" were produced by a machine, the work lacks human authorship, and the Office will not register it [...] If, however, a work containing AI-generated material also contains sufficient human authorship to support a claim to copyright, then the Office will register the human's contributions [...] In such cases, the applicant must disclose AI-generated content that is "more than de minimis». In senso analogo, anche diverse sentenze hanno negato la possibilità di

accordare il diritto d'autore là dove, in relazione a un'opera, manchi il requisito costitutivo della human authorship (cfr. ad esempio [United States District Court For The District Of Columbia, Stephen Thaler v. Shira Perlmutter, Civil Action No. 22-1564 BAH](#)). La Cassazione italiana, nell'ambito di una recente [ordinanza](#) (Cass. Civ., I, ord. 1107/2023) pur definita nel senso dell'inammissibilità del ricorso a essa sottoposto, ha comunque osservato come la «protezione del diritto d'autore postula il requisito dell'originalità e della creatività, consistente non già nell'idea che è alla base della sua realizzazione, ma nella forma della sua espressione, ovvero dalla sua soggettività, presupponendo che l'opera rifletta la personalità del suo autore, manifestando le sue scelte libere e creative; la consistenza in concreto di tale autonomo apporto forma oggetto di una valutazione destinata a risolversi in un giudizio di fatto» per poi aggiungere, ai fini che qui interessano, come l' «aver utilizzato un software per generare l'immagine [...] è pur sempre compatibile con l'elaborazione di un'opera dell'ingegno con un tasso di creatività che andrebbe solo scrutinato con maggior rigore». La pronuncia, pur non sciogliendo la questione in via definitiva e compiuta, non conclude a priori che il concorso dell'intelligenza artificiale alla realizzazione dell'opera escluda in ogni caso la configurabilità del diritto d'autore, dovendo valutarsi caso per caso.



### SESSIONE 3 - IL SETTORE SANITARIO DI FRONTE ALL'INTELLIGENZA ARTIFICIALE: PROSPETTIVE E SFIDE

In campo sanitario, la prospettiva dell'applicazione dell'Intelligenza Artificiale (AI) riguarda segnatamente la diagnosi clinica e l'assistenza alla persona, quale strumento della Telemedicina e del trattamento dei dati sensibili raccolti in un unico Fascicolo sanitario elettronico, integrando le diverse abilità e competenze degli operatori sanitari e medici. Il grande potenziale dell'AI è riconosciuto nelle [linee guida dell'OMS](#), in particolar modo quando medici specialistici ed operatori sanitari non dovessero risultare disponibili per la loro scarsa presenza in determinati settori, come ad esempio la radiologia e l'emergenza-urgenza.

Nell'utilizzo dei dati sanitari, i sistemi di intelligenza artificiale potrebbero avere accesso non autorizzato ad informazioni personali sensibili, che necessitano pertanto di tutele normative dei dati personali e della *privacy* e della sicurezza ed integrità dei dati stessi per mantenerne l'etica e la corretta informazione.

Come precisato dall'OMS, la telemedicina è una “scienza aperta e in continua evoluzione, poichè incorpora nuovi progressi nella tecnologia e risponde e si adatta alle mutevoli esigenze sanitarie e ai contesti delle società” ([WHO 2010](#)). In prospettiva essa può dimostrarsi in grado di ottimizzare i processi della medicina tradizionale in presenza per fornire al paziente maggiore possibilità di prevenzione, grazie alla periodicità controllata della visita e maggior comfort, soprattutto nel caso di pazienti disabili o particolarmente fragili che possono custodire i dispositivi utilizzati per il monitoraggio direttamente presso il domicilio, senza necessità di spostamento, limite molto evidente soprattutto durante emergenze pandemiche.

A livello europeo, il Comitato direttivo sui diritti umani nel campo della biomedicina e della salute ([CDBIO](#)) del Consiglio d'Europa ha pubblicato nel dicembre 2021 un [rapporto](#) sull'impatto dell'intelligenza artificiale sulla relazione medico-paziente e sui diritti umani secondo sei direttrici: 1) disuguaglianza nell'accesso a cure sanitarie di qualità, 2) trasparenza di fronte agli operatori sanitari e ai pazienti, 3) rischio di pregiudizio sociale nei sistemi di IA, 4) indebolimento della considerazione del benessere del

paziente, 5) rischio di condizionamento dell'automazione, dequalificazione e dislocamento della responsabilità e 6) impatto sul diritto alla *privacy*.

In Italia, il Ministero della salute ha definito nel 2014 specifiche indicazioni nazionali e [linee di indirizzo](#) per un'armonizzazione dei modelli di applicazione della Telemedicina, come erogazione di servizi di assistenza sanitaria mediante il ricorso a tecnologie innovative nel campo ICT (*Information and Communication Technologies*) in situazioni in cui il professionista o i professionisti della salute ed il paziente non si trovano nella stessa località. In ogni caso, i servizi della Telemedicina, potendo essere assimilati a qualunque servizio diagnostico e terapeutico, comportano la trasmissione sicura di informazioni e dati di carattere medico nella forma di testi, suoni, immagini o altre forme necessarie per la prevenzione, la diagnosi, il trattamento ed il successivo controllo dei pazienti (*follow up*).

I servizi di Telemedicina con applicazione delle tecnologie AI, a livello nazionale, possono inserirsi nel solco della riforma dell'assistenza territoriale/distrettuale già approvata nell'ambito delle riforme obiettivo del PNRR, con il [D.M. Salute 23 maggio 2022, n. 77](#), un regolamento che detta nuovi modelli e standard del sistema finalizzato a modernizzare le cure extraospedaliere per renderle più accessibili ed efficaci rispetto ai bisogni dei cittadini. (v. l' [articolo in Monitor 2021](#), Agenas, Il connubio tra telemedicina e intelligenza artificiale per un salto di qualità nelle cure).

Oltre a stabilire i pilastri dell'assistenza primaria, come le nuove Case della Comunità quali punto di riferimento per la risposta ai bisogni di natura sanitaria e socio-sanitaria della popolazione di riferimento ed il potenziamento delle cure domiciliari e dell'integrazione tra assistenza sanitaria e sociale per la presa in carico del paziente, il nuovo regolamento stabilisce la creazione di **servizi digitalizzati**, per favorire sia l'assistenza a domicilio, attraverso gli strumenti di telemedicina e telemonitoraggio, sia per l'integrazione della rete professionale che opera sul territorio e in ospedale.

In proposito, a maggio 2022 è stato pubblicato il [Decreto salute 29 aprile 2022](#)) contenente l'approvazione delle linee guida organizzative relative al «[Modello digitale per l'attuazione dell'assistenza domiciliare](#)».

Il [D.M. Salute 1° aprile 2022](#), ha inoltre ripartito analiticamente il subinvestimento 1.2.3, attribuendo la specifica sub-codifica, 1.2.3.1 alla

"Piattaforma di telemedicina" a cui sono stati destinati 250.000.000 euro e 1.2.3.2 "Servizi di telemedicina" a cui sono stati destinati 750.000.000 euro. Da febbraio 2023 fino al dicembre 2023, è prevista la fase di start up, con realizzazione della **Piattaforma nazionale di Telemedicina** da parte dell'operatore economico con collaudo e verbale di avvio dell'infrastruttura entro il 31/12/2023. Il [DM Salute del 28 settembre 2023](#) (G.U. del 20.11.2023) ha disposto il riparto delle risorse per i **Servizi di Telemedicina**, essendo stati acquisiti e valutati tutti i Piani operativi regionali e provinciali dalla Commissione tecnica di valutazione, istituita presso Agenas con [DM Salute 30 settembre 2022](#). Ciascun piano è stato approvato mediante atto deliberativo di ogni Regione e Provincia autonoma, a seguito del parere di congruità espresso dalla citata Commissione tecnica<sup>1</sup>.

All'Intelligenza artificiale si prospetterebbe un ruolo propedeutico di valutazione del **bisogno sanitario del cittadino** finalizzato ad assisterlo in una prima fase e, nei casi più gravi, affidarlo successivamente alle cure di medici specialisti ovvero indirizzarlo presso altre strutture sanitarie del SSN per accertamenti diagnostici. Ciò anche al fine di sollevare l'attuale numero dei medici dalla pressione degli iscritti dovuta in molti casi alla loro carenza<sup>2</sup>.

In base ai dati dell'Annuario statistico italiano, i MMG nel 2021 erano circa 40.000, con una continua diminuzione nel triennio, visto il calo del 3,5 per cento (2023 su 2020) e del 5,1 per cento rispetto al 2019. Anche l'offerta

---

<sup>1</sup> Il riparto, per complessivi 527.101.620 euro (v. [tabella del riparto](#)) è stato effettuato in base ai fabbisogni di servizi minimi di telemedicina e del numero dei pazienti da assistere (complessivamente 158.433 entro il 2023 per televisite e telemonitoraggi) indicati in ciascun piano operativo regionale e di provincia autonoma. Le centrali di acquisto sono collocate presso la regione Puglia (per l'acquisizione di postazioni di lavoro) e la regione Lombardia (per l'acquisto di servizi minimi di telemedicina)

<sup>2</sup> Gli Accordi collettivi nazionali per la disciplina dei rapporti con i medici di medicina generale e con i pediatri di libera scelta prevedono, salvo eccezioni, che ciascun medico di medicina generale assista al massimo 1.500 pazienti adulti (di età superiore ai 13 anni) e ciascun pediatra 800 bambini (di età compresa tra 0 e 13 anni). Esistono comunque realtà territoriali in cui, per carenza di medici pediatri o per libera scelta dei genitori, è consentito che i bambini siano assistiti da medici di medicina generale. Nel 2021 si ha un valore di 6,8 medici ogni 10 mila abitanti, rispetto ai 7,1 medici del 2019 e 2020. A livello territoriale la variabilità regionale passa da 6,2 medici ogni 10 mila abitanti nel Nord-ovest e 6,3 nel Nord-est, a 7,4 nel Centro e 7,8 nelle Isole. Per quanto riguarda l'offerta di medici pediatri, sul territorio nazionale nel 2021 operano circa 7 mila medici pediatri: 9,2 ogni 10 mila bambini fino a 14 anni, con valori più bassi nel Nord-ovest (8,2 pediatri) e più alti nel Centro e nelle Isole (9,9 rispettivamente).

di medici pediatri è in diminuzione rispetto all'anno precedente, con un calo del 3,6 per cento rispetto al 2020 e del 5,2 per cento rispetto al 2019<sup>3</sup>.

Sulla **digitalizzazione dei servizi sanitari**, il PNRR destina in particolare risorse per il Servizio sanitario nazionale con riferimento sia ad un **punto unico di accesso ai servizi di sanità digitale**, sia alla messa a regime del Fascicolo sanitario elettronico (FSE), dirette alla trasformazione digitale entro l'anno 2025 ed entro la metà del 2026 (M6 C2 I1.3.2 Infrastruttura tecnologica del Ministero della salute e analisi dei dati, modello predittivo e di simulazione per la vigilanza LEA) con **292,6 milioni** destinati:

- a) al rafforzamento infrastrutturale degli strumenti tecnologici e di *data analysis* del Ministero della salute volti a completare la piattaforma open data e migliorare i sistemi di raccolta dei dati sanitari (92,7 milioni);
- b) alla reingegnerizzazione del Nuovo sistema informatico sanitario (NSIS) a livello locale per completare il monitoraggio dei LEA e potenziare la qualità dei dati clinici ed amministrativi (103,3 milioni);
- c) alla costruzione e realizzazione del cd. *National Health Hub*, un modello predittivo di simulazione degli scenari di medio e lungo termine del Sistema sanitario (77 milioni);
- d) allo sviluppo della piattaforma nazionale per i servizi di Telemedicina per la loro governance ed effettiva diffusione (19,6 milioni).

Riguardo il **potenziamento del Fascicolo sanitario elettronico (FSE)**, il PNRR prevede l'obiettivo che almeno l'85% dei medici di base possa alimentare il FSE regolarmente mediante sostegno e formazione per l'aggiornamento digitale e l'adozione ed utilizzo del FSE da parte di tutte le regioni, garantendo l'omogeneità, interoperabilità e l'accessibilità ad assistiti ed operatori sanitari a livello nazionale. La spesa prevista è di **1.380 milioni** di cui 569,6 milioni già stanziati per l'Infrastruttura nazionale per

---

<sup>3</sup>I medici di guardia medica, nel 2021, sono circa 10 mila, con un valore di 17,4 ogni 100 mila abitanti, in diminuzione del 9,6 per cento rispetto al 2020 e del 10,1 per cento rispetto al 2019. Un servizio che svolge un ruolo importante, sia nel favorire il processo di deospedalizzazione, sia nel garantire una risposta adeguata alla domanda sanitaria da parte di persone non autosufficienti o con gravi problemi di salute, è rappresentato dalle strutture per l'assistenza residenziale e semiresidenziale.

l'interoperabilità dei Fascicoli sanitari elettronici finalizzato alla realizzazione del Sistema di Tessera sanitaria elettronica (STS), tramite:

- l'integrazione/inserimento dei documenti nel FSE da documenti nativi digitali, con migrazione/ trasposizione *ad hoc* di documenti cartacei attuali o vecchi;
- il sostegno finanziario a favore dei fornitori di servizi sanitari, affinché aggiornino la loro infrastruttura e per garantire che i dati, i metadati e la documentazione relativi all'assistenza sanitaria siano generati in formato digitale;
- il sostegno finanziario per i fornitori di servizi sanitari che adotteranno la piattaforma nazionale, l'interoperabilità e gli standard UI/UX.

Con il [D.M Salute 20.5.2022](#), il Ministero della salute ha adottato le Linee guida per l'attuazione del Fascicolo sanitario elettronico che definiscono i nuovi contenuti, servizi ed architettura del FSE. Per quanto riguarda i progetti regionali, in conformità con quanto previsto all'interno dei Piani operativi allegati ai CIS sottoscritti con le Regioni e le Province autonome in data 30 e 31 maggio 2022, è stato siglato il [D.I. Ministro Innovazione Tecnologica e Transizione digitale, Min. Salute e MEF 8 agosto 2022](#) per l'assegnazione di risorse all'attività per l'“Adozione e utilizzo FSE da parte delle Regioni”<sup>4</sup>. Il [Decreto Interministeriale 18.5.2022](#) ha inoltre definito l'“Integrazione dei dati essenziali che compongono i documenti del FSE”, ampliando i documenti clinici presenti nel Fascicolo nelle diverse Regioni.

### **Attività parlamentari in corso**

Si segnala che presso la Commissione XII (Affari sociali) i temi dell'Intelligenza artificiale sono stati affrontati in primo luogo, sia pure in maniera indiretta, con riferimento alla **digitalizzazione in ambito sanitario, obiettivo della Missione 6** (Salute) cui sono destinate risorse del Piano nazionale di ripresa e resilienza - PNRR, in termini di **nuovo Fascicolo sanitario elettronico** (circa 1,67 miliardi di euro): da un lato, per il trattamento, condivisione ed interoperabilità di **grandi dati** acquisiti grazie all'accesso garantito a tutti i cittadini alle piattaforme dei servizi, e di **Telemedicina e cure domiciliari** (circa 4 miliardi), dall'altro, per assicurare

---

<sup>4</sup> M6C2 1.3.1(b).

un'assistenza sanitaria personalizzata, in particolar modo per i pazienti fragili.

Sul tema della Telemedicina è stata poi discussa nella seduta del 5 dicembre 2023 l'interrogazione a risposta immediata in Commissione [5-01699 \(MORGANTE Maddalena\)](#), in particolare sugli aspetti della televisita di pazienti affetti da malattie croniche come la sclerosi multipla, a cui il Governo ha risposto confermando l'intenzione, in accordo con gli obiettivi del PNRR, di implementare una rete infrastrutturale per connettere le strutture mediche tra loro e con i pazienti nelle loro unità remote.

Va infine ricordato che è attualmente all'esame della Commissione XII, la risoluzione in Commissione [7-00183 \(LOIZZO Simona\)](#), diretta ad impegnare il Governo a definire una normativa in grado di sfruttare pienamente il potenziale dei dati sanitari, tutelando il consenso, la privacy e la sicurezza dei cittadini, e individuando tra le finalità della proposta di regolamento comunitario sullo "spazio europeo dei dati sanitari" (cd. EHDS – *European Health Data Space*), quella di garantire l'accesso delle persone ai propri dati sanitari elettronici ed un maggiore controllo di tali dati, a livello nazionale e transfrontaliero, per assicurare l'omogeneità dei dati nell'ambito del mercato unico dei sistemi di cartelle cliniche elettroniche, dei dispositivi medici e dei sistemi di intelligenza artificiale (IA) ad alto rischio (cd. "uso primario dei dati").

Sul tema l'Ufficio di Presidenza della Commissione ha deliberato di audire la direzione generale del Ministero della salute, l'Istituto superiore di sanità, l'Agenas, l'Istat, il Garante per la protezione dei dati personali e le associazioni dei pazienti: le audizioni si svolgeranno nel corso delle prossime settimane.

## **SESSIONE 4 - LE SFIDE DELL'INTELLIGENZA ARTIFICIALE PER LA GOVERNANCE PUBBLICA**

### **Trasformazione della vita delle persone attraverso le piattaforme digitali pubbliche**

Al giorno d'oggi l'evoluzione tecnologica ci mette a disposizione degli strumenti che sono in grado di trasformare in modo profondo tanto le organizzazioni pubbliche quanto quelle private. Tra questi strumenti, un ruolo di primo piano è assunto dalle piattaforme digitali, le quali stanno ridisegnando non solo le modalità che gli individui hanno di relazionarsi tra di loro, ma anche con il potere pubblico.

Non c'è dubbio che, tra le innumerevoli potenzialità delle piattaforme, figuri anche quella di indirizzare l'attività della pubblica amministrazione verso obiettivi, tra l'altro, di efficienza, trasparenza e semplificazione. È in questa direzione che si muovono istituti quali la firma elettronica, la posta elettronica certificata, la carta nazionale dei servizi, il Sistema Pubblico di Identità Digitale (SPID), che il Codice dell'amministrazione digitale definisce disciplinando l'utilizzo delle tecnologie dell'informazione e della comunicazione nell'attività amministrativa. Quelle citate peraltro non sono le uniche "infrastrutture abilitanti" attualmente operative, tra le quali troviamo ad esempio anche la Carta d'identità elettronica, l'applicazione dei servizi pubblici IO, la fatturazione elettronica, l'Anagrafe nazionale della popolazione residente o, ancora, il sistema di Gestione elettronica dei pagamenti verso la PA (PagoPA).

Il percorso di digitalizzazione dei servizi della Pubblica Amministrazione, avviato quasi vent'anni fa, è stato senz'altro accelerato dalla pandemia, la quale ha messo in luce l'importanza delle infrastrutture della rete e della connettività. Non a caso, la realizzazione degli obiettivi di crescita digitale, di modernizzazione della pubblica amministrazione e di rafforzamento della capacità amministrativa del settore pubblico sono considerate una priorità per il rilancio del sistema Paese da parte del Piano nazionale di ripresa e resilienza.

La digitalizzazione delle pubbliche amministrazioni, in particolare, assume un ruolo centrale nel contesto del Piano, costituendo, assieme alla innovazione e alla sicurezza nella PA, una delle tre componenti progettuali attorno cui si sviluppano le linee di intervento della Missione n. 1.

Un'altra finalità a cui il progresso tecnologico può verosimilmente rivolgersi è quella di favorire la partecipazione democratica. Lo stesso Codice dell'amministrazione digitale, a tale proposito, introduce un vero e proprio diritto di partecipazione democratica elettronica laddove prevede che i cittadini sono chiamati a partecipare al processo democratico e ad esercitare i propri diritti politici usufruendo delle possibilità offerte dalle nuove tecnologie. Quello della "democrazia elettronica" costituisce comunque un terreno piuttosto scivoloso, ad oggi fermo a una fase di isolate sperimentazioni, essendo molteplici e innegabili i rischi connessi a una concezione digitale della democrazia. La delicatezza del tema, d'altra parte, mal si presta a raccogliere facili entusiasmi.

Più in generale, a fronte delle straordinarie opportunità che offrono le infrastrutture digitali, notevoli sono anche i rischi connessi al loro utilizzo, a cominciare da quelli che corrono, ad esempio, i minori, la garanzia della cui sicurezza oggi rappresenta una priorità assoluta. Ma i rischi connessi alla digitalizzazione sono, in realtà, molteplici, e non si limitano a riguardare soltanto soggetti, per così dire, deboli.

Si pensi, a tale riguardo, all'aumento estremamente significativo, sia in termini di quantità che di sofisticatezza, degli attacchi informatici che hanno interessato le istituzioni pubbliche negli ultimi anni. Il che, oltre a rendere evidente la vulnerabilità di questi sistemi, manifesta in tutta la sua impellenza la necessità di intervenire per migliorare la resilienza e le capacità di risposta agli incidenti informatici, investendo nel settore della cibersicurezza, come d'altra parte sia l'Italia che l'Europa stanno facendo.

Il potenziamento della protezione delle reti, dei sistemi informativi e dei loro utenti dalle minacce informatiche rappresenta un obiettivo prioritario per la tutela dei cittadini, delle imprese e delle stesse istituzioni pubbliche, rispetto al cui conseguimento la cooperazione tra Stati è in grado di giocare un ruolo fondamentale.

### **Le sfide dell'implementazione dell'intelligenza artificiale nel settore pubblico**

Esistono molteplici ragioni per cui l'implementazione della tecnologia AI nelle istituzioni governative è più complicata di quanto lo sia per le imprese private. Queste sfide includono:

- **Vincoli finanziari:** molti governi dispongono di risorse finanziarie limitate rispetto alle grandi aziende che possono investire

massicciamente in nuove tecnologie come l'intelligenza artificiale. Di conseguenza, le organizzazioni del settore pubblico potrebbero avere difficoltà a stanziare i fondi necessari per sviluppare e implementare progetti di intelligenza artificiale.

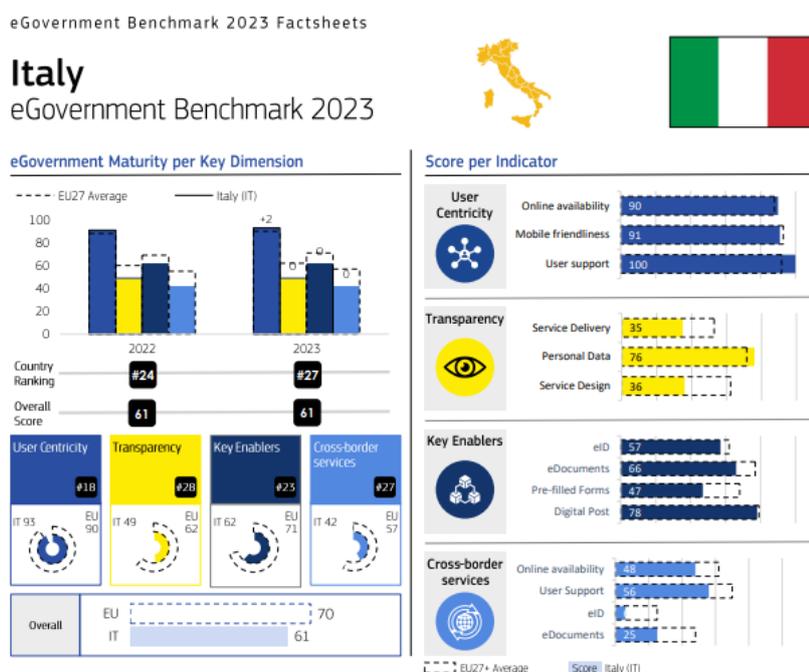
- processo decisionale burocratico: a differenza delle entità aziendali in cui le decisioni tendono a muoversi rapidamente attraverso le gerarchie, il processo decisionale governativo spesso richiede tempo a causa di processi burocratici o considerazioni politiche. Ciò può portare a ritardi nell'implementazione dei progetti di intelligenza artificiale e ostacolare la tempestiva attuazione;
- conformità normativa: le organizzazioni governative spesso operano in base a normative rigorose, che possono limitare la loro capacità di adottare determinate tecnologie o richiedere passaggi aggiuntivi al momento della loro introduzione. Le leggi sulla protezione dei dati, le preoccupazioni sulla privacy e le questioni etiche relative agli algoritmi di apprendimento automatico devono essere attentamente considerate prima dell'implementazione;
- infrastruttura tecnologica: le organizzazioni del settore pubblico potrebbero non disporre dell'infrastruttura tecnologica necessaria per supportare i progetti di intelligenza artificiale. Ciò include hardware, software e funzionalità di rete necessarie per eseguire algoritmi avanzati di intelligenza artificiale e gestire set di dati di grandi dimensioni;
- fiducia e responsabilità pubblica: i governi devono mantenere la fiducia del pubblico e garantire la responsabilità nell'implementazione della tecnologia IA. Ciò implica affrontare le preoccupazioni relative alla privacy, all'equità e ai potenziali pregiudizi nei sistemi di intelligenza artificiale.

### **Approcci regolatori e politiche pubbliche in materia di AI nei settori dell'amministrazione pubblica, delle istituzioni e dei processi democratici e dei diritti fondamentali**

Attraverso [l'eGovernment Benchmark](#) la Commissione europea ogni anno effettua un test su un campione di servizi digitali pubblici, nazionali e locali, per verificarne affidabilità, efficienza ed efficacia per gli utenti, e stila una classifica dei paesi più virtuosi. Gli indicatori e sottoindicatori utilizzati per effettuare tale valutazione sono la centralità dell'utente, la trasparenza, la

mobilità transfrontaliera e i fattori chiave abilitanti, vale a dire le precondizioni tecniche per la fornitura dei servizi digitali.

Nella classifica stilata per gli anni 2021 e 2022, l'Italia ha ottenuto 61 punti su 100, posizionandosi al di sotto della media (70) dei paesi partecipanti all'esercizio del Benchmark (EU27+).



Fonte: Commissione europea

L'organo consultivo sull'intelligenza artificiale attivato dal Segretario generale delle Nazioni Unite ha emesso il documento Interim Report: [Governing AI for Humanity](#) – attualmente in consultazione pubblica –, in cui si suggerisce un più stretto allineamento tra le norme internazionali e il modo in cui l'intelligenza artificiale viene sviluppata e implementata e si propone come rafforzare la *governance* internazionale dell'IA.

In particolare, il report rileva che le opportunità e i rischi connessi all'IA per le persone e la società sono entrambi evidenti ma non equamente distribuiti. Questa tecnologia pertanto richiede una *governance*, non solo per affrontare le sfide e i rischi, ma anche per garantire che il suo potenziale venga sfruttato in modo da non lasciare indietro nessuno.

Una *governance* globale con una partecipazione di tutti gli Stati è necessaria per rendere le risorse accessibili, i meccanismi di rappresentanza

e di supervisione ampiamente inclusivi, nonché garantire che la competizione geopolitica non conduca ad una IA irresponsabile.

**L'European Committee on Legal Co-operation** supervisiona il lavoro del Consiglio d'Europa nel campo del diritto pubblico e privato, sviluppando standard comuni e promuovendo la cooperazione giuridica. Esso è incaricato di affrontare le nuove ed emergenti sfide derivanti dall'uso dell'IA nella sua area di competenza, ovvero il diritto pubblico, il diritto privato e l'amministrazione della giustizia.

Il principale documento prodotto nel contesto di tale attività è lo “[Studio comparativo sul diritto amministrativo e sull'uso dell'IA e di altri sistemi algoritmici nel processo decisionale amministrativo negli Stati membri](#)” (2022).

**L'European Committee on Democracy and Governance** - che è il forum intergovernativo del Consiglio d'Europa per la definizione e lo scambio di standard nel campo della democrazia e della *governance* e il rafforzamento delle istituzioni democratiche a tutti i livelli di governo – offre una guida agli Stati membri, a tutti i livelli di governo, per sfruttare le opportunità offerte dalla trasformazione digitale riducendo al contempo i possibili rischi, in particolare per quanto riguarda l'uso dell'IA e del processo decisionale automatizzato nel settore pubblico.

I principali documenti prodotti in tale ambito sono:

- [Linee guida sull'uso delle tecnologie dell'informazione e della comunicazione \(TIC\) nei processi elettorali \(2022\)](#);
- [Studio sull'impatto della trasformazione digitale, compresa l'intelligenza artificiale e il processo decisionale automatizzato, sulla democrazia e sul buon governo \(2021\)](#);
- [Manuale sulla democrazia elettronica \(2020\)](#);
- [Raccomandazione sugli standard per il voto elettronico \(2017\)](#).

La **Commissione di Venezia**, che è l'organo consultivo del Consiglio d'Europa sulle questioni costituzionali, fornisce consulenza legale agli Stati membri nei settori delle istituzioni democratiche e dei diritti fondamentali, della giustizia costituzionale e della giustizia ordinaria, nonché in materia di elezioni, referendum e partiti politici. La Commissione elabora anche

rapporti trasversali e ha già prodotto due documenti riguardanti le tecnologie digitali e le elezioni. Inoltre, ha dedicato la 19a Conferenza europea degli organi di gestione elettorale al tema "Intelligenza artificiale e integrità elettorale".

I principali documenti disponibili sul tema sono i seguenti:

- [Conclusioni della 19a Conferenza europea degli organi di gestione elettorale "Intelligenza artificiale e integrità elettorale" \(2022\)](#);
- [Principi per un uso delle tecnologie digitali conforme ai diritti fondamentali nei processi elettorali \(2020\)](#);
- [Rapporto congiunto della Commissione di Venezia e del direttorato della Società dell'Informazione e Azione contro il Crimine della Direzione generale per i diritti umani e lo stato di diritto \(DGI\) sulle tecnologie digitali e le elezioni \(2019\)](#).

Dal [rapporto The Council of Europe & Artificial Intelligence](#) del Consiglio d'Europa emerge che l'obiettivo principale del suo **Steering Committee for Human Rights** è quello di garantire che le attività di definizione degli standard dell'IA siano compatibili con le norme sui diritti umani stabilite dalla Convenzione europea dei diritti dell'uomo, così come interpretate dalla Corte europea dei diritti dell'uomo. Il Comitato è incaricato di preparare un manuale sull'intelligenza artificiale e i diritti umani entro il 2024.

### **Le attività in corso presso la Camera dei deputati**

Mercoledì 19 Aprile 2023 la I Commissione (Affari costituzionali) della Camera dei deputati ha svolto l'[audizione](#) del sottosegretario alla Presidenza del Consiglio con delega all'innovazione tecnologica e alla transizione digitale, Alessio Butti, sulle **linee programmatiche** dell'attività di Governo in materia di **digitalizzazione della pubblica amministrazione**.

Mercoledì 29 novembre 2023 il sottosegretario Butti è stato [auditato](#) dalle Commissioni riunite I (Affari costituzionali) e IX (Trasporti, poste e telecomunicazioni) della Camera dei deputati sullo **stato di attuazione delle misure relative alla transizione digitale nell'ambito del PNRR**.

## **Accordo tra Camera e Agenzia per la Cybersicurezza Nazionale sulla protezione dalle minacce informatiche**

La Camera dei deputati e l'Agenzia per la Cybersicurezza Nazionale hanno sottoscritto un protocollo d'intesa in materia di sicurezza informatica. La collaborazione si inserisce in un contesto globale in cui la minaccia cyber si è fatta sempre più forte e in cui la collaborazione e il confronto sulle strategie di rafforzamento diventano cruciali anche in considerazione del percorso di trasformazione digitale avviato dalla Camera nello svolgimento della sua funzione istituzionale. In questo scenario, lo scambio di informazioni per il potenziamento dei servizi di gestione e contenimento delle minacce cibernetiche, la realizzazione di sinergie attraverso la definizione di buone pratiche e l'aggiornamento e la formazione del personale rivestono una straordinaria importanza. L'accordo permetterà di avviare un qualificato confronto a tutela dell'Istituzione e nell'interesse generale del Paese.

### **La disciplina vigente in materia di sicurezza cibernetica**

La materia della sicurezza cibernetica è regolata a livello di Unione europea dalla c.d. direttiva NIS (*Network and Information Security*, direttiva (UE) 2016/1148) che reca misure per conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea<sup>5</sup>.

La direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 2018, che costituisce la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS.

---

<sup>5</sup> Obiettivo della direttiva era quello di definire un'unica linea strategica tra i vari Stati membri per fronteggiare il rischio di incidenti ai danni delle reti informatiche e dei sistemi informativi, assicurando che i medesimi fossero adeguatamente preparati a rispondervi attraverso: - la designazione di autorità competenti in materia di sicurezza delle reti e dei sistemi informativi; - la creazione di gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT); l'adozione di strategie nazionali per la sicurezza della rete e dei sistemi informativi.

Oltre a prevedere una collaborazione a livello dell'Unione europea sia sul piano strategico che su quello tecnico, la direttiva NIS introduceva, a carico degli operatori di servizi essenziali e dei fornitori di servizi digitali, l'obbligo di adottare le misure di sicurezza appropriate e di segnalare all'autorità nazionale competente il verificarsi di incidenti gravi.

Successivamente, al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è stato adottato il decreto-legge n. 105 del 2019 con il quale è stato istituito un perimetro di sicurezza nazionale cibernetica e sono state introdotte misure volte a garantire i necessari *standard* di sicurezza rivolti a minimizzare i rischi.

Dando seguito all'art. 1, comma 2, lettera b), del citato decreto-legge, è stato adottato il Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici ([DPCM n. 81 del 2021](#)).

In base a quanto disposto dall'art. 3 del DPCM, i soggetti pubblici e privati che abbiano ricevuto la comunicazione di inclusione all'interno del perimetro provvedono a notificare al CSIRT italiano le tipologie di incidenti previste nell'allegato A del medesimo DPCM che impattino sui beni ICT di propria pertinenza. Tale obbligo di notifica è esteso, dal comma 3 del medesimo articolo, anche agli incidenti che impattino su beni "contigui" a quelli ICT.

La notifica deve essere effettuata entro sei ore, qualora si tratti di un incidente individuato nella tabella 1 dell'allegato A (meno grave), ed entro un'ora, qualora si tratti di un incidente individuato nella tabella 2 del medesimo allegato (più grave). Tali termini decorrono dal momento in cui i soggetti inclusi nel perimetro sono venuti a conoscenza di un incidente riconducibile a una delle tipologie individuate nell'allegato A.

A fronte dell'esigenza di garantire la conoscenza delle informazioni relative agli incidenti anche laddove questi non colpiscano i beni ICT o quelli ad essi contigui, nell'art. 1 del decreto-legge n. 105 del 2019 è stato inserito il nuovo comma 3-bis<sup>6</sup>, il quale per l'appunto stabilisce che l'obbligo di notifica di cui si è detto sorga anche in presenza di incidenti aventi un impatto sulle reti, sui sistemi informativi e sui servizi informatici di pertinenza del soggetto "diversi" dai beni ICT. In questi casi la notifica deve essere effettuata entro il termine di 72 ore.

La [determina](#) del 3 gennaio 2023 del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale riporta la tassonomia degli incidenti informatici relativi

---

<sup>6</sup> Decreto-legge n.115 del 2022, art. 37-quater, comma 1.

alla cybersicurezza che hanno un impatto su reti, sistemi informativi e servizi informatici attinenti ai soggetti che sono tenuti alla notifica ai sensi dell'art. 1, comma 3-bis, del decreto-legge n. 105 del 2019.

Con il decreto-legge n. 82 del 2021 si è proceduto, poi, a definire l'architettura nazionale di cybersicurezza e ad istituire l'Agenzia per la cybersicurezza nazionale<sup>7</sup>, in attuazione di precisi obiettivi del Piano nazionale di ripresa e resilienza (PNRR) che, in considerazione dell'accresciuta esposizione alle minacce cibernetiche ad oggi riscontrabile, individua la sicurezza cibernetica come uno dei principali interventi da realizzare nell'ambito della trasformazione digitale della p.a. e della digitalizzazione del Paese<sup>8</sup>.

La normativa europea è stata aggiornata dalla c.d. direttiva NIS 2 (direttiva (UE) 2022/2555), che ha sostituito il quadro di riferimento in materia al fine di tener

---

<sup>7</sup> Il sistema di *governance* del sistema nazionale di sicurezza cibernetica definito dal decreto-legge n. 82 del 2021 ha al suo vertice il Presidente del Consiglio dei ministri, a cui è attribuita l'alta direzione e la responsabilità generale delle politiche di cybersicurezza e al quale spetta l'adozione della relativa strategia nazionale nonché la nomina dei vertici della nuova Agenzia per la cybersicurezza nazionale. Presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

L'Agenzia per la cybersicurezza nazionale (ACN) è istituita a tutela degli interessi nazionali nel campo della cybersicurezza. Essa è qualificata come Autorità nazionale per la cybersicurezza e, in quanto tale, tra l'altro: assicura il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale; promuove la realizzazione di azioni comuni dirette a garantire la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore; predisporre la strategia nazionale di cybersicurezza; è Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto; è Autorità nazionale di certificazione della cybersicurezza e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni.

<sup>8</sup> Nell'ambito del PNRR la Cybersecurity è uno dei 7 investimenti della Digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo". All'investimento, volto alla creazione e al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese a partire dall'attuazione della disciplina prevista dal perimetro di sicurezza nazionale cibernetica, sono destinati circa 620 milioni di euro, di cui 241 per la creazione di una infrastruttura per la cybersicurezza; 231 per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica PNSC; 15 per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'Interno, Difesa, Guardia di Finanza, Giustizia e Consiglio di Stato.

conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza.

L'aggiornamento della direttiva mira inoltre ad eliminare le ampie divergenze riscontrabili tra gli Stati membri, i quali hanno attuato gli obblighi stabiliti dalla direttiva NIS in materia di sicurezza e segnalazione degli incidenti, nonché di vigilanza ed esecuzione, in modi significativamente diversi, con un effetto potenzialmente pregiudizievole sul funzionamento del mercato interno. La delega per la trasposizione della direttiva NIS 2 nel diritto interno è contenuta nel disegno di legge di delegazione europea 2022-2023, attualmente all'esame delle Camere (A.C. 1342).

Abrogando la NIS 1, direttiva NIS 2 si propone, dunque, di eliminare le divergenze esistenti tra gli ordinamenti degli Stati membri, rafforzando gli obblighi di cybersecurity, ampliando il numero di settori e di soggetti coinvolti e potenziando la cooperazione tra le autorità competenti di ciascuno Stato al fine di raggiungere una maggiore uniformità di applicazione. Nel perseguimento di tali obiettivi, la direttiva NIS 2:

- pone in capo agli Stati membri l'obbligo di adottare strategie nazionali in materia di cybersicurezza, di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza e team di risposta agli incidenti di sicurezza informatica (CSIRT);
- stabilisce misure in materia di gestione dei rischi di cybersicurezza e obblighi di segnalazione per i soggetti operanti nei settori ad alta criticità e nei settori critici di cui agli allegati I e II, nonché per soggetti identificati come critici dalla direttiva (UE) 2022/2557 (Direttiva CER- *Resilience of Critical Entities*);
- introduce norme e obblighi in materia di condivisione delle informazioni sulla cybersicurezza tra le varie autorità europee;
- prevede in capo agli Stati membri obblighi di vigilanza ed esecuzione a cui sottoporre gli operatori destinatari della direttiva.

Per quanto riguarda le principali novità introdotte dalla direttiva NIS 2, essa, come si è anticipato, anzitutto amplia il novero dei settori di applicazione della normativa<sup>9</sup>, nonché quello dei soggetti destinatari della medesima.

---

<sup>9</sup> La direttiva NIS 1 si applicava ai seguenti settori: acqua potabile; energia; infrastrutture digitali; infrastrutture del mercato bancario e finanziario; salute; trasporti. I settori a cui si applica la NIS 2 si dividono in **settori ad alta criticità** (energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestori di servizi Tlc *business-to-business*, **pubblica amministrazione** e settore spazio) e **altri settori critici** (servizi postali e di corriere; gestione dei rifiuti; prodotti chimici; alimenti; fabbricazione di dispositivi medici, computer ed elettronica, macchine e attrezzature, veicoli a motore, rimorchi e

Mentre, ai sensi della previgente direttiva NIS, la responsabilità di determinare quali soggetti soddisfacessero i criteri per essere considerati operatori di servizi essenziali spettava agli Stati membri, la nuova direttiva NIS 2 introduce, invece, la regola della soglia di dimensione, in virtù della quale tutti i soggetti di medie e grandi dimensioni che operano nei settori o forniscono i servizi contemplati dalla direttiva medesima rientrano nel suo ambito di applicazione<sup>10</sup>.

Ad alcuni soggetti – come, tra l’altro, quelli ritenuti critici per i settori citati, i fornitori di reti di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, quelli che forniscono servizi di registrazione dei nomi di dominio, nonché le pubbliche amministrazioni centrali e regionali<sup>11</sup> – la NIS 2 si applica indipendentemente dalla loro dimensione<sup>12</sup>.

Come si accennava, la direttiva NIS 2 essenzialmente rafforza gli obblighi già previsti dalla NIS 1.

Anzitutto, adottando un approccio “multirischio”, la direttiva stabilisce che gli Stati membri provvedano affinché i soggetti essenziali e importanti individuati adottino misure di sicurezza tecniche, operative ed organizzative adeguate e proporzionate: per gestire i rischi per la sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi; nonché per prevenire o ridurre al minimo l’impatto degli incidenti sui destinatari

---

semirimorchi e altre attrezzature di trasporto; fornitori digitali - mercati online, motori di ricerca online e piattaforme di servizi di social networking – e organizzazioni di ricerca).

La direttiva NIS 2 supera, dunque, la distinzione dei soggetti interessati – operata dalla direttiva NIS 1 – in “operatori di servizi essenziali” (OES) e “fornitori di servizi digitali” (FSD), lasciando spazio alle nuove categorie dei “**soggetti essenziali**” e dei “**soggetti importanti**”. Si segnala che, a differenza di quanto previsto dalla precedente normativa, nella prima categoria rientrano anche le pubbliche amministrazioni. Entro il 17 aprile 2025 gli Stati membri dovranno definire un elenco dei soggetti essenziali e importanti, da riesaminare ed eventualmente aggiornare almeno ogni due anni.

<sup>10</sup> Vengono pertanto escluse dall’ambito di applicazione della direttiva – con residuali eccezioni connesse alla criticità dei servizi forniti – solamente le piccole imprese e le microimprese. In ogni caso, data l’intensificazione e la crescente sofisticazione delle minacce informatiche, gli Stati membri dovranno adoperarsi per garantire che anche i soggetti esclusi dall’ambito di applicazione della NIS 2 raggiungano un livello elevato di cybersicurezza (considerando n. 13).

<sup>11</sup> Stando alla definizione riportata all’articolo 6, n. 35), della direttiva, per «**ente della pubblica amministrazione**» si intende un soggetto riconosciuto come tale in uno Stato membro conformemente al diritto nazionale, **che non comprende** la magistratura, **i parlamenti** e le banche centrali, e che soddisfa determinati criteri, illustrati dalla medesima disposizione.

<sup>12</sup> Gli Stati membri possono prevedere che la direttiva si applichi altresì ad enti della pubblica amministrazione di livello locale e ad istituti di istruzione, in particolare ove svolgano attività di ricerca critiche. Dall’applicazione del nuovo regime sono **esclusi**, invece, gli enti della pubblica amministrazione che svolgono le loro attività nei settori della **sicurezza nazionale**, della **pubblica sicurezza** o della **difesa**, del **contrasto**, comprese la prevenzione, le indagini, l’accertamento e il perseguimento dei **reati**.

dei loro servizi e su altri servizi (art. 21). Le misure minime da implementare sono stabilite dalla medesima disposizione<sup>13</sup>.

Essa, inoltre, rafforza gli obblighi di segnalazione e notifica di “incidenti significativi” alle autorità competenti e al CSIRT gravanti sugli operatori di servizi essenziali o importanti, prevedendo una procedura articolata in più fasi con tempistiche predefinite (art. 23)<sup>14</sup>.

Gli Stati membri devono provvedere affinché le sanzioni amministrative pecuniarie imposte ai soggetti essenziali e importanti in relazione alle violazioni della direttiva siano effettive, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso. Laddove ad essere violati siano gli obblighi di cui agli artt. 21 e 23, gli Stati membri provvedono affinché: i soggetti essenziali siano soggetti a sanzioni pecuniarie amministrative pari a un massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore; i soggetti importanti siano soggetti, a sanzioni pecuniarie amministrative pari a un massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

---

<sup>13</sup> I vari operatori dovranno, pertanto, tracciare il perimetro di riferimento relativo ai sistemi informatici effettivamente utilizzati ed individuare, per l'appunto secondo un approccio multirischio, le misure idonee a proteggere tali sistemi da incidenti, verificando anche, mediante un *assessment*, quale sia la loro effettiva capacità di risposta e reazione alle minacce.

<sup>14</sup> Secondo quanto disposto dall'art. 23, i detti operatori dovranno notificare al CSIRT o, se opportuno, alla propria autorità competente:

- senza indebito ritardo, e comunque **entro 24 ore** da quando sono venuti a conoscenza dell'incidente significativo, un **preallarme** che, se opportuno, indichi se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

- senza indebito ritardo, e comunque **entro 72 ore** da quando sono venuti a conoscenza dell'incidente significativo, una **notifica** dell'incidente che, se opportuno, aggiorni le informazioni date con il preallarme e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

- su richiesta di un CSIRT o, se opportuno, di un'autorità competente, una **relazione intermedia** sui pertinenti aggiornamenti della situazione;

- una **relazione finale** entro un mese dalla trasmissione della notifica dell'incidente.

In caso di incidente in corso al momento della trasmissione della relazione finale, gli Stati membri provvedono affinché i soggetti interessati forniscano una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente.

Al fine di colmare le differenze riscontrabili tra gli Stati membri in tema di *reporting* sugli incidenti e successive azioni di rafforzamento, la direttiva NIS 2 prevede, poi, l'istituzione di una rete europea delle organizzazioni di collegamento per le crisi informatiche (CyCLONe, *Cyber Crisis Liaison Organisation Network*), chiamata a supportare la gestione coordinata degli incidenti di sicurezza informatica su vasta scala.



## **FOCUS: L'EXECUTIVE ORDER DEL PRESIDENTE BIDEN IN MATERIA DI AI**

### **Premessa**

In data 30 ottobre 2023, il Presidente degli Stati Uniti ha emanato un *Executive Order* (il n. 14110) sulla [\*Safe, Secure, and Trustworthy Artificial Intelligence\*](#) (decreto per un'intelligenza artificiale sicura e affidabile).

L'*Executive order* è provvedimento normativo che ha un effetto vincolante sulle amministrazioni pubbliche ma per i terzi ha efficacia più limitata, tanto – come peraltro è specificato in coda al testo – non attribuisce diritti o pretese ad alcuno; nel nostro ordinamento ha i tratti, in parte, del decreto-legge e, in parte, del d.P.C.M.

L'*Executive order* 14110 si presenta lungo e articolato: è un testo che si pone come primo e organico **atto di regolazione** del fenomeno dell'**intelligenza artificiale** (d'ora innanzi anche **IA**) negli Stati Uniti. Esso ha però anche il dichiarato scopo di collocare gli USA nel ruolo guida sul piano internazionale nel governo della materia.

Esso proclama anzitutto le sue **finalità**; indi contiene una nutrita serie di **definizioni**; e poi sviluppa una corposa serie **indirizzi** e **istruzioni** alle **strutture ministeriali** incaricate di portare avanti compiti coerenti con le finalità dichiarate, assegnando loro anche una griglia di scadenze temporali entro cui adottare i conseguenti atti. Da questo punto di vista, l'*Executive order* 14110 si atteggia, quindi, a **cronoprogramma** per la **creazione di un ambiente normativo e amministrativo** entro cui il progresso dell'intelligenza artificiale sia ben stimolato ma anche regolato.

Tutto il testo dell'*Executive order* è infatti ispirato dalla consapevolezza che l'intelligenza artificiale è un movimento in costante evoluzione, che offre enormi opportunità di benessere individuale e collettivo ma che comporta anche rischi e pericoli.

### **Le 8 finalità**

Anzitutto, il provvedimento del Presidente Biden dichiara le **finalità** che il sistema istituzionale statunitense nel suo complesso – e salvo comunque l'auspicio che il Congresso intervenga tempestivamente a dare maggiore compiutezza e forza normativa alla regolazione – deve conseguire. Esse sono:

- a) **la sicurezza.** Nell'originale inglese è usata l'endiadi “*safe and secure*”, vale a dire la sicurezza intesa sia come **intrinseca inidoneità a nuocere**, sia come protezione da **usi malevoli e dannosi** da parte di una persona contro un'altra. L'obiettivo della sicurezza è raggiungibile attraverso un fitto reticolo di iniziative e azioni pubbliche e private che di fatto erigano un sistema di controlli robusti, affidabili, reiterati e con *standard* omogenei;
- b) **l'innovazione responsabile.** L'Amministrazione federale americana si propone di predisporre un ambiente socio-economico e normativo in cui vi sia **apertura di mercato, concorrenza, formazione** e addestramento sul piano tecnologico e promozione della ricerca;
- c) **la promozione e la protezione del lavoro negli Stati Uniti.** L'Amministrazione federale si propone di far **partecipare i lavoratori americani** (e con essi i sindacati, gli insegnanti e i datori) ai processi di sviluppo e di governo dell'intelligenza artificiale. Essa avverte l'esigenza di proteggere responsabilmente i lavoratori da un peggioramento delle condizioni sul posto di lavoro ed economiche.

Da questo punto di vista, appare chiara l'eco dello [sciopero dei lavoratori dello spettacolo](#) in California, prolungatosi per circa 4 mesi nel 2023, alla base del quale erano anche rivendicazioni inerenti ai pericoli posti dall'IA per le attività a contenuto creativo, imitativo e riproduttivo nell'industria cinematografica;

- d) **la tutela dell'uguaglianza e dei diritti umani.** Il provvedimento premette che l'uso non regolato dell'IA ha già mostrato di poter approfondire le diseguaglianze e le discriminazioni. Viceversa, ci si propone di emanare uno statuto dell'IA (*AI Bill of Rights*) che affianchi altre politiche pubbliche volte alla rimozione delle cause della sperequazione economica, sociale e razziale;
- e) **la protezione dell'uso quotidiano dell'IA.** Preso atto che vi sono settori nei quali l'impiego dell'IA è già avanzato (sanità, servizi finanziari, istruzione, politiche per la casa, trasporti e amministrazione della giustizia), l'*Executive order* si prefigge l'obiettivo di proteggere **utenti, pazienti e consumatori** che giornalmente vengono a contatto con meccanismi produttivi e commerciali gestiti (anche) dall'IA;

- f)* **la protezione dei dati personali.** Le potenzialità dell'IA sono enormi sotto il profilo dell'estrazione, dell'elaborazione e del collegamento dei dati (disponibili in rete o nelle banche-dati). Si tratta spesso di dati sensibili, che delle persone rivelano identità, ubicazione, abitudini e desideri. Ne deriva il rischio di improprio sfruttamento ed esposizione pubblica dei dati (compresi quelli attinenti alle opinioni politiche), per combattere i quali il governo federale si propone di adoperare tutti gli strumenti di legge per **difendere la *privacy* individuale;**
- g)* **il reclutamento nelle agenzie federali di personale qualificato.** Il perseguimento delle finalità sinora esposte ne implica un'ulteriore, relativa a chi possa farsi carico delle azioni che materialmente siano tese a conseguirle. Il governo federale degli Usa pertanto si propone una **campagna di assunzioni di figure professionali attrezzate** a comprendere i rischi dell'IA e a orientarne l'uso per risultati positivi per il popolo americano;
- h)* **l'assunzione di un ruolo guida nel mondo.** L'Amministrazione Biden si propone – con l'emanazione e l'attuazione dell'*Executive order* n. 14110 – di rendere gli USA come l'attore che, sulla scena mondiale, si pone come apri-pista e punto di riferimento nel governo dell'IA. Sotto questo aspetto, essa si prefigge di cooperare con i Paesi alleati nell'elaborazione di una strategia condivisa e globale volta ad assicurare che i rischi dell'IA siano minimizzati e che invece siano sviluppati e diffusi gli usi tesi al miglioramento della qualità della vita.

### **Le definizioni**

L'*Executive order* detta poi, in via preliminare, **33 definizioni** normative, alcune nuove, altre già presenti nella legislazione statunitense, cui rinvia.

La definizione di **intelligenza artificiale (AI)** è ripresa dallo United States Code (15 USC 9401(3): un **sistema basato su macchine** (*id est*: automatico) che può – per una serie prestabilita di scopi dettati dall'uomo – **fare previsioni, dare consigli e assumere decisioni** che **influenzano l'ambiente reale o virtuale** circostante. I sistemi di IA adoperano stimoli umani o automatizzati per calarsi in un ambiente reale o virtuale, ne sintetizzano le caratteristiche in modelli astratti in base ai quali poi formulano interazioni informative con l'esterno o prendono decisioni.

Sicché, per **modello di IA** l'*Executive order* n. 14110 intende quella componente di un sistema informatico che alimenta una tecnologia di IA e

usa tecniche computazionali, statistiche e di apprendimento meccanico per fornire un prodotto (*output*) da una serie prestabilita di stimoli (*inputs*).

Tra le nuove definizioni, v'è anche quella di “**AI red-teaming**”, vale a dire la **formazione di “squadre rosse”** formate da figure professionali esperte nel simulare le condotte avversarie (vale a dire quelle dei potenziali soggetti malintenzionati, i quali possono attaccare un sistema di IA “sana”, impossessarsi dei dati e manipolarne gli *outputs*) e prevenirle e combatterle.

Per **sistema di IA** s'intende quindi un sistema di dati, un *software*, un *hardware*, un'applicazione, uno strumento o un'utilità che lavora con l'IA, in tutto o in parte.

Altra definizione di rilievo è quella di “**dual-use foundation model**”. Per esso s'intende quel modello di IA particolarmente potente, il quale è addestrato su **masse enormi** di dati (almeno **10 miliardi**) ed è pertanto applicabile a un'**ampia gamma di contesti** e ha una **resa molto efficace**. Esso è generalmente dotato di meccanismi di autocontrollo ma ciò non esclude i **fattori di alto rischio** cui esso espone. I pericoli del modello *dual-use* elencati al riguardo dalla definizione dell'*Executive order* sono:

- i) l'**abbassamento della soglia di accesso**, da parte di non addetti, alle armi biologiche, chimiche, radiologiche e nucleari;
- ii) l'**esposizione ai cyber-attacchi** attraverso la scoperta delle **vulnerabilità** del sistema oggetto di attacco;
- iii) l'**elusione del controllo umano**.

L'*Executive order* precisa che si definiscono *dual-use* anche quei modelli che dotano l'utente di mezzi tecnici appositamente immaginati per ridurre i predetti rischi.

Esso poi contiene una serie di definizioni, che presuppongono anche nozioni matematiche di frequente uso nell'IA, quali, tra le altre:

- IA generativa;
- operazione con integrali;
- *machine learning*;
- *model weight* (peso del modello);
- *omics* (biomolecole).

In chiusura, la lista di definizioni reca sia **testbed** (vale a dire il meccanismo costruito per collaudare e verificare la tenuta, la funzionalità e

l'efficacia di un sistema di IA) sia **watermarking** (cioè la condotta di marcare il prodotto di IA con un segno difficilmente cancellabile, che consenta di tracciarlo e di riconoscerne la genuinità).

### **Il cronoprogramma di attuazione delle singole politiche**

Le 8 finalità testé illustrate si dovranno tradurre nello svolgimento di **precise politiche pubbliche**, da attuarsi mediante **azioni** – spesso coordinate e intrecciate tra loro – cui sono preposti **diversi dipartimenti governativi** e secondo **cadenze temporali** prefissate.

In estrema sintesi:

- la finalità della **sicurezza** è affidata **Ministro del commercio**, il quale si avvale *National Institute of Standards and Technology* (NIST). Il Ministro del commercio e il NIST hanno il compito di emanare – entro **270 giorni** dal 30 ottobre 2023 - **Linee guida** e di indentificare **buone pratiche** per la sicurezza dei sistemi di IA (tra queste l'uso del *watermarking*) e del relativo impiego.

Il Ministro del commercio è incaricato anche – entro **90 giorni** dall'entrata in vigore dell'*Executive order* – di domandare alle **imprese** che sviluppano sistemi *dual-use* di **notificarli inizio, fasi di avanzamento e cautele** adottate in tale attività (compresa l'eventuale istituzione di *red-teams*), nonché gli **assetti proprietari** e la **titolarità** sui quei sistemi (in pratica, al Ministro del commercio è autorizzato a esercitare tutti i poteri che la legge gli conferisce per acquisire notizie sulla circolazione dei diritti di proprietà materiale e intellettuale sui sistemi di IA). Entro **180 giorni** dall'entrata in vigore dell'*Executive order*, il Ministro del commercio deve anche proporre l'adozione di regole al riguardo. Azioni e scadenze sono anche previste a tutela delle **infrastrutture critiche** degli USA, specialmente contro gli attacchi cybernetici.

È coinvolto, inoltre, il **Ministro per l'energia**, al quale spettano compiti di verifica dell'impatto dell'uso dell'IA sui settori della sicurezza energetica;

- la finalità dell'**innovazione responsabile** è affidata ai **Ministri degli Esteri e dell'Interno** (Segretario di Stato e *Secretary of Homeland Security*).

In questo contesto, al **Segretario di Stato** sono assegnati **tre** termini:

- uno di **90 giorni** per dare apposite istruzioni onde **accelerare** le procedure d'esame delle **domande di ingresso** negli Stati Uniti per **motivi di lavoro** nel campo dell'**IA**;
- uno di **120 giorni** per riscrivere le regole dei programmi di **scambio culturale e professionale** con i Paesi terzi;
- uno di **180 giorni** ampliare la platea di beneficiari dei permessi d'ingresso rivolti ai ricercatori e ai docenti di scienze dure (scienze naturali, tecnologia, matematica e ingegneria).

Al **Ministro dell'interno**, a sua volta, sono dati **180 giorni** per rivedere le regole sull'esame delle **domande di soggiorno**.

È coinvolto, inoltre, il **Ministro del lavoro**, al quale è assegnato il compito di stilare una nuova lista di **figure professionali** legate allo **sviluppo tecnologico** e dell'**IA** di cui negli Stati Uniti v'è **carezza**.

Sono inoltre assegnati funzioni e termini a vari altri soggetti istituzionali per il **potenziamento** della **ricerca**, delle **università**, delle **procedure di brevetto** e della **concorrenza**;

- la finalità della **tutela dei lavoratori americani** è affidata al **Capo dei consiglieri economici** del Presidente degli USA e al **Ministro del lavoro**. Quest'ultimo entro **180 giorni** dall'entrata in vigore pubblica un documento in cui siano riportati principi e buone pratiche cui i datori dovrebbero ispirarsi per garantire che l'uso dell'**IA** assicuri livelli elevati di qualità sui luoghi di lavoro;
- la finalità relativa all'**uguaglianza** e ai **diritti umani** è affidata al **Ministro della giustizia** (*Attorney general*). Questi – entro **90 giorni** dall'entrata in vigore – è tenuto a dare istruzioni al sottosegretario con delega ai diritti umani di promuovere un **convegno generale** con tutti i funzionari federali incaricati della tutela dei diritti per identificare i fenomeni di discriminazione algoritmica e i mezzi per combatterla; inoltre, entro **un anno** dall'entrata in vigore, l'*Attorney general* dovrà predisporre una **relazione al Presidente degli USA** in cui siano offerti dati precisi sull'uso di **sistemi di IA** nei seguenti ambiti:
  - quantificazione delle pene;
  - misure alternative alla detenzione;
  - cauzioni e misure cautelari;

- valutazione dei rischi nella concessione dei benefici penitenziari;
- sorveglianza speciale;
- prognosi criminologiche e attività di polizia predittiva;
- gestione delle carceri;
- medicina legale;
- la finalità della **protezione di utenti, pazienti e consumatori** è deferita ai **Ministeri della difesa, della sanità e dei trasporti** e a diverse *Authorities*. L'*Executive order* prevede compiti e scadenza a tutela dei veterani di guerra, degli utenti dei servizi sanitari pubblici e privati, dei consumatori e di quanti acquistano valori mobiliari;
- la finalità della **protezione dei dati personali** è affidata al **Direttore dell'Ufficio per il bilancio** del Presidente degli stati Uniti (*Director of the OMB*). Questi ha l'onere di coordinare iniziative concrete per verificare l'efficacia delle misure vigenti al riguardo, nei confronti dei sistemi di IA e per potenziare la ricerca sulla tutela della *privacy*;
- la finalità della **gestione e dell'uso dell'IA nell'Amministrazione federale** è affidata – anch'essa - al **Direttore dell'Ufficio per il bilancio** del Presidente degli stati Uniti (*Director of the OMB*). Anche in questo caso gli sono assegnati compiti e scadenze volte al coordinare e uniformare l'impiego dell'IA nei dipartimenti federali, anche attraverso la nomina di un *Chief AI Officer*, responsabile del concreto uso e della diffusione dei sistemi di IA nei pubblici uffici, con particolare riferimento alla promozione dell'uso dell'IA generativa e agli strumenti di gestione dei rischi da essa derivante. Specifiche scadenze sono anche stabilite per il **reclutamento di personale qualificato**;
- La finalità inerente alla **proiezione globale degli USA** in tema di governo dell'IA è affidata al **Segretario di Stato**. Questi è incaricato di promuovere a livello internazionale la costituzione di sedi specifiche per scambi di conoscenze, azioni coordinate, cooperazione e accordi per adottare *standard* tecnici comuni. A tale ultimo fine, gli sono assegnati **270 giorni** per promuovere:
  - l'adozione di una terminologia comune;
  - la descrizione di buone pratiche;

- sistemi di verifica e controllo dell'affidabilità dell'IA;
- strumenti di gestione del rischio.

In chiusura, l'*Executive order* istituisce il ***White House AI Council*** (vale a dire il Consiglio presidenziale per l'IA) con compiti di coordinamento generale del governo del fenomeno e di consiglio al Presidente. Ne fanno parte i ministri citati, unitamente ad altri membri del governo e ad altri alti ufficiali federali.

## **FOCUS: INTELLIGENZA ARTIFICIALE E ANALISI DEL RISCHIO FISCALE**

In Italia, in materia fiscale, l'intelligenza artificiale sta trovando una sua specifica applicazione nelle attività relative alle verifiche fiscali, in particolare favorendo l'elaborazione e il trattamento di *big data* negli ambiti **dell'analisi del rischio e del contrasto alle frodi**, con riguardo all'individuazione di **criteri di rischio, deterministici e probabilistici** da utilizzare per la predisposizione di liste selettive di controllo e di elenchi destinati all'alimentazione del processo di stimolo della *compliance*.

Nel proprio [Documento illustrativo della logica degli algoritmi](#), l'Agenzia delle entrate sottolinea l'importanza dell'utilizzo dell'IA in un'analisi probabilistica basata sull'insieme dei modelli e delle tecniche di analisi che, sfruttando soluzioni di intelligenza artificiale ovvero di statistica inferenziale, consentano di **isolare rischi fiscali, anche non noti a priori**, che, una volta individuati, possano essere utilizzati per l'elaborazione di autonomi criteri selettivi, ovvero **permettano di attribuire una determinata probabilità di accadimento ad un rischio fiscale noto** (definizione ripresa anche all'articolo 2, comma 1, lettera *f*) dello schema di decreto legislativo in materia di procedimento accertativo A.G.105).

A tale proposito, il comma 682 della legge di bilancio 2020 (legge 27 dicembre 2019, n. 160) ha disposto che l'Agenzia delle entrate, per le summenzionate analisi del rischio, possa avvalersi, anche previa pseudonimizzazione dei dati personali, delle tecnologie, delle elaborazioni e delle interconnessioni con le altre banche dati di cui dispone, allo scopo di individuare i criteri di rischio utili a **far emergere le posizioni da sottoporre a controllo o nei cui confronti avviare attività di stimolo dell'adempimento spontaneo**.

In Francia, nel medesimo periodo, e con analogo strumento normativo (loi de finances pour 2020, n. 2019-1479 del 28 dicembre 2019), le amministrazioni finanziarie sono state autorizzate a raccogliere ed elaborare, in via automatizzata, anche le informazioni pubblicate dagli utenti sui propri *social network*, riconoscendo così alle amministrazioni fiscali e doganali la possibilità di utilizzare i dati resi pubblici sui *social network* per indagini sul rischio di violazioni fiscali e doganali. In pratica, le informazioni diffuse

pubblicamente dagli utenti stessi (con l'esclusione delle conversazioni private e in generale di tutto ciò che è accessibile dopo aver inserito una *password*) confluiranno in una banca dati dove saranno raccolte in modo aggregato e automatizzato, per essere poi utilizzate nella stesura delle analisi di rischio (per una più ampia lettura della misura si rinvia all'articolo dell'Agenzia delle entrate: [Francia, dai social media nuovi strumenti anti evasione](#)).

In tale ottica, l'Agenzia delle entrate, al fine di valorizzare al meglio il vasto patrimonio di dati di cui dispone (per ogni singola annualità, 42 milioni di dichiarazioni, 750 milioni di informazioni comunicate da soggetti terzi, 400 milioni di rapporti finanziari attivi, 197 milioni di versamenti F24, circa 2 miliardi di fatture elettroniche e oltre 150 milioni di immobili censiti) ha ottenuto anche [il via libera dell'Unione europea](#) al finanziamento del progetto *A data driven approach to tax evasion risk analysis in Italy* ideato e presentato dall'Agenzia stessa con la finalità di innovare i processi di valutazione del rischio di *non-compliance*. In pratica, con tale progetto si cerca di **attuare nuovi approcci e strumenti di analisi del rischio basati sui dati per individuare la frode e l'evasione fiscale**. Attraverso soluzioni tecnologiche all'avanguardia come l'intelligenza artificiale e le tecniche di apprendimento automatico *machine learning*, l'Agenzia mira pertanto a rafforzare la conformità volontaria, ridurre l'economia sommersa e migliorare la sostenibilità delle finanze pubbliche.

Nel corso [dell'audizione in merito ai Progetti di digitalizzazione e innovazione tecnologica del settore fiscale](#), svoltasi presso la VI Commissione Finanze e tesoro del Senato, il direttore dell'Agenzia delle entrate rappresentava che l'Agenzia è impegnata a realizzare una complessiva strategia di **sviluppo di tecniche di analisi sui cosiddetti big data, finalizzata a superare i tradizionali controlli basati sugli incroci** volta a promuovere approcci innovativi e diversificati. Inoltre, considerata la valenza strategica che, per l'Agenzia delle entrate, rivestono l'innovazione tecnologica e l'ampliamento delle attuali conoscenze nell'ambito della disciplina dell'analisi dei dati, gli investimenti in questo campo favorirebbero un significativo incremento di efficienza ed efficacia dei processi di contrasto all'evasione e della promozione della *tax compliance*, oltre che una riduzione della spesa pubblica e una migliore offerta di servizi digitali ai cittadini. Gli

investimenti in infrastrutture tecnologiche e in *know-how* per un migliore utilizzo del patrimonio informativo dell'Amministrazione finanziaria potrebbero concentrarsi sulle seguenti due linee di intervento generali:

- investimenti infrastrutturali, finalizzati a rendere ancora più fruibile e tempestivo l'accesso e la gestione dei flussi delle informazioni di vaste basi di dati (ad esempio archivio dei rapporti finanziari, fatturazione elettronica e corrispettivi), per l'applicazione di tecniche di intelligenza artificiale, *machine learning*, *text mining*, ecc.; potenziamento delle dotazioni tecnologiche a disposizione delle strutture centrali e territoriali preposte all'attività di prevenzione e contrasto all'evasione, con ricadute positive sulla celerità nello scambio di informazioni tra strutture centrali, nonché sull'incremento delle capacità di analisi anche a livello locale;
- investimenti in *software* e in *know how*, nel campo delle nuove tecnologie di analisi di vaste basi di dati, con particolare riferimento allo sviluppo della *network analysis*, con conseguente aggiornamento dell'*hardware* a disposizione degli analisti.

Tale approccio è stato definito nella [Convenzione triennale per gli esercizi 2023-2025](#) tra MEF e le Agenzie fiscali dove si prevede che l'Agenzia monitorerà il comportamento dei contribuenti che hanno subito un controllo fiscale per **verificare nel tempo il loro grado di propensione all'adempimento e, più in generale, per valutare il livello di fedeltà fiscale**; si dovrà, inoltre, incrementare la capacità operativa nell'ottica di favorire il miglioramento della qualità dei controlli, attraverso nuovi strumenti e progetti di analisi avanzata dei dati, l'applicazione di tecniche come l'intelligenza artificiale, il *machine learning* e il *text mining*.

La tendenza al sempre maggiore utilizzo della IA nel contrasto all'evasione, ovviamente, non è un fenomeno esclusivamente italiano o europeo. L'Agenzia delle entrate, [nella sua rivista on line](#), segnala come negli Stati Uniti l'*Internal Revenue Service* (l'Agenzia federale delle entrate statunitense) ha dato il via all'utilizzo a regime dell'intelligenza artificiale per investigare sull'evasione fiscale delle società multimiliardarie, cosiddette *partnership*, sui contribuenti facoltosi e sui gruppi di investitori nei settori immobiliare e in quello dei fondi d'investimento. A tal fine l'IRS sta già utilizzando **una parte degli 80 miliardi di dollari stanziati, su base**

**decennale, con l'*Inflation Reduction Act* del 2022** per affrontare meccanismi di elusione fiscale divenuti troppo complessi da gestire con le ridotte risorse nella disponibilità dell'Irs. I nuovi fondi nella disponibilità dell'Irs hanno permesso la costruzione d'una nuova infrastruttura con al centro proprio l'intelligenza artificiale. Gli sforzi si concentreranno sulle grandi *partnership* complesse, che di fatto gestiscono e indirizzano miliardi d'investimenti in fondi obbligazionari e/o puramente azionari in ogni angolo del pianeta, e sui contribuenti ad alto reddito che spesso proprio su tali strumenti investono i loro patrimoni percependo in cambio ricchi dividendi e lucrose plusvalenze. In sostanza, l'Irs avvierà accertamenti sulle più grandi *partnership* statunitensi, tutte identificate con l'aiuto dell'intelligenza artificiale.

Si ricorda, altresì, il caso brasiliano dove viene utilizzato un sistema di intelligenza artificiale (basata sull'apprendimento automatico (*machine learning*)) chiamato the *Customs Selection System Through Machine Learning-SISAM*, in grado di calcolare la probabilità di irregolarità fiscali e, conseguentemente, di valutare l'opportunità di un controllo doganale. Più in particolare, si tratta di un'intelligenza artificiale che, dal 2014, analizza ogni dichiarazione di importazione registrata in Brasile e per ogni articolo in ciascuna dichiarazione di importazione calcola la probabilità di circa 30 tipi di errori aiutando così a ridurre la percentuale di merci verificate durante lo sdoganamento, l'evasione fiscale e l'inosservanza dei requisiti amministrativi. (Per un approfondimento del sistema SISAM si rinvia alla lettura del documento: [Artificial Intelligence Initiatives in the Special Secretariat of Federal Revenue of Brazil](#), per un approfondimento generale dell'utilizzo dell'apprendimento automatico nell'analisi frodi nel settore doganale si rinvia al documento della Commissione economica per l'Europa delle Nazioni Unite: [Machine Learning Approaches for Fraud Analytics in Customs](#)).

Come sopra ricordato, la legge di delega per la riforma fiscale, n. 111 del 2023, ha espressamente previsto nell'articolo 17, comma 1, lettere *c*) ed *f*), l'obiettivo di prevenire, contrastare e ridurre l'evasione e l'elusione fiscale **razionalizzando le disposizioni normative concernenti le attività di analisi del rischio** nonché potenziando l'utilizzo di tecnologie digitali, anche **con l'impiego di sistemi di intelligenza artificiale**, al fine di ottenere, attraverso la piena interoperabilità tra le banche di dati, la disponibilità delle informazioni rilevanti. Tale previsione è stata recepita al comma 2

dell'articolo 1 dello schema di decreto legislativo in materia di procedimento accertativo ([A.G.105](#)) dove sono indicate alcune definizioni finalizzate a perimetrare in maniera esaustiva il processo di analisi del rischio, chiarendo, in maniera esplicita, che lo stesso può basarsi anche sull'utilizzo di soluzioni di *machine learning* e intelligenza artificiale.

Il Governo osserva nella relazione illustrativa che tale possibilità, invero, pur essendo già prevista dal Regolamento *privacy* - in particolare nelle parti in cui si discorre di profilazione - non risultava ancora espressamente contemplata da una norma definitoria nazionale. Il Governo precisa inoltre che nel testo non vengano analiticamente descritte le varie soluzioni di intelligenza artificiale utilizzabili, poiché le stesse saranno perimetrare da un Regolamento unionale di prossima emanazione.

Sempre nella relazione illustrativa del sopra citato schema di decreto legislativo, si evidenzia, altresì, che il potenziamento dell'attività di analisi del rischio è stato ampiamente valorizzato anche nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR), che, a completamento delle azioni, prevede diverse riforme, intese quali misure destinate a concorrere alla realizzazione degli obiettivi, già indicati nelle *Country Specific Recommendations* rivolte all'Italia dall'Unione Europea, di equità sociale e miglioramento della competitività del sistema produttivo. Tra queste, quella denominata Riduzione del *tax gap*, prevede esplicitamente che «L'obiettivo del potenziamento dei controlli sarà realizzato attraverso selezioni più mirate dei contribuenti a maggiore rischio di evasione, rese possibili dall'applicazione di strumenti di *data analysis* più avanzati e dall'interoperabilità delle banche dati». Tra gli strumenti di *data analysis* vengono citate le «tecniche sempre più avanzate come intelligenza artificiale, *machine learning*, *text mining*, analisi delle relazioni».

In concreto, per il perseguimento degli obiettivi sopra descritti, l'Agenzia delle entrate, con la [direttiva 74424 del 2023](#), recante modifiche all'organizzazione e alle attribuzioni della Divisione contribuenti e della Direzione Centrale Piccole e Medie Imprese, ha istituito al suo interno l'Ufficio *data science* con i compiti di:

- realizzazione di processi informatici complessi di elaborazione e trattamento di *big data* negli ambiti dell'analisi del rischio e del contrasto alle frodi, finalizzati all'individuazione di criteri di rischio,

deterministici e probabilistici, da utilizzare per la predisposizione di liste selettive di controllo e di elenchi destinati all'alimentazione del processo di stimolo della *compliance*;

- supporto tecnico-informatico alle strutture centrali e regionali nelle attività di estrazione, modellizzazione ed elaborazione dei dati, anche per l'utilizzo delle piattaforme di analisi avanzata dei dati;
- sviluppo di metodologie di supporto alle **attività di controllo preventivo**, anche avvalendosi di tecniche di *machine learning* e **intelligenza artificiale**;
- **realizzazione di indicatori di rischio** basati su tecniche di *machine learning*, **intelligenza artificiale**, analisi di rete e *text mining* e loro implementazione negli applicativi di analisi;
- individuazione di soluzioni informatiche e metodologiche innovative per il trattamento dei dati provenienti dalla cooperazione internazionale;
- implementazione di tecniche di *text mining* finalizzate a consentire l'utilizzo dei "dati fattura integrati" nell'ambito dell'analisi del rischio.