Report sulle politiche a livello locale, nazionale ed internazionale

Deliverable 3.1



Versione 4/4/2024

Data di consegna prevista
29/2/2024

Data di consegna effettiva
29/2/2024

Data di inizio del progetto
1/9/2023

Work-package relativo al deliverable
WP3 (Supporto al policy-making)

Autori

Valerio Francola
Luca Megale
Gordon Mensah
Supervisione di Antonio Perrucci

Sommario

Sommario 2
Introduzione e scopo del documento 4
Executive Summary 5
Le iniziative dell'Unione europea 8
Una nuova stagione dell'intervento pubblico: politica industriale e regolazione 8
Le iniziative normative 9
Le iniziative di politica industriale 10
Infrastrutture abilitanti: supercalcolatori, reti e cloud 12
Supercalcolatori 12
Misure per la connettività e la diffusione dei servizi 13
A) Stato di approvazione 15
B) Panoramica sugli aggiornamenti/conferme di maggior rilievo 16
C) L'ufficio europeo per l'Intelligenza Artificiale 18
Focus: Cybersecurity e privacy alla luce del prossimo regolamento europeo sull'intelligenza artificiale 19
a) Cybersecurity 20
b) Privacy 22
c) Infrastrutture 22
Un "Brussels effect" per l'AI act? L'impatto sul (e rispetto al) mercato globale 23
Le iniziative dell'Italia 27
Le politiche per il digitale in Italia 27
Livello Nazionale 27
Livello locale 29
L'approccio italiano all'intelligenza artificiale 30
Iniziative del Governo 31
Iniziative del Parlamento e Autorità Amministrative Indipendenti 31
Il possibile impatto di un problema di governance 32
Misure nazionali in tema di cybersecurity 33
Linee di sviluppo della ricerca e alcune preliminari indicazioni 36
Allegato – Ricostruzione recenti documenti UE in materia di IA e strategie/tecnologie abilitanti 38

Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione 38
Trilogo 38
Commissione Europea 38
Consiglio dell'Unione Europea 38
Parlamento Europeo 39
Altre istituzioni 39
Politica industriale 40
Connettività 41
Dati 41
Cybersecurity 42
Media 43
Finanza 43
Protezione del consumatore e concorrenza 43

Introduzione e scopo del documento

Nell'era digitale in cui viviamo, le politiche a livello locale, nazionale ed internazionale svolgono un ruolo cruciale nel plasmare il futuro delle tecnologie e dei dati. Questo documento si propone di fornire una panoramica sulle politiche in materia di dati e tecnologie, concentrandosi sulle iniziative dell'Unione europea, dell'Italia e su alcuni sviluppi chiave a livello globale.

L'obiettivo principale di questo report è quello di analizzare le politiche pubbliche e le iniziative normative volte a regolare e promuovere l'adozione responsabile delle tecnologie emergenti, con particolare attenzione alle infrastrutture tecnologiche abilitanti, alla cybersecurity, alla privacy e alla politica industriale. Per farlo, sarà indispensabile riferirsi al nascente quadro normativo in materia di Intelligenza Artificiale che riguarda molto da vicino ogni aspetto legato al Supercalcolo.

Questo rapporto rappresenta il primo contributo di Astrid LED (https://www.astrid-online.it/) nell'ambito della collaborazione avviata con l'International Foundation Big Data and Artificial Intelligence for Human Development (IFAB) entro il progetto dell'Osservatorio ICSC, avente ad oggetto un approfondimento sulle politiche locali, nazionali ed europee sui temi del supercalcolo, dell'intelligenza artificiale, del *quantum computing* e – più in generale - della trasformazione digitale.

Questo deliverable è da considerarsi una ricognizione critica di partenza per quanto riguarda l'identificazione di traiettorie nell'ambito regolatorio a livello internazionale e nazionale. Ben consapevoli del fatto che le politiche e la regolamentazione non sono un punto di arrivo ma di partenza per la generazione di impatti sul futuro delle comunità, è obiettivo più ampio dell'Osservatorio riflettere sui potenziali, possibili e desiderabili impatti di queste policy sull'ecosistema della ricerca e dell'innovazione per il nostro sistema Italia.

Sulla base della ricognizione critica e delle traiettorie individuate in questo documento, verranno infatti impostati, in sinergia con altri work-package del progetto (si veda il piano di lavoro previsto nel WP1), gruppi di lavoro per la realizzazione di scenari possibili, anche al variare dell'interpretazione di tali normative su scala nazionale e sovranazionale, e verranno proposte misure per il monitoraggio dei loro impatti su varie dimensioni di attenzione.

Executive Summary

L'avvento e la progressiva affermazione delle tecnologie digitali, in particolare quelle legate al supercalcolo ai Big data ed all'intelligenza artificiale, stanno determinando ovunque profonde trasformazioni negli assetti dei mercati, oltre che nella società. Il processo di transizione digitale costituisce uno dei pilastri della definizione di una nuova più solida collocazione dell'Unione europea nella competizione internazionale.

In questo percorso, sicuramente, sono importanti le strategie di adattamento delle imprese, di ogni taglia dimensionale, come pure la nascita di start up e il sostegno del venture capital allo sviluppo di nuovi modelli di business che utilizzino le tecnologie digitali.

Tuttavia, l'impegno degli operatori privati è condizione necessaria, ma non sufficiente, per garantire che il sistema produttivo sia in grado di sfruttare appieno le opportunità offerte dalle nuove tecnologie digitali, nel rispetto – in ogni caso – di valori fondamentali, quali l'accessibilità di tutti (imprese, cittadini, pubblica amministrazione) ai nuovi beni e servizi digitali, la tutela della concorrenza, il diritto alla privacy ed alla corretta informazione, per citarne alcuni.

In altre parole, serve l'intervento pubblico, nelle sue diverse articolazioni: politica industriale, regolamentazione dei mercati e delle tecnologie, promozione e tutela della concorrenza, tutela della privacy.

Peraltro, l'intervento pubblico deve avere un "respiro" il più possibile internazionale, dal momento che tanto le tecnologie quanto le imprese (in primis, le grandi piattaforme digitali) operano su scala internazionale.

Nel nostro caso, l'Unione europea è il riferimento fondamentale per politiche industriali e di regolamentazione dell'ecosistema digitale. Tuttavia, l'impostazione di questi interventi a livello comunitario deve – necessariamente – trovare una declinazionale nazionale, anche nel caso in cui si tratti di regolamenti che, in quanto tali, non necessitano di recepimento nell'ordinamento nazionale. Ed, infine, altrettanto importante è che le strategie industriali e le misure regolamentari vengano confrontate con le caratteristiche strutturali e le vocazioni produttive dei territori, ossia a livello locale.

Questo, in sintesi, è l'approccio che verrà seguito da Astrid LED nel percorso di ricerca svolto assieme ad IFAB nella realizzazione del Work-Package di Supporto al Policy-making dell'Osservatorio sulle tendenze e le applicazioni del Supercalcolo.

In tale contesto, il presente contributo inizia dall'esame delle iniziative dell'Unione europea, tanto sul versante regolamentare e normativo, quanto dal punto di vista degli strumenti di politica industriale, descrivendo questa nuova "stagione" della politica comunitaria, che – dopo aver giustamente insistito su promozione e tutela della concorrenza e regolamentazione pro-concorrenziale dei mercati – da alcuni anni, si sta preoccupando ed occupando della competitività dell'economia europea. In tal senso, la stessa regolazione ha modificato il proprio orizzonte: da interventi prevalentemente "verticali", ossia per specifici settori (energia, telecomunicazioni, poste, trasporti, etc.) ad una nuova dimensione, "orizzontale", come testimoniato dal varo di regolamenti, quali quelli in materia di protezione dei dati personali, dei mercati digitali, dei servizi digitali, dei big data ed – in questi giorni – dell'intelligenza artificiale. Dal canto suo, la politica industriale, tornata ad essere un tema di intervento per l'Unione europea, comincia ad assumere profili più significativi e certi, sia pure attraverso interventi mirati a specifici settori o tecnologie, senza che – al momento – sia individuabile un chiaro approccio di sistema.

Dato il tema assegnato ad Astrid LED, l'attenzione principale viene riservata alle iniziative normative ed industriali e di ricerca nell'ambito di "tecnologie" e "mercati" digitali più prossimi all'attività del Centro Nazionale: il cloud, i big data, i microchip, il supercalcolo, la cybersecurity, l'intelligenza artificiale.

Così, ad esempio, si richiamano le vicende della impresa comune ("joint undertaking") *EuroHPC* e l'iniziativa "*GenAI4EU*", in quanto elementi fondamentali per lo sviluppo dell'intelligenza artificiale (generativa, in particolare), nonché per il rafforzamento della connettività e la diffusione dei servizi digitali.

Sul versante normativo, l'analisi è fondamentalmente rivolta alla proposta di Regolamento europeo in materia di intelligenza artificiale (AI act), che si prefigura essere la normativa principe del settore digitale, indicandone lo stato di avanzamento e con un approfondimento sui tratti di maggior rilievo. Tra i temi trattati, vi è la costituzione dell'ufficio europeo dell'AI ed il suo ruolo guida della strategia globale dell'UE sull'IA, quale non solo organo di vigilanza del "Patto sull'Intelligenza Artificiale", ma anche luogo di interazione tra la Commissione, i Paesi e altri portatori di interesse. Un focus è poi dedicato all'impatto del Regolamento rispetto ai temi della *cybersecurity*, della *privacy* e delle infrastrutture.

La disamina porta così ad una delle principali domande per il seguito della ricerca, ossia circa la capacità del Regolamento IA di ripercorrere l'esperienza del Regolamento Generale sulla Protezione dei Dati, attraverso il noto *Brussels Effect*. Più precisamente, ci si interrogherà sulla possibilità per l'Unione europea di "esternalizzare" le proprie scelte regolatorie a livello globale. Il tema verrà indagato primariamente sotto tre profili, i) effettività regolatoria; ii) bilanciamento tra innovazione, regolazione e investimenti tecnologici; iii) politica estera dei singoli Stati membri, con particolare riguardo ai profili di cooperazione.

Dopo l'analisi a livello comunitario, il testo in esame conduce una analisi delle politiche per il digitale nel nostro Paese, con riguardo sia al contesto nazionale, sia, per ora in via preliminare, alla dimensione locale. Si presentano così le iniziative in corso del Governo, del Parlamento e delle Autorità amministrative indipendenti, nonché le Agende Digitali promosse a livello locale, soprattutto Regionale. Con il medesimo approccio utilizzato per le iniziative europee, ci si concentra quindi sull'approccio italiano all'intelligenza artificiale, con due approfondimenti, il tema della *cybersecurity ed* i possibili problemi di *governance*.

Riguardo a questa parte della ricerca, si sono individuate due direttrici di analisi per il seguito: i) la possibile frammentarietà della dimensione Unionale, ii) il rapporto tra innovazione ed *enforcement* in termini di interpretazione e attuazione della normativa.

Da ultimo, nelle "conclusioni" si riassumono altri profili di analisi per il seguito della ricerca, a partire dal ruolo dell'IA Act per il rafforzamento del posizionamento dell'UE nell'ecosistema digitale, e, quindi, per gli impatti nel nostro Paese, a livello nazionale e locale.

In questo ambito, una particolare attenzione verrà riservata agli impatti delle misure europee sulle PMI, rispetto al contesto competitivo nazionale ed internazionale, sia valutando gli oneri derivanti dall'attività di *compliance*, sia considerando le opportunità per le imprese di sfruttare le tecnologie digitali per rafforzare la propria competitività.

Quale "sample" di possibili indicazioni finali da parte della ricerca, si formulano – infine - alcuni indirizzi in materia di cybersecurity, in particolare per la mitigazione dei rischi.

Le iniziative dell'Unione europea

Una nuova stagione dell'intervento pubblico: politica industriale e regolazione

Premesso che una accezione ampia di politica industriale, spesso usata in passato, ricomprendeva la regolazione dei mercati tra i possibili strumenti di politica industriale, in questa sede, manteniamo la distinzione – ormai ampiamente accettata – tra interventi di regolamentazione e misure di politica industriale in senso proprio.

Nell'esperienza degli ultimi decenni, la regolazione dei mercati ha ampiamente prevalso sulla politica industriale, come dimostra l'ampia produzione normativa, in primo luogo a livello europeo[1]. La stessa espressione "politica industriale" è stata vista con sospetto negli ultimi due decenni del secolo scorso e solo da una decina di anni a questa parte è tornata ad essere considerata, alla luce delle grandi trasformazioni e crisi che hanno attraversato i sistemi economici e che hanno dimostrato l'incapacità dei mercati ad affrontarli, per riprendere un processo di sviluppo equilibrato (tra i paesi ed all'interno degli stessi).

Con riguardo all'Unione Europa (UE), la politica industriale si pone l'obiettivo di creare le migliori condizioni per rendere l'industria europea competitiva, sostenibile, con attenzione anche ai riflessi sul mercato del lavoro (livelli occupazionali e retributivi, adeguamento competenze)[2].

Più recentemente, le c.d. transizioni digitale ed ecologica hanno accelerato lo sviluppo di strategie finalizzate al rafforzamento del tessuto industriale dell'Unione europea, anche a seguito della pandemia da Covid-19 e della guerra in Ucraina che hanno avuto effetti particolarmente negativi sulle catene di approvvigionamento di diversi settori industriali e produttivi (ad esempio, semiconduttori, materie prime).

La maggiore attenzione verso la definizione di migliori condizioni per l'industria UE ha avviato una riflessione sugli strumenti da introdurre o rafforzare per sostenere la ripresa economica, con l'obiettivo di fondo di accrescere l'autonomia strategica dell'economia europea.

In questo contesto, lo sviluppo diffuso e su vasta scala delle tecnologie digitali e delle loro applicazioni sia nelle reti che nei servizi finali sta trasformando – in profondità - l'economia, tanto l'offerta quanto la domanda, e gli stessi assetti delle società e delle democrazie europee.

L'agenda digitale europea per il decennio 2020-2030 affronta tali questioni concentrandosi sulla creazione di spazi e servizi digitali sicuri, sulla promozione di condizioni di *level playing field* nei mercati digitali al fine di limitare il potere delle grandi piattaforme, nonché sul rafforzamento della sovranità digitale dell'Europa, contribuendo allo stesso tempo all'obiettivo europeo della neutralità climatica entro il 2050.

---

[1] Peraltro, diversi studiosi e *practitioners* hanno sostenuto che la regolazione settoriale ha talora sopperito all'assenza di una vera politica industriale.

[2] La politica industriale dell'UE mira in maniera specifica a: (1) "accelerare l'adattamento dell'industria alle trasformazioni strutturali"; (2) "promuovere un ambiente favorevole all'iniziativa e allo sviluppo delle imprese di tutta l'Unione, segnatamente delle piccole e medie imprese"; (3) "promuovere un ambiente favorevole alla cooperazione tra imprese»; 4) "favorire un migliore sfruttamento del potenziale industriale delle politiche d'innovazione, di ricerca e di sviluppo tecnologico" (articolo 173 TFUE).

Alla luce di quanto precede, si rende necessaria la ricognizione degli interventi dell'Unione europea in tema di politica industriale e regolamentazione, con particolare riguardo alle iniziative a sostegno delle tecnologie digitali, nel contesto della doppia transizione digitale ed ecologica.

Tra le iniziative, verranno distinti gli atti normativi (in particolare, *Digital Service Act*[3], *Digital Market Act*[4], *Data Act*[5] e Data Governance Act[6], nonché il prossimo *Artificial Intelligence Act*[7]) rispetto agli strumenti di politica industriale quali, ad esempio, gli IPCEI (Importanti Progetti di Interesse Comune Europeo) e le Alleanze industriali.

Le iniziative normative

In questo campo, ossia nella produzione di regole, l'UE ha dimostrato una indubbia capacità, mediante l'introduzione di un insieme articolato di norme per l'ecosistema digitale. Il riconoscimento della validità dell'impianto normativo europeo per il digitale è esteso a livello internazionale, tanto che le discipline comunitarie in materia tendono a divenire standard per altri paesi, definendo così quel fenomeno denominato *Brussels Effect*[8].

Nello specifico, oltre ai regolamenti più noti che stanno attirando molto anche l'attenzione dei media, ed esattamente il *Digital Services Act* (DSA) ed il *Digital Markets Act* (DMA) – di cui non si tratterà in questo rapporto - e l'*Artificial Intelligence Act* (AI Act) di prossima approvazione, è bene tenere in conto il *Data Governance Act* (DGA)[9], propedeutico peraltro al *Data Act*.

Un ulteriore strumento di armonizzazione digitale a livello europeo è poi rappresentato dall'Identità Digitale europea[10]. Lo strumento nasce per sopperire alle carenze presentate dai sistemi di identificazione digitale offerti oggi dai governi degli stati membri dell'UE: i) non sono disponibili per l'intera popolazione, ii) spesso sono limitati ai servizi pubblici online, iii) non consentono un accesso senza soluzione di continuità a livello transfrontaliero[11].

---

[3] Regolamento (UE) 2022/2065.
[4] Regolamento (UE) 2022/1925.
[5] Regolamento (UE) 2023/2854.
[6] Regolamento (UE) 2022/868.
[7] COM/2021/206.
[8] A. Bradford, *The Brussels Effect. How the European Union Rules the World*, Oxford University Press, Oxford, 2020.
[9] Si tratta di uno strumento che mira a regolamentare il riutilizzo di dati pubblici/conservati e protetti, promuovendo la condivisione dei dati attraverso la regolamentazione di nuovi intermediari di dati e incoraggiando la condivisione di dati per scopi cosiddetti altruistici. Sia i dati personali che quelli non personali rientrano nell'ambito di applicazione del DGA e, quando si tratta di dati personali, si applica il Regolamento generale sulla protezione dei dati (General Data Protection Regulation, GDPR).
[10] V. https://www.consilium.europa.eu/it/press/press-releases/2023/11/08/european-digital-identity-council-and-parliament-reach-a-provisional-agreement-on-eid/.
[11] Si consideri che solo il 14% dei fornitori dei principali servizi pubblici in tutti gli Stati membri consente l'autenticazione transfrontaliera con un'e-ID, ad esempio per dimostrare l'identità di una persona su Internet senza bisogno di una password. Lo strumento europeo - al contrario - sarà disponibile ai cittadini, ai residenti e alle imprese dell'UE che desiderino identificarsi o confermare determinate informazioni personali. Può essere utilizzata per i servizi pubblici e privati sia online che offline in tutta l'UE.

L'insieme di queste misure rappresenta una visione integrata di armonizzazione, gestione e processo dei dati, mantenendo ben saldi i capisaldi dei diritti alla privacy europei, come definiti dal Regolamento Generale sulla Protezione dei Dati (General Data Protection Regulation, GDPR[12]), entrato in vigore nel maggio 2016 ed applicato dal maggio 2018.

Le iniziative di politica industriale

Per quanto concerne gli strumenti di politica industriale, l'obiettivo è rafforzare la cooperazione industriale per accelerare le attività economiche e produttive che non si svilupperebbero altrimenti, laddove contribuiscano ad attrarre investitori privati ed attivare nuovi partenariati e modelli commerciali, coinvolgendo anche le piccole e medie imprese (PMI) e le start-up[13].

In questo ambito, meritano attenzione specifica quegli *Important Projects of Common European Interest* (IPCEI) che interessano il digitale, nonché misure quali il *Chips Act*[14]. Questa ultima iniziativa, con la formula del *Joint Undertaking* per le fabbriche *first of a kind*, rappresenta un modello innovativo che, in forza delle eccezioni dell'art. 107 comma b) e c) del Trattato sul Funzionamento dell'UE (TFUE), prevede una possibilità di finanziamento pubblico all'industria ed alle stesse aziende[15]. Recente, inoltre, l'approvazione finale del Consiglio del *Critical Raw Materials Act*[16].

A queste iniziative, si sono aggiunte norme mirate ad aumentare e accelerare l'accesso ai finanziamenti pubblici nazionali/dell'UE e ai finanziamenti privati: in particolare, il nuovo quadro temporaneo per la crisi e la transizione in materia di aiuti di Stato[17].

Evidentemente, l'efficacia di queste iniziative dipenderà dalle risorse che verranno allocate dall'Unione europea, nonché da politiche fiscali comuni, come è accaduto nel caso del *Next Generation EU*.

[12] Regolamento (UE) 2016/679.

[13] Ad esempio, si citano il caso delle alleanze per le tecnologie per i processori e semiconduttori, per i dati industriali, l'edge e il cloud, ed i progetti di alleanze per i vettori spaziali e un'aviazione a emissioni zero.

[14] Regolamento (UE) 2023/1781.

[15] Il Chips Act consente aiuti di stato da parte degli Stati Membri. Per ogni euro impegnato da uno stato, la Commissione investe altrettanto (effetto *matching*). I fondi utilizzati dalla Commissione derivano dai Programmi Horizon Europe e Digital Europe. Tali aiuti di stato e comunitari sono possibili, come eccezione alle regole generali degli aiuti di stato, solo fino al *first industrial deployment* ossia fino all'arrivo sul mercato.

[16] Regolamento (UE) 2019/1020.

[17] Il nuovo quadro ha consentito, ad esempio, di semplificare la concessione di aiuti di Stato per la diffusione di energie rinnovabili e la decarbonizzazione dei processi industriali e offre agli Stati membri la possibilità di concedere livelli di aiuto più elevati per la produzione di tecnologie strategiche a zero emissioni nette per raggiungere gli aiuti ricevuti dai concorrenti situati in paesi terzi.

Da ultimo, la Commissione europea – a gennaio di questo anno - ha presentato un pacchetto di misure per sostenere lo sviluppo di sistemi di intelligenza artificiale (IA) affidabili da parte delle start-up e delle PMI europee, nel rispetto dei valori e delle norme dell'UE[18].

[18]Questo intervento fa seguito all'accordo politico del dicembre 2023 sulla prima legge globale sull'IA dell'UE, volta a promuovere lo sviluppo e l'adozione di IA affidabile nell'Unione Europea https://ec.europa.eu/commission/presscorner/detail/it/ip_23_6473

Infrastrutture abilitanti: supercalcolatori, reti e cloud

La Commissione Europea ha adottato una prospettiva strategica nell'impiego dell'intelligenza artificiale. In linea con questa visione strategica, la Commissione si prepara internamente per l'attuazione della legge dell'UE sull'IA, considerando anche i fattori abilitanti dell'IA. Questi includono i supercalcolatori essenziali per l'addestramento di modelli affidabili e la creazione di infrastrutture e misure per promuovere la connettività e la diffusione dei servizi.

Supercalcolatori

L'Unione europea si trova attualmente in prima linea a livello mondiale nel campo del supercalcolo, un risultato reso possibile dagli sforzi dell'impresa comune *EuroHPC*[19]. Tra i successi di EuroHPC, spiccano tre supercomputer dell'UE che figurano tra i migliori al mondo: LEONARDO, LUMI e MareNostrum5. Con l'espansione imminente delle capacità di *EuroHPC* verso prestazioni a esa-scala (oltre un miliardo di miliardi di calcoli al secondo) e oltre, grazie ai supercomputer JUPITER e al consorzio JULES VERNE, che saranno ancora più potenti per lavorare con i modelli di intelligenza artificiale, le risorse europee di supercalcolo assumeranno un ruolo centrale nella creazione e nell'addestramento di modelli di IA di grandi dimensioni[20].

Nell'ambito del "pacchetto" di interventi promossi a gennaio 2024, è stata annunciata un'iniziativa finalizzata a mettere a disposizione delle start-up europee innovative nel settore dell'IA, e alla comunità dell'innovazione in senso lato, un accesso privilegiato ai supercomputer europei, al fine di agevolare l'addestramento di modelli di IA affidabili. Il lancio della "*Large AI Grand Challenge*"[21] a novembre 2023, un premio finanziario che offre supporto alle start-up nel settore dell'IA e accesso ai supercalcoli, è stato il primo passo[22].

Inoltre, il "pacchetto" propone una modifica al regolamento *EuroHPC*[23], per introdurre "fabbriche di intelligenza artificiale" come nuovo elemento centrale delle attività dell'impresa comune relative ai supercomputer dell'UE. Le sue componenti includono l'acquisizione, l'aggiornamento e la gestione di supercomputer dedicati all'IA per agevolare l'apprendimento automatico e l'addestramento di modelli di IA su larga scala (GPAI). Inoltre, oltre alla facilitazione dell'accesso ai supercomputer dedicati all'IA, si propone – come anticipato - di contribuire all'uso dell'IA per una ampia platea di utilizzatori, a cominciare da start-up e PMI. Il "pacchetto" prevede anche l'istituzione di uno sportello unico per start-up e innovatori, il sostegno alle start-up nel settore dell'IA e all'ecosistema della ricerca per lo sviluppo

[19] V. https://eurohpc-ju.europa.eu/index_en.

[20] COMUNICATO STAMPA16 novembre 2023, Dalla Commissione via libera all'accesso ai supercomputer dell'UE per accelerare lo sviluppo dell'intelligenza artificiale. https://ec.europa.eu/commission/presscorner/detail/it/ip_23_5739

[21] V.https://aiboost-project.eu/.

[22] COMUNICATO STAMPA16 novembre 2023, Dalla Commissione via libera all'accesso ai supercomputer dell'UE per accelerare lo sviluppo dell'intelligenza artificiale. https://ec.europa.eu/commission/presscorner/detail/it/ip_23_5739

[23] REGOLAMENTO (UE) 2021/1173 DEL CONSIGLIO del 13 luglio 2021 relativo all'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo e che abroga il regolamento (UE) 2018/1488https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32021R1173&qid=1706091812789

di algoritmi, test, valutazioni e convalida di modelli di IA su larga scala. Infine, promuove lo sviluppo di diverse applicazioni emergenti di IA basate su modelli generali.

È altresì significativo il contributo del Parlamento europeo e del Consiglio, i quali saranno chiamati a esaminare le modifiche proposte dalla Commissione al regolamento che riguarda l'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo[24].

Per garantire un'implementazione efficace, l'Unione Europea ha delineato diverse iniziative chiave nel settore delle start-up e dell'innovazione nell'IA. Queste comprendono il sostegno finanziario attraverso i programmi *Horizon Europe* e Europa Digitale, con l'obiettivo di generare entro il 2027 un investimento complessivo di circa 4 miliardi di euro per l'IA generativa. Altre attività coinvolgono iniziative per potenziare il bacino di talenti dell'UE nell'IA generativa, la promozione di investimenti pubblici e privati nelle start-up e scale-up del settore, l'accelerazione degli spazi comuni europei dei dati, e l'iniziativa "*GenAI4EU*"[25] che sostiene lo sviluppo di nuovi casi d'uso e applicazioni emergenti in diversi settori industriali e pubblici, tra cui robotica, salute, biotecnologie, attività industriale, mobilità, clima e mondi virtuali.

Misure per la connettività e la diffusione dei servizi

La competitività futura dell'economia europea si basa su infrastrutture di rete digitale avanzate e servizi all'avanguardia, poiché una connettività veloce, sicura e diffusa è fondamentale per implementare le tecnologie all'avanguardia attualmente in via di sviluppo.

Il Libro Bianco su "Come soddisfare le esigenze di infrastruttura digitale dell'Europa?" esamina le sfide nel promuovere lo sviluppo di connettività integrata e infrastrutture di elaborazione collaborativa.[26] Per conseguire tale obiettivo, tra le diverse misure, il Libro Bianco propone la creazione di una "Rete di Elaborazione Collaborativa Connessa" ("3C Network") per istituire infrastrutture e piattaforme integrate end-to-end per il cloud e l'*edge* delle telecomunicazioni. Queste potrebbero essere sfruttate per coordinare lo sviluppo di tecnologie innovative e applicazioni di intelligenza artificiale in diversi contesti. Un tale approccio collaborativo potrebbe essere preparato mediante l'implementazione di occasioni di confronto o attraverso un (eventuale) nuovo progetto IPCEI nel "computing continuum".

L'ottimizzazione delle sinergie tra iniziative esistenti, come l'IPCEI sulla Infrastruttura e Servizi Cloud di Prossima Generazione, e programmi di finanziamento come il *Connecting Europe Facility*[27] e il *Digital Europe*[28] risultano cruciali.

---

[24] REGOLAMENTO (UE) 2021/1173 DEL CONSIGLIO del 13 luglio 2021 relativo all'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo e che abroga il regolamento (UE) 2018/1488 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32021R1173&qid=1706091812789

[25] V. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383.

[26] White Paper - How to master Europe's digital infrastructure needs? https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

[27] V. https://cinea.ec.europa.eu/programmes/connecting-europe-facility_en.

[28] V. https://digital-strategy.ec.europa.eu/it/activities/digital-programme.

Questo potrebbe prevedere un ruolo di coordinamento per il partenariato *Smart Networks and Services* (SNS JU)[29], per favorire la creazione di un ecosistema collaborativo dedicato alla connettività e all'elaborazione[30].

I dati indicano che IPCEI-CIS sarà un'iniziativa chiave per rendere disponibile la tecnologia necessaria per raggiungere alcuni degli obiettivi del Decennio Digitale, nello specifico raggiungere: i) il 75% di imprese dell'UE che utilizzano Cloud, Intelligenza Artificiale o Big Data; ii) 10.000 nodi periferici altamente sicuri e neutrali dal punto di vista climatico distribuiti in tutta Europa entro il 2030. L'obiettivo è di produrre l'accelerazione del processo che condurrà ad un mercato europeo interoperabile del cloud e dell'*edge computing*, sempre considerando la privacy dei dati, la *cybersecurity* e la sostenibilità come preoccupazioni primarie.[31]

Inoltre, il Libro Bianco presuppone la necessità da parte dell'Unione Europea di sfruttare appieno il potenziale del mercato unico digitale per le telecomunicazioni, adottando misure concrete per garantire una reale parità di condizioni tra operatori di comunicazioni elettroniche e grandi piattaforme digitali (level playing field), e rivedendo l'attuale quadro sia per la regolamentazione delle comunicazioni elettroniche, sia con riferimento all'applicazione della disciplina antitrust in materia di operazioni di concentrazione.

In questo contesto, la sicurezza dell'infrastruttura svolge un ruolo chiave anche in termini di competitività. Come evidenziato nel documento, si pone l'esigenza di tutelare le reti e le infrastrutture di elaborazione dell'Europa, fondamentali per la sicurezza economica; in tale ambito, l'UE dovrebbe rafforzare la sicurezza e la resilienza delle infrastrutture strategiche dei cavi sottomarini.

Infine, in merito alla creazione di infrastrutture e misure per favorire la connettività e la diffusione dei servizi, la Commissione ha collaborato con vari Stati membri per istituire due consorzi nell'ambito dell'infrastruttura digitale europea (EDIC): i) l'"Alleanza per le tecnologie del linguaggio" (ALT-EDIC), che si propone di sviluppare un'infrastruttura comune europea nel campo delle tecnologie linguistiche[32]; ii) L'EDIC "CitiVERSE" applica avanzati strumenti di IA per potenziare gemelli digitali locali, focalizzati sulle comunità intelligenti. Questo approccio supporta le città nel simulare e ottimizzare vari processi, dalla gestione del traffico alla gestione dei rifiuti.

Attualmente, gli Stati membri stanno istituendo i consorzi per l'infrastruttura digitale europea ALT-EDIC e l'EDIC CitiVERSE con il supporto della Commissione.

---

[29] V. https://smart-networks.europa.eu/.

[30] IPCEI on Next-Generation Cloud Infrastructure and Services to boost Europe's Digital Decade. https://digital-strategy.ec.europa.eu/en/news/ipcei-next-generation-cloud-infrastructure-and-services-boost-europes-digital-decade

[31] PRESS RELEASE 5 December 2023, Commission approves up to €1.2 billion of State aid by seven Member States for an Important Project of Common European Interest in cloud and edge computing technologies. https://digital-strategy.ec.europa.eu/en/news/commission-approves-eu12-billion-state-aid-seven-member-states-important-project-common-european

[32] Il consorzio è finalizzato a superare la mancanza di dati linguistici europei per l'addestramento di soluzioni di IA e, contemporaneamente, a preservare la diversità linguistica e culturale dell'Europa, facilitando così lo sviluppo di ampi modelli linguistici europei

La proposta di regolamento europeo sull'intelligenza artificiale

Il presente paragrafo è suddiviso in tre parti: A) stato di approvazione dell'AI act; B) panoramica sugli aggiornamenti/conferme di maggior rilievo nel testo; C) ruolo e compiti dell'ufficio europeo per l'intelligenza artificiale.

Si propone poi un focus su: a) cybersecurity e b) privacy, alla luce dell'ormai prossima approvazione del regolamento, con anche c) cenni ai riferimenti riguardanti il tema delle infrastrutture.

A) Stato di approvazione

Nel mese di dicembre, è stato raggiunto un accordo politico provvisorio sulla proposta di regolamento europeo sull'intelligenza artificiale (AI act)[33]. Il 24 gennaio, la presidenza belga dell'UE ha presentato la versione finale del testo in una riunione tecnica. La maggior parte degli Stati membri ha espresso riserve, ritirate il 2 febbraio con l'adozione dell'AI Act da parte del Comitato dei rappresentanti permanenti[34].

Le Commissioni per il mercato interno e la protezione dei consumatori (IMCO) e per le libertà civili, la giustizia e gli affari interni (LIBE) del Parlamento europeo hanno poi adottato il regolamento il 13 febbraio. Il 13 marzo, il Parlamento europeo ha poi approvato, con ampia maggioranza, il Regolamento sull'intelligenza artificiale, ora soggetto a revisione da parte dei giuristi-linguisti e che sarà poi adottato nella prossima sessione plenaria del Parlamento europeo (aprile), nonché approvato dal Consiglio e pubblicato sulla Gazzetta Ufficiale dell'Unione (presumibilmente nel mese di maggio).

L'AI Act entrerà così in vigore 20 giorni dopo la pubblicazione sulla Gazzetta ufficiale. Dall'entrata in vigore, le pratiche proibite dovranno essere conformi in 6 mesi; i *general-purpose AI systems* dovranno essere conformi in 12 mesi; i sistemi ad alto rischio (allegato II del Regolamento) dovranno essere conformi in 36 mesi; i sistemi ad alto rischio (allegato III del Regolamento) dovranno essere conformi in 24 mesi. Tuttavia, il regolamento si applicherà ai sistemi AI ad alto rischio immessi nel mercato o in servizio prima della data di applicazione[35], solo laddove soggetti a cambiamenti significativi nel loro *design*. Inoltre, nel caso di sistemi AI ad alto rischio destinati all'uso da parte delle autorità pubbliche, i fornitori e gli utilizzatori dovranno adottare misure necessarie per conformarsi entro 4 anni dalla data di entrata in vigore del Regolamento. Da ultimo, i fornitori di *general-purpose AI systems,* immessi sul mercato prima della data di applicazione del Regolamento, dovranno adottare misure necessarie per conformarsi agli obblighi entro 2 anni dall'entrata in vigore dello stesso.

---

[33] IMCO/LIBE, *Comunicato stampa: "Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI"*, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

[34] Consiglio dell'Unione europea, *Comunicato stampa: "Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world"*, https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

[35] Diversi dai sistemi elencati nell'allegato IX.

B) Panoramica sugli aggiornamenti/conferme di maggior rilievo

Nonostante il contenuto della proposta di regolamento sia oramai definitivo, la numerazione dei considerando e degli articoli potrebbe ancora subire variazioni nella versione definitiva, al pari di possibili affinamenti linguistici nella terminologia utilizzata.

- L'art 3 (1) definisce ora l'intelligenza artificiale come "*un sistema basato su macchina progettato per operare con vari livelli di autonomia [enfasi aggiunta] e che può manifestare adattabilità dopo il dispiegamento e che, per obiettivi espliciti o impliciti, deduce [enfasi aggiunta]*[36]*, dall'input che riceve, come generare output come previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*"[37].
- I *foundation models* sono di nuovo definiti *general-purpose AI systems - GPAI* ("*Sistema di intelligenza artificiale basato su un modello di intelligenza artificiale generale, che ha la capacità di servire una varietà di scopi, sia per uso diretto, sia per l'integrazione in altri sistemi di intelligenza artificiale*"[38]).
- Un "fornitore" di intelligenza artificiale è definito come l'entità che "*sviluppa un sistema di intelligenza artificiale o un modello di intelligenza artificiale generale o che ha un sistema di intelligenza artificiale o un modello di intelligenza artificiale generale sviluppato e li mette sul mercato o mette il sistema in servizio sotto il proprio nome o marchio commerciale, sia a pagamento che gratuitamente*"[39].
- Un "implementatore" è definito come un'entità sotto la cui autorità viene utilizzato un sistema di intelligenza artificiale, ad eccezione di usi personali e dunque al di fuori di attività professionali[40].
- In materia di *copyright*, all'Ufficio europeo per l'intelligenza artificiale è affidato il compito di fornire un *template* che gli sviluppatori dovranno utilizzare per segnalare il contenuto utilizzato nella fase di addestramento dei modelli di base[41]. Il sommario dovrà elencare "*le principali raccolte o insiemi di dati utilizzati per addestrare il modello, come grandi database privati o pubblici o archivi di dati, e una spiegazione narrativa su altre fonti di dati utilizzate*"[42]. Inoltre, le imprese dovranno mettere in atto misure organizzative e tecniche per garantire il rispetto dei diritti di *opt-out* dei titolari dei diritti. Tutto ciò al fine di facilitare un approccio trasparente e la conformità alla normativa sul *copyright*.
- È richiesto di adottare misure appropriate per garantire che i contenuti generati dalla GPAI siano identificati come tali, incluso, attraverso il *watermarking*, l'identificazione dei metadati e/o metodi crittografici[43].
- I fornitori dovranno tracciare, documentare e segnalare il consumo energetico conosciuto o stimato dei modelli sviluppati[44].

[36] "Autonomia" e "deduzione" rappresentano parole chiave per differenziare l'IA da un semplice software, v. considerando n. 6.

[37] V. l'ultima definizione dell'OCSE a cui si sono ispirati i lavori del parlamento europeo: https://oecd.ai/en/wonk/ai-system-definition-update

[38] Considerando 44e.

[39] Art. 2.

[40] *Ibid.*

[41] Considerando 60K.

[42] *Ibid.*

[43] Considerando 70a.

[44] Allegato IX a-c.

- *Red Teaming*[45]: i fornitori dovranno eseguire valutazioni dei modelli utilizzando protocolli e strumenti all'avanguardia[46]. Nel testo è richiesta la conduzione e documentazione dei c.d. *red teaming test* per identificare e mitigare i rischi sistemici. I rischi sistemici nell'Unione dovranno essere valutati e mitigati attraverso un sistema di gestione dei rischi (prevenzione di incidenti gravi, interruzioni dei settori critici e gravi conseguenze per la salute pubblica e la sicurezza; processi democratici, sicurezza pubblica ed economica; diffusione di contenuti illegali, falsi o discriminatori)[47].
- L'AI Act delega l'enforcement alle agenzie degli Stati membri, con la relativa base giuridica radicata nella legislazione degli Stati Membri[48]. L'AI Act andrà di pari passo con una struttura di governance complessa e stratificata che coinvolgerà molteplici entità, come organismi notificati e notificanti, organismi di valutazione della conformità, un consiglio per l'IA, un ufficio per l'IA, autorità nazionali competenti e autorità di vigilanza del mercato. Le sanzioni andranno da 35 milioni di euro o il 7% del fatturato globale annuo per le violazioni relative ai sistemi di intelligenza artificiale non permessi, a 15 milioni di euro o il 3% del fatturato globale annuo per altre violazioni dell'AI Act, e a 7,5 milioni di euro o l'1,5% del fatturato globale annuo per la fornitura di informazioni errate alle autorità di regolamentazione[49].
- I sistemi AI non saranno considerati ad alto rischio se mancanti di un rischio significativo per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, ivi compresa la propensione a influenzare in modo sostanziale l'esito delle decisioni. Tale previsione si applicherà se uno o più dei seguenti criteri saranno soddisfatti: (i) il sistema AI è destinato a svolgere un compito procedurale non rilevante; (ii) il sistema AI è destinato a migliorare il risultato di un'attività umana precedentemente completata; (iii) il sistema AI è destinato a rilevare schemi decisionali o deviazioni dai precedenti schemi decisionali e non è destinato a sostituire o influenzare la valutazione umana precedentemente completata, senza una corretta revisione umana; (iv) il sistema AI è destinato a svolgere un compito preparatorio per valutazioni rilevanti per le finalità degli utilizzi elencati nell'allegato III[50]. Tuttavia, indipendentemente dai criteri sopra indicati, un sistema AI sarà sempre considerato ad alto rischio in caso di profilazione di persone fisiche.
- I fornitori di sistemi di intelligenza artificiale ad alto rischio, che sono soggetti ad obblighi relativi ai sistemi di gestione della qualità ai sensi della regolamentazione settoriale dell'Unione, avranno "*la possibilità di includere gli elementi del sistema di gestione della qualità previsti nel regolamento come parte del sistema di gestione della qualità esistente previsto in tale altra legislazione settoriale dell'Unione*"[51]. Tuttavia, manca nel

[45] Il *Red Teaming* è una pratica di sicurezza informatica in cui un gruppo di esperti, chiamato "team red", assume il ruolo di aggressore o avversario per testare e valutare la sicurezza di un sistema, una rete o un'organizzazione. L'obiettivo del Red Teaming è identificare e sfruttare le vulnerabilità nel sistema in modo simile a come lo farebbe un attaccante reale, al fine di migliorare le misure di sicurezza e la risposta agli attacchi. Questa pratica può coinvolgere una serie di attività simulate, tra cui test di penetrazione, social engineering, analisi delle vulnerabilità e altri metodi per identificare e correggere i punti deboli nel sistema. Sul punto, v. https://www.ibm.com/blog/red-teaming-101-what-is-red-teaming/

[46] Allegato IXa.

[47] Considerando 60m.

[48] Art. 71.

[49] *Ibid.*

[50] Art. 6 (2a).

[51] Considerando 54.

testo una mappatura delle regole dell'AI Act da considerarsi "presumibilmente rispettate" in caso di sistema conforme a normative settoriali.

- È importante notare che nella catena del valore dell'IA, gli implementatori, in caso di modifiche sostanziali al modello, assumeranno le responsabilità dei fornitori[52]. Questa previsione assume particolare rilevanza rispetto ai *GPAI*, spesso adattabili a casi d'uso specifici. Per gli esperti in materia, si pone anche un problema di equilibrio tra la promozione dell'innovazione e la garanzia di chiarezza normativa; precisamente, nel delineare il confine in cui una variazione del modello porta a nuovi obblighi[53].
- L'AI Act riporta due tipi[54] di sistemi di intelligenza artificiale da considerare ad alto rischio: i) sistemi destinati ad essere utilizzati come prodotto (o componenti di sicurezza di un prodotto) coperti da specifica legislazione dell'UE, quali aviazione civile, sicurezza dei veicoli, attrezzature marine, giocattoli, ascensori, attrezzature a pressione e attrezzature di protezione individuale; ii) sistemi di intelligenza artificiale elencati nell'allegato III, quali i sistemi di identificazione biometrica remota, AI utilizzata come componente di sicurezza nelle infrastrutture critiche e AI utilizzata nell'istruzione, nell'occupazione, nel punteggio di credito, nell'accesso e godimento di servizi privati essenziali e servizi pubblici essenziali e per il riconoscimento di benefici e assistenza pubblica, nell'applicazione della legge, nell'immigrazione e nel processo democratico.
- I soggetti pubblici e le entità private che forniscono servizi pubblici (ad esempio, istruzione, assistenza sanitaria, alloggi, servizi sociali e entità coinvolte nel punteggio di credito o nell'assicurazione sulla vita e sulla salute) saranno tenuti a effettuare una valutazione dell'impatto sui diritti fondamentali prima di implementare un sistema AI ad alto rischio[55]. Questa valutazione richiederà agli enti di elencare i rischi, le misure di controllo, le misure di mitigazione dei rischi, le categorie di persone naturali interessate, la frequenza d'uso prevista e le funzioni per cui il sistema sarà utilizzato.
- Qualsiasi persona interessata avrà il diritto di accesso a informazioni (e a presentare eventualmente reclamo) sull'impatto del sistema di intelligenza artificiale nel processo decisionale (si pensi, rispetto a tale previsione, al potenziale conflitto con eventuali segreti industriali[56])[57].

C) L'ufficio europeo per l'Intelligenza Artificiale

La decisione della Commissione che istituisce l'Ufficio europeo per l'intelligenza artificiale è entrata in vigore il 21 febbraio 2024[58]. Più specificamente, l'ufficio supervisionerà l'attuazione e l'applicazione dell'AI Act. Altrettanto importante, giocherà un ruolo fondamentale nel rafforzare lo sviluppo e l'uso di un'IA affidabile, guidando il

[52] Art. 28(1)(b).

[53] C. Novelli *et al.*, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, Working Paper, accessibile su ssrn.com: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4694565.

[54] Art. 6.

[55] Considerando 58g e art. 5 e art. 29a.

[56] C. Novelli *et al.*, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, op. cit.

[57] Art. 52e.

[58] Commissione europea, Decisione della Commissione del 24 gennaio 2024 che istituisce l'Ufficio europeo per l'intelligenza artificiale, C/2024/1459, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C_202401459

coordinamento della politica sull'IA in Europa e promuovendo la cooperazione internazionale. L'entrata in vigore segue il già richiamato pacchetto di innovazione sull'IA, lanciato il 24 gennaio 2024[59].

Come componente cruciale della strategia globale dell'UE sull'IA, l'ufficio svolgerà un ruolo chiave nell'attuazione dell'AI Act - in particolare per quanto riguarda l'applicazione delle norme per i modelli di IA ad uso generale. L'ufficio agevolerà inoltre l'applicazione delle regole relative ai sistemi di IA ad alto rischio, nonché offrirà orientamenti e linee guida per gli interessati. Servendo da segreteria del Consiglio per l'IA - un organo di coordinamento essenziale per le autorità nazionali degli Stati membri - l'ufficio collaborerà strettamente con entità esistenti, come il Centro europeo per la trasparenza degli algoritmi presso il Centro comune di ricerca della Commissione Europea. Fori dedicati e gruppi di esperti consentiranno una condivisione di competenze all'interno della comunità scientifica, dell'industria, dei *think tank* e della società civile.

L'ufficio per l'intelligenza artificiale vigilerà, inoltre, sul "Patto sull'Intelligenza Artificiale"[60], che consente alle imprese di interagire con la Commissione e altri portatori di interessi, con la condivisione delle migliori pratiche e la partecipazione a particolari iniziative. Questo coinvolgimento inizierà prima che l'AI Act entri in vigore e consentirà alle imprese di pianificare e prepararsi all'attuazione dell'AI Act.

Focus: Cybersecurity e privacy alla luce del prossimo regolamento europeo sull'intelligenza artificiale

I temi della cybersecurity e della privacy sono strettamente correlati tra loro, nonché parte integrante del prossimo regolamento europeo sull'intelligenza artificiale. L'analisi si limita, in questa primo rapporto, al contenuto dell'ultima versione della proposta. Un potenziale, e necessario, approfondimento di quanto segue dovrà riguardare un'analisi comparativa dei numerosi testi legislativi europei che toccano i temi in trattazione. Ciò al fine di identificare possibili sovrapposizioni, nonché contraddizioni e dunque problemi di interpretazione, sia da parte del settore pubblico (anche in termini di controllo e attuazione), sia privato (in termini di misure per assicurare la conformità). Si pensi, a titolo esemplificativo, al Regolamento n. 881/2019 (*Cybersecurity Act*), alla Direttiva n. 2555/2022 (Direttiva *NIS 2*), alla Direttiva n. 2557/2022 sulla resilienza dei soggetti critici (*Direttiva CER – Resilience of Critical Entities*), al Regolamento 2019/1010 (*Cyber Resilience Act*), al Regolamento n. 2554/2022 (*DORA*), al recente Regolamento di esecuzione relativo all'adozione di un sistema europeo di certificazione della cibersicurezza basato sui criteri comuni[61], nonché chiaramente al GDPR, ai *Data Act* e *Data governance Act*, ai *Digital Market Act* e *Digital Service Act* e al Regolamento sullo spazio europeo dei dati sanitari.

Come per i paragrafi precedenti, nonostante il contenuto della proposta di regolamento sia oramai definitivo, la numerazione dei considerando e degli articoli potrebbe ancora subire variazioni nella versione definitiva, al pari di possibili affinamenti linguistici nella terminologia utilizzata.

[59] V. https://digital-strategy.ec.europa.eu/it/news/commission-launches-ai-innovation-package-support-artificial-intelligence-startups-and-smes.

[60] V. https://digital-strategy.ec.europa.eu/it/policies/ai-pact.

[61] V. https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-adoption-european-common-criteria-based-cybersecurity-certification-scheme

a) Cybersecurity

Come è noto, la sicurezza informatica è di competenza nazionale[62], ma ciò non influisce sulla rilevanza di un coordinamento europeo e di un impegno congiunto sul tema. Il termine "*cybersecurity*" appare numerose volte nell'AI act e, principalmente, con riferimento ai sistemi ad alto rischio e ai *general-purpose AI systems*. La sicurezza informatica è definita come cruciale nel garantire che i sistemi di IA siano costantemente resilienti durante il loro ciclo di vita e rispetto allo stato dell'arte a livello di innovazione[63]. In particolare, i sistemi dovranno essere in grado di mitigare i rischi di alterazione del loro utilizzo o di compromissione degli elementi sicurezza[64]. Al fine di garantire un livello di sicurezza informatica appropriato, il testo pone anche enfasi sulla necessità di adottate misure adeguate riguardo alle infrastrutture abilitanti[65].

Il focus centrale, in tema di sicurezza informatica, è nell'attuale art. 15 del regolamento, intitolato "accuratezza, robustezza e cybersicurezza", il quale prevede che:

i. la Commissione, in collaborazione con le parti interessate e le organizzazioni pertinenti, dovrà promuovere lo sviluppo di benchmark e metodologie di misurazione per valutare l'accuratezza e la robustezza dei sistemi AI ad alto rischio;
ii. i livelli di accuratezza e le metriche di accuratezza pertinenti dovranno essere dichiarati nelle istruzioni d'uso dei sistemi AI ad alto rischio. Sul punto, l'art. 13 prevede, infatti, che i sistemi ad alto rischio debbano essere accompagnati da istruzioni per l'uso in un formato digitale appropriato o in altro modo, che includano informazioni concise, complete, corrette e chiare che siano rilevanti, accessibili e comprensibili per gli utenti;
iii. i sistemi AI ad alto rischio dovranno essere il più resilienti possibile rispetto agli errori, ai difetti o alle inconsistenze che possono verificarsi nel sistema o nell'ambiente in cui opera, e dovranno adottare misure tecniche e organizzative in questo senso. La robustezza potrà essere ottenuta attraverso soluzioni di ridondanza tecnica, come piani di *backup* o *fail-safe*[66];
iv. dovranno essere adottate misure tecniche appropriate per garantire la sicurezza informatica dei sistemi AI ad alto rischio, comprese quelle volte a prevenire, rilevare, rispondere, risolvere e controllare attacchi informatici che potrebbero influenzare il set di dati di addestramento ("avvelenamento dei dati") o i componenti pre-addestrati utilizzati nell'addestramento ("avvelenamento del modello") , input progettati per causare un errore al modello ("esempi avversari" o "evasione del modello"), o eventuali difetti del modello.

Nonostante quanto sopra, i sistemi di IA ad alto rischio adempienti ai requisiti di cui al Regolamento 2022/0272[67] saranno da considerare conformi anche all'AI act[68]. Inoltre, i sistemi biometrici destinati esclusivamente a fini di

[62] (Cybersecurity Act, Considerando 5)
[63] Considerando 49.
[64] Considerando 51.
[65] *Ibid.*
[66] V. https://www.treccani.it/enciclopedia/fail-safe/.
[67] artt. 8 e 10 e allegato I del Regolamento 2022/0272.
[68] Considerando 51a.

sicurezza informatica non ricadranno tra i sistemi ad alto rischio[69]; parimenti, i componenti tecnici utilizzati a fini di sicurezza informatica, non rientreranno nella categoria di *safety components*[70].

Per quanto concerne i *general-purpose AI systems*, il testo chiede ai fornitori di integrare "appropriate salvaguardie di sicurezza e sicurezza"[71], riprendendo l'approccio a due livelli. In particolare, i fornitori di modelli di IA ad uso generale che presenteranno rischi sistemici dovranno essere soggetti, oltre agli obblighi previsti per i fornitori di modelli di IA ad uso generale, a obblighi volti a identificare e mitigare tali rischi ed assicurare un livello adeguato di protezione della sicurezza informatica. Quanto sopra indipendentemente dal fatto che il sistema sia fornito come modello autonomo o integrato in un altro sistema di IA o in un prodotto. Per raggiungere tali obiettivi, il Regolamento demanda ai fornitori di effettuare le necessarie valutazioni del modello, in particolare prima dell'immissione sul mercato, compresa la conduzione e la documentazione dei "test avversari" dei modelli (anche attraverso la collaborazione con soggetti esterni e indipendenti).

In aggiunta, ai fornitori di modelli di IA ad uso generale con rischi sistemici è richiesto di valutare e mitigare continuamente i rischi sistemici. Ad esempio, attraverso l'adozione di politiche di gestione del rischio, come processi di responsabilità e governance, implementando il monitoraggio post-commercio, adottando misure appropriate lungo l'intero ciclo di vita del modello e cooperando con attori rilevanti lungo la catena del valore dell'IA[72]. Sempre sul punto, in caso di incidente facente seguito ad una adozione corretta delle misure di sicurezza, il fornitore del modello di IA ad uso generale dovrà tenere traccia dell'accaduto e segnalare qualsiasi informazione rilevante e possibili misure correttive alla Commissione e alle autorità nazionali competenti (sulla scia di quanto avviene con il GDPR)[73].

Peraltro, non è da sottovalutare la propensione dei *large language models* (LLM) a rappresentare informazioni false o fuorvianti (c.d. allucinazioni). Si tratta di un tema che è già stato connesso a possibili frodi, truffe, manipolazioni mirate e non mirate nella fase di addestramento dei dati[74]. Con riguardo a rischi di allucinazione con ricadute di tale genere, secondo già richiamati esperti[75], l'AI act avrebbe dovuto focalizzarsi su qualsiasi sistema di IA, non solo quelli ad alto rischio. Inoltre, il testo avrebbe dovuto fornire misure tecniche proporzionate agli attacchi di un LLM specifico, indipendentemente dai livelli di rischio[76]. Per quanto concerne la disinformazione generata dai *foundation models*, occorrerebbe intervenire sia sull'IA act che sul Digital Service Act[77]. Infine, per contrastare gli "attacchi avversari" si

[69] Considerando 33.
[70] Considerando 34.
[71] Art. 28b.
[72] Considerando 60q.
[73] Considerando 60r.
[74] AlgorithmWatch; AIForensics, 'An Analysis of Microsoft's Bing Chat Generative AI and Elections: Are Chatbots a Reliable Source of Information for Voters?', 2023.
[75] C. Novelli *et al., Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, op. cit.
[76] Ibid.
[77] Ibid.

potrebbe limitare l'accesso dei LLM agli utenti o istituzioni registrate e restringere la quantità o la natura delle richieste degli utenti[78].

b) Privacy

Il tema della privacy è indubbiamente legato allo sviluppo di sistemi di intelligenza artificiale, nella misura in cui i dati utilizzati per l'addestramento racchiudono sfide di dimensioni adeguate dei *datasets*, standard di qualità, integrità e sicurezza[79]. Un utilizzo errato dei dati può portare a gravi violazioni dei diritti fondamentali, incluso il diritto alla privacy. Gli spazi comuni di dati europei istituiti dalla Commissione[80] e la facilitazione della condivisione dei dati tra imprese e con il governo nell'interesse pubblico saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di alta qualità per la formazione, la convalida e il test di sistemi di intelligenza artificiale.

Tra la questioni di maggior rilevanza è se, e come, i dati personali possano essere elaborati per addestrare i LLM. Gli elementi essenziali[81], in tal senso, sarebbero: i) la base legale appropriata per l'addestramento dell'IA (art. 6, 1, a, GDPR) – che è legata al tema della difficoltà del consenso informato e specifico per il trattamento di grandi quantità di dati personali[82]; ii) la base legale appropriata per l'elaborazione dei *prompt*; iii) requisiti informativi (artt. 12-15 GDPR); iv) inversione del modello, perdita di dati e diritto all'oblio; v) decisioni automatizzate (es. art. 22 GDPR); vi) protezione dei minori; e vii) limitazione dello scopo e minimizzazione dei dati. Sull'ultimo punto, l'AI act richiede una valutazione della quantità e della idoneità dei dati utilizzati[83] - che vanno oltre alla pseudo-anonimizzazione e crittografia[84].

In merito, c'è chi[85] ha suggerito: a) come una parte significativa di questi insiemi di dati potrebbe anche beneficiare delle eccezioni del diritto all'oblio del GDPR per l'interesse pubblico, la ricerca scientifica e storica; b) di incoraggiare l'implementazione corretta del diritto di *opt-out* da parte dei fornitori e utilizzatori di LLM; c) di esplorare il potenziale delle tecniche di "disapprendimento" delle macchine.

c) Infrastrutture

L'AI act non manca di far riferimento al tema delle infrastrutture. A tal riguardo:

i. per "infrastruttura critica" si intende un "*asset, un impianto, apparecchiature, una rete o un sistema, o una parte di essi, che è necessario per la fornitura di un servizio essenziale ai sensi dell'articolo 2, paragrafo 4, della direttiva*

[78] Ibid.

[79] L'AI act non interviene sui regolamenti (UE) 2016/679 e (UE) 2018/1725 e sulle direttive 2002/58/CE e (UE) 2016/680, fatta eccezione per le disposizioni previste all'articolo 10, comma 5, e all'articolo 54 (Art. 2 (5a)).

[80] V. https://digital-strategy.ec.europa.eu/it/policies/data-spaces.

[81] Ricordati in C. Novelli *et al.*, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, *op. cit.*

[82] Gli autori *ibid.* suggeriscono come strumento ideale il test di bilanciamento di cui all'art. 6(1)(f) del GDPR, che richiede un approccio caso per caso.

[83] Articolo 10(e).

[84] Art. 10.

[85] C. Novelli *et al.*, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, *op. cit*; L. Floridi, *Machine Unlearning: Its Nature, Scope, and Importance for a "Delete Culture"*, in *Philosophy & Technology* 36 (2): 42.

(UE) 2022/2557"[86]. Inoltre, lo stesso termine fa riferimento anche a "*sistemi di intelligenza artificiale destinati ad essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento dell'infrastruttura digitale critica, del traffico stradale e della fornitura di acqua, gas, riscaldamento ed elettricità*"[87];

ii. i sistemi di intelligenza artificiale ad alto rischio nell'ambito dell'infrastruttura critica dovranno essere registrati solo a livello nazionale[88];

iii. i fornitori saranno tenuti a istituire un sistema per segnalare alle autorità competenti qualsiasi incidente grave derivante dall'uso dei loro sistemi di intelligenza artificiale. Si intende, per incidente o malfunzionamento, un evento che comporta la morte o un grave danno alla salute, un'interruzione grave e irreversibile della gestione e del funzionamento dell'infrastruttura critica, nonché violazioni degli obblighi previsti dal diritto dell'Unione intesi a proteggere i diritti fondamentali o danni gravi alle proprietà o all'ambiente[89];

iv. la Commissione potrà progettare iniziative, anche di natura settoriale, per facilitare la riduzione delle barriere tecniche che ostacolano lo scambio transfrontaliero di dati per lo sviluppo dell'IA, compresa l'infrastruttura di accesso ai dati, l'interoperabilità semantica e tecnica di diversi tipi di dati[90];

v. per quanto riguarda la gestione e il funzionamento dell'infrastruttura critica, si prevede di classificare come ad alto rischio i sistemi di intelligenza artificiale destinati ad essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento dell'infrastruttura digitale critica. Questo poiché il malfunzionamento o guasto potrebbe mettere a rischio la vita e la salute di persone su larga scala e portare a interruzioni apprezzabili nella conduzione ordinaria delle attività sociali ed economiche;

vi. i componenti di sicurezza dell'infrastruttura critica, compresa l'infrastruttura digitale critica, sono considerati sistemi utilizzati per proteggere direttamente l'integrità fisica dell'infrastruttura critica o la salute e la sicurezza delle persone e delle proprietà, ma non necessari affinché il sistema funzioni.

Un "Brussels effect" per l'AI act? L'impatto sul (e rispetto al) mercato globale

È globalmente noto il lavoro di Anu Bradford laddove ha descritto il successo dell'Unione europea nell'esternalizzare le proprie scelte regolatorie[91]. Il riferimento tradizionale è al GDPR, secondo alcuni un esempio di standard globale cui le imprese sono state obbligate a conformarsi in tutto il mondo[92]. Si tratta, peraltro, di una tendenza dell'UE che ha origini antecedenti alla discussione sul digitale (si pensi alla sicurezza alimentare[93], settore in cui l'UE ha dagli albori ispirato la regolazione al di fuori dei propri confini).

[86] Considerando 44h.

[87] Allegato III (2).

[88] Considerando 69.

[89] Considerando 78.

[90] Considerando 81.

[91] A. Bradford, *The Brussels Effect: How the European Union Rules the World*, cit., 2020.

[92] Tra i molti, si veda S. Gunst e F. De Ville, *The Brussels Effect: How the GDPR Conquered Silicon Valley*, in *European Foreign Affairs Review*, 26, 3, 2021, pp. 437 – 458.

[93] Sul punto, si veda il Reg. (CE) 178/2002.

Diviene dunque doveroso chiedersi se l'IA act sarà in grado di rafforzare il posizionamento dell'UE nel contesto geopolitico e nel mercato globale. Si tratta però di un tema che dovrà essere indagato, quantomeno, sotto tre profili: l'effettività regolatoria[94], il bilanciamento tra innovazione, regolazione e investimenti economici, la politica estera dei singoli Stati membri, con particolare riguardo ai profili di cooperazione.

Quanto al tema dell'effettività, l'UE si propone come regolatore globale dell'IA con un testo ricco di disposizioni, la cui flessibilità è tema di dibattito rispetto alla concretezza dell'approccio informato al rischio[95], nonché caratterizzato da un importante e graduale lasso di tempo antecedente all'applicabilità delle singole disposizioni. Si tratta di tempistiche, quelle del processo regolamentare europeo, chiaramente incompatibili con lo sviluppo del settore e l'AI act dovrà dunque dimostrare di essere un regolamento in grado di resistere al futuro, anche solo prossimo. Ciò anche alla luce del fatto che l'approccio *risk-based* è atecnico rispetto a come viene applicato nei settori, ad esempio, finanziario, della sicurezza alimentare o dell'aviazione. Infatti, non si pone come mezzo per calcolo del rischio al momento dell'*enforcement* o in chiave predittiva, ma positivizzando il rischio noto al momento della fase di regolazione.

Sarà così centrale, nel discorso sull'impatto dell'IA nel mercato globale, attuare una prima linea di ricerca e approfondimento sul monitoraggio e la capacità del regolamento di qualificarsi come "attuale" e nel bilanciamento con lo sviluppo tecnologico.

Il secondo profilo, di particolare rilevanza, riguarda gli investimenti per lo sviluppo del settore. L'IA è caratterizzata da crescente pervasività in ogni aspetto della quotidianità e dalla capacità di innescare cambiamenti di paradigma in ogni specifico settore. Si pensi anche solo all'impatto sull'automazione del mondo del lavoro. In tale contesto, risulterebbe probabilmente fallimentare un mero approccio normativo, laddove si punti a creare uno standard internazionale di riferimento per l'intelligenza artificiale. Sul tema, nel 2022, gli Stati Uniti hanno accumulato 47,4 miliardi di dollari in investimenti nell'intelligenza artificiale[96], circa 3,5 volte di più rispetto al secondo maggior contributore (la Cina, che ha registrato 13,4 miliardi di dollari)[97]. Sempre gli Stati Uniti ospitano anche il maggior numero di aziende di intelligenza artificiale maggiormente finanziate privatamente, superando di quasi il doppio il totale combinato di UE e Regno Unito e superando la Cina con un numero di imprese 3,4 volte superiore[98]. Peraltro, quello statunitense è un approccio che non dimentica l'aspetto regolatorio e ne è la prova il noto (e copioso) executive

[94] «Da un lato, vi sarebbe il semplice rispetto delle norme e delle decisioni amministrative da parte dei destinatari (effettività formale), dall'altro il perseguimento dell'obiettivo ultimo di queste (effettività sostanziale)» (M. De Benedetto e N. Rangone, *La questione amministrativa dell'effettività: regole, decisioni e fatti*, in *Diritto pubblico*, 3, 2918, pp. 764 ss.);

[95] G. Finocchiaro, *The regulation of artificial intelligence*, in *AI&Society*, 2023.

[96] N. Maslej *et al.*, *Artificial Intelligence Index Report 2023*, Stanford University, April 2023, 6, https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf.

[97] *Ibid.*

[98] *Ibid.*

order di Biden[99], cui seguiranno e stanno seguendo indicazioni aggiuntive da singoli attori governativi[100]. Si tratta, tuttavia, di una prospettiva che riconosce la necessità di mitigare i rischi potenziali dell'IA, ma che accompagna anche lo sviluppo economico e digitale (è forte, ad esempio, il riferimento alla fase di *testing* in ambienti protetti o reali). Tale seconda linea di ricerca ha dunque l'obiettivo di approfondire gli elementi necessari per una politica globale dell'intelligenza artificiale, tra approccio regolatorio e sovranità economico-tecnologica.

Il ruolo di *leadership* dipende anche però da un terzo fattore, riguardante la cooperazione, sia in termini interni, sia di politica estera. Sul punto, l'UE racchiude il rischio di apparire (ed essere nella pratica) disomogenea internamente rispetto alle politiche di investimento nel settore dell'IA e di interpretazione del Regolamento (si è visto, nel caso del GDPR, un certo grado di differenziazione tra gli Stati membri nell'applicazione delle sanzioni e nel bilanciamento tra innovazione e intervento pubblico delle autorità nazionali[101]). Vi è poi un profilo di disponibilità dei singoli Stati membri ad un dialogo e ad una cooperazione extra-UE. Si pensi, rispetto ad un punto di crescente rilevanza, al tema della strategia di difesa europea (anche digitale), un tema frammentato per questioni di competenze e sempre più dipendente dallo sviluppo e dall'applicazione di sistemi di intelligenza artificiale.

Occorre dunque, in questa terza linea di ricerca, indagare la capacità dell'UE di evitare frammentarietà interne che andrebbero a ledere, tanto la tenuta dell'assetto economico Unionale, quanto la coerenza comunicativa verso l'esterno (con potenziali rischi di "cattura" da parte di imprese e di altri attori extra-UE).

[99] Si veda https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/fact-sheet-president-biden-issues-executive-order-and-announces-new-actions-to-advance-womens-health-research-and-innovation/

[100] Si veda, tra gli altri, il recentissimo e rilevante documento dell'OMB: https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf

[101] Tra i molti, si veda J. Wolff e N. Atallah, *Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020*, in *Journal of Information Policy*, 11, 2021, pp. 63-103.

Le iniziative dell'Italia

Le politiche per il digitale in Italia

Livello Nazionale

La strategia italiana per il digitale nasce avendo a riferimento l'Agenda Digitale europea varata nel 2010, poi seguita da altre fondamentali iniziative che hanno integrato quel progetto: Digital Single Market (2015), Shaping Europe's Digital Future (2020), Decennio digitale 2030 (*digital compass*) (2021)[102].

Nel quadro del piano europeo, il nostro Paese ha sviluppato l'Agenda Digitale Italiana, ossia una strategia nazionale, in collaborazione con la Conferenza delle Regioni e delle Province Autonome, per raggiungere gli obiettivi indicati dall'Agenda Europea.

Lo scopo dell'Agenda Digitale è fare leva sul potenziale delle tecnologie ICT per favorire innovazione, progresso e crescita economica, avendo come obiettivo principale lo sviluppo del mercato unico digitale.

Nell'ambito dell'Agenda Digitale Italiana, sono stati inizialmente predisposti la *Strategia italiana per la banda ultralarga*[103] e la *Strategia per la Crescita Digitale 2014-2020* per il perseguimento degli obiettivi dell'Agenda Digitale.

Per quanto riguarda la connettività, ossia la disponibilità di reti a banda ultra-larga, dal 2015 in avanti, sono stati finanziati – attraverso apposite procedure di gara - piani per il deployment di queste infrastrutture ad elevata capacità di banda, ed è stata promossa la costituzione di un operatore pubblico (Open Fiber) che ha sfidato l'incumbent (Telecom Italia) nella realizzazione delle reti a banda ultra-larga. Peraltro, l'intervento pubblico, come richiamato in precedenza, ha anche interessato il lato della domanda, con i piani voucher, destinati alle famiglie ed alle piccole e medie imprese.

Un ulteriore impulso allo sviluppo delle reti e dei servizi digitali è venuto, quindi, dal Piano Nazionale di Ripresa e Resilienza (PNRR), che ha assegnato il 27% delle risorse complessive (191,1 miliardi di euro) proprio alla transizione digitale[104]. Nell'aprile 2021, è stato così definito un (nuovo) Piano strategico per la transizione digitale e la connettività del Paese. Si tratta del c.d. Italia Digitale 2026, un piano strategico per il digitale che si articola lungo sei ambiti di intervento: Connettività, Migrazione al Cloud e Servizi Digitali della PA, Sanità Digitale, Competenze Digitali, Tecnologia e Spazio, Riforme e interventi normativi.

---

[102] Il Primo Rapporto sullo stato di avanzamento del Digital Decade è stato pubblicato a settembre 2023.

[103] La Strategia italiana per la Banda Ultra larga definisce le azioni necessarie al raggiungimento degli obiettivi di trasformazione digitale indicati dalla Commissione europea nel 2016 (Comunicazione sulla Connettività per un mercato unico digitale europeo cd. 'Gigabit Society') e nel 2021 (Comunicazione sul decennio digitale cd. Digital Compass). Più in particolare il 25 maggio 2021 è stata lanciata la Strategia Italiana per la Banda Ultralarga "Verso la Gigabit Society" che amplia e rilancia le azioni previste dalla Strategia Italiana per la Banda Ultralarga approvata il 3 marzo 2015 sulla base di quanto previsto dal PNRR.

[104] Al PNRR, si è affiancato il Piano Nazionale Complementare - PNC, che ha stanziato ulteriori 30,6 miliardi, per finanziare specifiche azioni che integrano e completano il PNRR.

L'attuale Governo ha, di recente, rivisto ed integrato la Strategia per la Banda Ultra larga, fissando obiettivi fino al 2026, in sintonia tanto con le precedenti versioni della strategia, quanto con gli obiettivi che si è data l'Europa. Per questa via, l'Italia dovrebbe – almeno in parte – migliorare la propria collocazione nell'ecosistema digitale che, come risulta dall'indice DESI, permane tuttora alquanto insoddisfacente[105].

Tra le iniziative legate invece alla Strategia per la crescita digitale, hanno avuto particolare attenzione le c.d. piattaforme abilitanti. Si tratta di quei servizi che abilitano in maniera trasversale la trasformazione digitale della PA, quali i servizi unificati di identificazione, pagamento e raccolta dati che semplificano l'interazione tra cittadini, imprese e Pubbliche Amministrazioni. Più nello specifico, le iniziative hanno riguardato: i sistemi di autenticazione SPID e CIE, la piattaforma IO che consente ai cittadini di usufruire di servizi, ricevere comunicazioni, effettuare pagamenti e reperire documenti in possesso delle PA nazionali o locali tramite l'utilizzo di un'unica applicazione software, l'Anagrafe centrale di tutti i cittadini (ANPR), il Sistema dei Pagamenti Elettronici (PagoPA), la Piattaforma Digitale Nazionale Dati (PDND) e il Fascicolo Sanitario Elettronico (FSE).

Inoltre, nel contesto delle strategie per il digitale che vedono il dato come elemento sempre più determinante per garantire qualità ed efficienza amministrativa si inserisce anche la Strategia Cloud Italia, realizzata dal Dipartimento per la trasformazione digitale e dall'Agenzia per la cybersicurezza nazionale (ACN). Si tratta di una iniziativa che delinea gli indirizzi strategici che agevolano il processo di migrazione verso il cloud di dati e servizi digitali della Pubblica Amministrazione. Il documento indica i criteri di classificazione di dati e servizi e la composizione della infrastruttura ad alta affidabilità (Polo Strategico Nazionale) che ospiterà i servizi strategici e critici.

Un richiamo è quindi opportuno al Piano Transizione 4.0[106], che prosegue il piano Industria 4.0, con l'obiettivo di avviare una politica industriale del Paese più inclusiva e attenta alla sostenibilità e dotata di maggiore attenzione all'innovazione e agli investimenti green.

Se, poi, si esaminano specifici settori/tecnologie, una menzione deve essere fatta per le iniziative italiane in ambito di microelettronica e supercalcolo.

Nel primo caso, è stato presentato a novembre 2023, a Pavia, il Centro italiano per il design dei circuiti integrati a semiconduttore (Fondazione Chips.IT), tassello fondamentale della strategia italiana per la microelettronica. Il Centro, infatti, si pone come coordinatore delle attività di ricerca e design con attori pubblici e privati, mettendo a disposizione attrezzature e software di ultima generazione, e, attraverso il ruolo di Competence Centre, aiutando a formare nuove generazioni di talenti nel settore.

[105] Il DESI (Digital Economy and Society Index) è un indice introdotto nel 2014 dalla Commissione europea, con l'intenzione di monitorare i progressi degli stati membri verso il conseguimento degli obiettivi fissati dall'Europa per il mercato unico digitale. Il DESI si basa su 33 indicatori, raccolti in quattro aree: Capitale umano, Connettività, Integrazione delle tecnologie digitali, Servizi pubblici digitali.

[106] Il piano si sviluppa tramite tre strumenti principali: Credito d'imposta per investimenti in beni strumentali, Credito d'imposta ricerca, sviluppo, innovazione e design e Credito d'imposta formazione 4.0.

Sul versante del supercalcolo, il riferimento obbligato è al Centro Nazionale di Ricerca in High Performance Computing, Big Data e Quantum Computing.

Livello locale

L'Agenda Digitale Italiana fa a sua volta da guida alle Agende Digitali promosse da enti locali, soprattutto le Regioni[107].

Da una prima sommaria ricostruzione delle informazioni disponibili, le strategie digitali locali e le iniziative ad esse legate sono finalizzate a superare – a livello territoriale - gli ostacoli alla digitalizzazione di economia e società: scarsa alfabetizzazione digitale, carenza di adeguate competenze digitali, difficoltà nell'accesso a dati, ai contenuti e ai servizi, dovute spesso all'insufficiente capillarità delle infrastrutture digitali.

Un esempio di riferimento è l'iniziativa *Data Valley Bene Comune*[108], l'Agenda Digitale dell'Emilia-Romagna 2020 - 2025, che affronta otto sfide per favorire l'innovazione digitale e tecnologica e lo sviluppo della società dell'informazione nei territori: i) i dati per una intelligenza diffusa a disposizione del territorio; ii) le competenze digitali: la nuova infrastruttura per lo sviluppo socio-economico; iii) la trasformazione digitale della Pubblica Amministrazione; iv) la trasformazione digitale dei settori produttivi e dei servizi; v) servizi pubblici digitali centrati sull'utente, integrati, aumentati, semplici e sicuri; vi) più reti e più rete per una Emilia-Romagna iperconnessa; vii) da contesti marginali a comunità digitali; viii) donne e digitale: una risorsa indispensabile.

Un altro esempio significativo è rappresentato dall'Agenda Digitale del Lazio 2022-2026 (maggio 2022). Un piano che si rivolge a cittadini, imprese ed Enti Locali e che si declina lungo cinque macro-aree strategiche e di azione: i) infrastrutture abilitanti; ii) Cybersecurity; iii) cultura digitale e competenze digitali delle persone; iv) accessibilità alla tecnologia; v) design dei servizi e delle relazioni: fruibilità dei servizi e semplificazione dei processi.

Infine, tra le iniziative di rilievo prese in considerazione in questa preliminare analisi della dimensione locale, si segnala il progetto Comuni Digitali della Regione Lombardia. L'iniziativa, frutto della collaborazione[109] tra la Regione e ANCI, si pone l'obiettivo di sostenere lo sviluppo di processi di semplificazione e trasformazione digitale nelle Amministrazioni comunali lombarde ed in particolare l'impegno prevede di: i) sostenere lo sviluppo di processi di semplificazione e trasformazione digitale nelle Amministrazioni comunali; ii) attivare iniziative pilota sperimentali negli ambiti di collaborazione; iii) definire un conseguente piano di diffusione ed estensione progressiva su tutto il territorio regionale dei risultati raggiunti con le iniziative pilota; iv) reperire risorse finanziarie a livello locale, statale e comunitario per dare attuazione al protocollo.

La Conferenza delle Regioni e le Province autonome ha inoltre recentemente espresso il proprio posizionamento[110] in merito all'introduzione dell'Intelligenza artificiale in ambito pubblico, elaborando proposte e sottoponendo alcune questioni su cui discutere. Tra queste si segnalano in particolare: i) la necessità di rivedere la Strategia nazionale sull'intelligenza artificiale (2022-2024); ii) l'attivazione di investimenti che vedano Regioni e Province autonome

[107] Il tema delle iniziative e delle strategie locali sarà oggetto di approfondimento nel prosieguo del progetto di ricerca di Astrid-LED.

[108] https://digitale.regione.emilia-romagna.it/dvbc

[109] Delibera N. XI/6174 del 28/03/2022 di Regione Lombardia.

[110] https://www.regioni.it/download/conferenze/657359/

come soggetti attuatori per avere "dati pubblici pronti per la AI"; iii) il potenziamento ruolo dell'Ufficio del Responsabile per la transizione digitale che va espressamente individuato anche come presidio immediato del tema intelligenza artificiale negli Enti; iv) il giusto riconoscimento del ruolo delle Regioni rispetto alla definizione di criteri e casi d'uso; v) una riflessione circa la straordinaria opportunità dello sviluppo dell'intelligenza artificiale, da conciliarsi con l'aspetto etico dei suoi utilizzi; vi) la definizione di regole e criteri standard di accettabilità delle decisioni algoritmiche; vii) la definizione di indirizzi specifici formativi che sappiano sviluppare le competenze necessarie per cogliere le opportunità offerte dall'intelligenza artificiale nell'ambito dell'innovazione organizzativa del lavoro nella PA.

Da ultimo, è bene ricordare le funzioni del Comitato interministeriale per la transizione digitale (CITD), che coordina l'azione del Governo nell'attuazione dell'agenda digitale italiana ed europea. In particolare, per quanto qui interessa, il Comitato svolge il compito di assicurare il coordinamento e il monitoraggio dell'attuazione delle iniziative di innovazione tecnologica e transizione digitale delle pubbliche amministrazioni competenti, comprese le attività di coordinamento e monitoraggio dell'attuazione delle iniziative relative, fra l'altro, alla strategia nazionale italiana per la banda ultra larga, alle reti di comunicazione elettronica satellitari, terrestri mobili e fisse, allo sviluppo e alla diffusione delle tecnologie emergenti dell'intelligenza artificiale, dell'internet delle cose (IoT) e della blockchain[111].

L'approccio italiano all'intelligenza artificiale

Anche in Italia si sta assistendo ad un utilizzo crescente dell'IA[112], in particolare a seguito dei recenti sviluppi della IA generativa. Di conseguenza, anche l'attenzione si è fortemente spostata sul tema dell'intelligenza artificiale.

Ad esempio, finora, abbiamo censito ben dodici iniziative avviate da istituzioni nazionali: in estrema sintesi, si tratta di: i) due Comitati governativi, uno dei quali incaricato di riformulare la Strategia italiana per l'IA (sottosegretario Alessio Butti); ii) otto indagini conoscitive promosse da Commissioni parlamentari della Camera (quattro), del Senato (tre) e dal Comitato per la documentazione; iii) una indagine conoscitiva del Garante per la protezione dei dati personali; iv) un Comitato di esperti promosso dall'Autorità per le Garanzie nelle Comunicazioni.

Senza dimenticare che due governi precedenti hanno presentato altrettante strategie italiane per l'intelligenza artificiale. L'auspicio è che, a questa ricchezza di analisi, segua anche la definizione di una visione organica, operativa e condivisa.

---

[111] Per queste ragioni, al Comitato, possono prendere parte, quando si trattano materie che interessano le regioni e le province autonome, il presidente della Conferenza delle regioni e delle province autonome o un presidente di regione o di provincia autonoma da lui delegato e, per i rispettivi ambiti di competenza, il presidente dell'Associazione nazionale dei comuni italiani (ANCI) e il presidente dell'Unione delle province d'Italia (UPI).

[112] Anche in Italia, sono molteplici le applicazioni, 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, con notevoli benefici, ma, allo stesso tempo, anche con rischi per la salute, la sicurezza e la tutela dei diritti fondamentali.

Iniziative del Governo

i. Innanzitutto, è da segnalare l'annuncio di un prossimo disegno di legge sull'intelligenza artificiale, che verrà presentato e discusso in Consiglio dei Ministri la prima settimana di aprile[113]. Nel disegno di legge si prevederanno, tra le altre cose, l'attribuzione alla Presidenza del Consiglio dei Ministri di responsabilità politica in materia di IA, rispetto ai temi della sicurezza strategica e della difesa; un comitato interministeriale per la trasformazione digitale; l'individuazione dell'autorità competenti per l'intelligenza artificiale; il riordino delle modalità di riconoscimento di fondi per l'avvio di start-up e partnership per l'innovazione; incentivi per attrarre risorse specializzate[114].

ii. Commissione sull'intelligenza artificiale per l'informazione. La Commissione è un organo del Dipartimento per l'Informazione e l'Editoria della Presidenza del Consiglio dei ministri istituito per studiare l'impatto dell'intelligenza artificiale sul mondo del giornalismo e dell'editoria;

iii. Comitato di coordinamento per l'intelligenza artificiale. Istituito dal Sottosegretario per l'innovazione alla Presidenza del Consiglio dei ministri Alessio Butti. Lo scopo del Comitato è di analizzare l'impatto dell'intelligenza artificiale e mettere a punto il piano strategico italiano con l'obiettivo di guidare lo sviluppo di questa tecnologia in modo responsabile e inclusivo.

Iniziative del Parlamento e Autorità Amministrative Indipendenti

i. Indagine conoscitiva sull'impatto dell'intelligenza artificiale nel settore della giustizia, deliberata dalla Commissione 2ª (Giustizia) del Senato[115];

ii. Indagine conoscitiva su nuovi profili e criticità relativamente alla difesa cibernetica[116], deliberata dalla Commissione IV (Difesa) della Camera;

iii. Indagine conoscitiva sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano, avviata dalla Commissione X (Attività produttive, commercio e turismo) della Camera;

iv. 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, avviata dalla Commissione XI (Lavoro pubblico e privato) della Camera;

v. Indagine conoscitiva sull'impatto dell'intelligenza artificiale nei settori di competenza della 7ª Commissione, anche con riferimento al servizio ChatGPT, avviata dalla Commissione 7ª (Cultura e patrimonio culturale, istruzione pubblica, ricerca scientifica, spettacolo e sport) del Senato;

vi. 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, avviata dalla Commissione 8ª (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) del Senato;

vii. Comitato Parlamentare di vigilanza sull'attività di documentazione, presieduto dalla vicepresidente della Camera dei deputati Anna Ascani, con l'obiettivo di conoscere l'avanzamento dell'intelligenza artificiale e

[113] Si veda l'intervista del Sen. Alessio Butti per la Repubblica: "Più ricercatori e campioni nazionali. L'AI parlerà italiano" del 12 marzo 2024.

[114] *Ibid.*

[115] Una proposta analoga è stata avanzata presso la Commissione Giustizia della Camera.

[116] La sicurezza cibernetica è intensamente integrata con l'Intelligenza Artificiale, tramite l'adozione sempre più frequente di strumenti e tecniche basati sull'Intelligenza Artificiale.

degli algoritmi e di studiare la loro possibile applicazione all'interno della documentazione parlamentare, a supporto dell'attività del Parlamento;

viii. Indagine conoscitiva sui siti internet pubblici e privati per verificare l'adozione di idonee misure di sicurezza adeguate ad impedire la raccolta massiva (*webscraping*) di dati personali a fini di addestramento degli algoritmi di intelligenza artificiale (IA) da parte di soggetti terzi, avviata dal Garante per la protezione dei dati personali;

ix. Comitato di esperti dell'Autorità per le Garanzie nelle Comunicazioni, presieduto dal professor Andrea Renda.

A queste indagini conoscitive, si è aggiunta nel corso dell'attuale legislatura la presentazione di numerosi disegni di legge di cui si terrà conto nel caso di uno sviluppo del relativo iter legislativo in Parlamento.

Il possibile impatto di un problema di governance

Un tema attuale e di cruciale rilevanza attiene alla governance dell'intelligenza artificiale. In particolare, si fa riferimento alla disposizione dell'AI act in base alla quale ogni Stato membro è chiamato ad istituire o assegnare specifiche competenze ad un'autorità nazionale per l'applicazione della normativa rilevante[117]. Sul punto, il Governo italiano non ha nascosto l'orientamento di voler affidare la governance ad un'agenzia dipendente dalla Presidenza del Consiglio dei Ministri e dunque non ad un'autorità indipendente[118]. In egual misura, le autorità indipendenti, ma anche alcune organizzazioni[119], hanno fortemente criticato questa eventuale decisione. Su tutti, il Garante privacy che ha trasmesso recentissimamente una segnalazione al Parlamento e al Governo[120].

Dal punto di vista del Governo, la competenza di una agenzia (o più, dato che si è parlato di duplice competenza tra AgiD e ACN per gli aspetti di cybersicurezza) alle dipendenze di Palazzo Chigi offre l'opportunità di fondere la vigilanza normativa, alla visione strategica sullo sviluppo del settore in Italia.

Dal punto di vista delle autorità indipendenti (o comunque dei sostenitori di tale seconda scelta), l'ingerenza dei sistemi di intelligenza artificiale sui diritti dei cittadini richiede certezze di *accountability*, competenze tecniche specializzate (nonché multidisciplinari) e autonomia rispetto ai mutamenti e agli interessi politici che nascono anche maggiori rischi di cattura da parte dei soggetti regolati. Queste sarebbero peculiarità proprio delle autorità indipendenti e che nessun altro ente può assicurare. Il Garante privacy, inoltre, ha evidenziato come l'AI act si fondi sull'art 16 del TFUE, ossia la base giuridica del GDPR, la quale racchiude infatti già alcune disposizioni sul processo decisionale automatizzato.

Il tema non è però solo politico. La scelta nasconde almeno due linee di ricerca: i) frammentarietà nella dimensione Unionale; ii) rapporto tra innovazione e *enforcement* in termini di interpretazione e attuazione della normativa.

A questi due aspetti si dedicherà un approfondimento in base alle evidenze conseguenti alla scelta italiana e degli altri Paesi). In ogni caso, leggendo i temi congiuntamente, lasciare agli Stati membri la scelta di affidare o meno le

[117] Art. 71.

[118] Si veda https://www.lastampa.it/economia/2024/03/26/news/il_garante_boccia_il_governo_chi_vigila_su_ai_e_privacy_deve_essere_indipendente-14175106/.

[119] Si veda https://www.thegoodlobby.it/intelligenza-artificiale-serve-unauthority-indipendente/

[120] Si veda https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9996508

competenze ad autorità indipendenti porterà potenzialmente ad approcci diversificati, i quali inficeranno proprio su quelle auspicate armonizzazione e uniformità di cui al paragrafo sul *brussels effect* dell'IA act. La scelta arriva così a racchiudere dinamiche di strategia politica tra gli Stati membri, laddove essi potrebbero influenzarsi negativamente verso la scelta di un'Agenzia dipendente dal Governo. Questo proprio per limitare di avere meno controllo, rispetto ad altri partner UE, sul bilanciamento tra innovazione e regolamentazione. Si sarebbero create così le condizioni per un conflitto interno nell'UE, laddove l'obiettivo è avere invece un approccio e una voce comune rispetto al contesto globale. Un tema che avrà un conseguente impatto sullo sviluppo del tessuto economico locale e nazionale e dell'innovazione nel Paese, che si propone di sviluppare in un prossimo approfondimento.

Misure nazionali in tema di cybersecurity

Il Consiglio dei Ministri n. 66 del 25 gennaio 2024 ha approvato uno *schema di disegno di legge recante disposizioni in materia di reati informatici e di rafforzamento della cybersicurezza nazionale*.

Il Ddl sul tema dei reati informatici e della cybersicurezza nazionale interviene con l'obiettivo di adeguare l'Italia al contesto geopolitico attuale, caratterizzato da un aumento degli attacchi informatici nonostante le misure europee introdotte con la Direttiva NIS. Il provvedimento prepara il terreno per il recepimento della già citata Direttiva NIS2, che mira a rafforzare la cybersicurezza nell'UE, includendo gli enti pubblici. Le nuove disposizioni riguardano obblighi per gli Stati membri, gestione dei rischi, condivisione delle informazioni e vigilanza.

Il provvedimento mira a proteggere le PMI, il settore finanziario, la Pubblica Amministrazione e il sistema sanitario. Introduce, inoltre, un nuovo coordinamento operativo tra l'Agenzia per la Cybersicurezza nazionale (ACN), la magistratura e i servizi di informazione per la sicurezza, e amplia l'obbligo di dotarsi di sistemi di cybersicurezza per soggetti pubblici ed erogatori di servizi di pubblica utilità. In aggiunta, viene introdotta la figura del referente per la cybersicurezza per le PA interessate, incaricato di coordinare le attività di sicurezza delle informazioni. In caso di attacco informatico, è prevista l'obbligatoria notifica entro 24 ore all'Agenzia per la cybersicurezza. Le figure del referente cybersecurity, dell'organismo di vigilanza e del *data protection officer* sono chiamate a integrarsi per prevenire reati informatici e violazioni dei dati personali, con particolare attenzione all'adeguamento agli standard ISO/IEC 27001:2022 e alla gestione condivisa dei rischi aziendali.

Il Ddl propone un approccio integrato tra le disposizioni sulla cybersicurezza e la tutela dei dati personali, come previsto dal GDPR e dal Decreto Legislativo 231/2001 sulla responsabilità amministrativa delle persone giuridiche. In questo contesto normativo, si rafforza il collegamento tra la responsabilità amministrativa degli enti e i reati informatici, richiedendo un'accurata analisi del rischio e l'adozione di misure tecniche e organizzative efficaci.

Lo schema introduce anche un inasprimento delle pene per i reati digitali, aumentando la reclusione fino a 10 anni per l'accesso illecito a sistemi informatici e fino a 12 anni in casi aggravati. Chi fornisce programmi dannosi potrebbe ricevere fino a 2 anni di detenzione e multe superiori a 10.000 euro. Sono previste, tuttavia, riduzioni di pena per chi collabora con le autorità inquirenti. L'Agenzia per la Cybersicurezza Nazionale (ACN) avrà poteri ispettivi e sanzionatori ampliati, potendo multare fino a 125.000 euro gli enti che non comunicano incidenti o non adottano interventi risolutivi entro 15 giorni. Inoltre, l'ACN promuoverà anche l'uso dell'intelligenza artificiale per rafforzare la cybersicurezza nazionale.

In aggiunta a quanto sopra, il decreto-legge n. 105/2019, convertito nella legge n. 133/2019, ha istituito il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) con l'obiettivo di garantire un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di enti pubblici e privati che svolgono funzioni essenziali per lo Stato.

Inoltre, la disciplina del golden power, derivante dal decreto-legge 15 marzo 2012, n. 21, ha subito numerose modifiche nel corso degli anni, con l'obiettivo di estendere e rafforzare i poteri speciali. Il decreto-legge 25 marzo 2019, n. 22, ha introdotto nuove disposizioni riguardanti le reti di telecomunicazioni 5G, mentre il decreto-legge 21 settembre 2019, n. 105, ha ampliato l'ambito operativo dei poteri speciali del governo nei settori strategici, in ottemperanza il Regolamento 2019/452 dell'Unione europea sul controllo degli investimenti esteri diretti nell'UE.

Un'importante novità è stata introdotta con il decreto-legge n. 104/2023, noto come *Decreto Asset*, che ha autorizzato l'applicazione del Golden Power a tecnologie particolarmente critiche, tra cui intelligenza artificiale, cybersecurity e macchinari per la produzione di chip.

Sempre in materia di cybersicurezza, l'Agenzia per la Cybersicurezza nazionale ha pubblicato una *strategia nazionale per il periodo 2022-2026*, che prevede il raggiungimento di 82 misure entro il 2026. Tra le sfide: a) assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione e del tessuto produttivo; b) anticipare l'evoluzione della minaccia cyber; c) contrastare la disinformazione nel più ampio contesto della c.d. minaccia ibrida; d) gestione di crisi cibernetiche; e) autonomia strategica nazionale ed europea nel settore del digitale. Tra gli obiettivi: a) protezione degli asset; b) risposta efficace alle minacce; c) sviluppo sicuro delle tecnologie digitali. La strategia è accompagnata da un *piano di implementazione* e da un *manuale operativo di attuazione*.

Sul punto, un recente ricerca I-COM[121] ha evidenziato che il 74 % delle imprese ritiene gli adempimenti inadeguati a favorire la competitività del Paese, in virtù dell'impatto negativo degli oneri burocratici richiesti, nonché della mancanza di politiche per incentivare gli investimenti e l'incertezza interpretativa tra il contesto normativo europeo e quello nazionale.

L'AgID è anche recentemente intervenuta attraverso la pubblicazione del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026, frutto di un processo collaborativo tra diverse istituzioni. Tale documento strategico è focalizzato sul potenziamento della sicurezza informatica nelle PA, con particolare enfasi sulla distribuzione e l'implementazione degli *Indicatori di Compromissione* (IoC) e sull'incremento degli strumenti di autovalutazione.

Il capitolo 7 del Piano, dedicato specificatamente alla sicurezza informatica, assume un'importanza prioritaria, delineando obiettivi chiari e misurabili per migliorare la sicurezza informatica nelle PA italiane. Gli obiettivi includono la distribuzione degli *IoC* a tutte le PA entro il 2026 e programmi formativi per aumentare la consapevolezza delle minacce digitali. Le linee guida si articolano in iniziative di monitoraggio proattivo, strumenti di autovalutazione dei rischi cyber e programmi formativi per promuovere una cultura della cybersecurity all'interno delle PA.

[121] I-COM – Istituto per la competitività, *Rapporto osservatorio sulla cibersicurezza: La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole*, https://d110erj175o600.cloudfront.net/wp-content/uploads/2024/02/15130401/Rapporto-I-Com_Osservatorio-sulla-Cibersicurezza_2024.pdf

In particolare, l'obiettivo RA7.6.1 si concentra sulla distribuzione degli IoC, con target intermedi del 30% entro il 2024, del 60% entro il 2025 e del 100% entro il 2026. L'obiettivo RA7.6.2 prevede la fornitura di strumenti per l'autovalutazione dei sistemi esposti, accessibili tramite il Portale del CERT-AGID, per consentire alle PA di valutare autonomamente la propria sicurezza e identificare vulnerabilità.

Infine, l'obiettivo RA7.6.3 mira a fornire supporto formativo e informativo alle PA, in particolare ai Responsabili per la Transizione Digitale, per aumentare la consapevolezza sulle possibili minacce. Questo approccio proattivo alla gestione del rischio cyber, supportato da strumenti di autovalutazione e formazione, contribuisce a rafforzare la resilienza delle infrastrutture informatiche pubbliche.

Da ultimo, giova ricordare che, entro ottobre, l'Italia dovrà integrare nel proprio sistema normativo due direttive europee. La prima, nota come CER, riguarda la resilienza cibernetica dei soggetti critici. La seconda, denominata NIS 2[122], impone nuovi obblighi sulla sicurezza dei dati e maggiori responsabilità per gli attori coinvolti, ampliando il campo di applicazione per includere numerose PMI italiane.

[122] Disegno di legge recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2022-2023" (Atto Camera 1342).

Linee di sviluppo della ricerca e alcune preliminari indicazioni

In precedenza, si sono indicati alcuni approfondimenti della ricerca svolta da Astrid LED che qui si richiamano, integrandoli con altre direttrici di analisi per il seguito della ricerca.

In primo luogo, si è segnalata la necessità di verificare se ed in quale misura l'IA act possa rafforzare il posizionamento dell'UE nel contesto geopolitico e nel mercato globale, ed – a tale riguardo – si sono proposte alcune direzioni di analisi.

Nello svolgimento di questo compito, sarà importante valutare in combinato disposto l'intervento regolamentare e le misure di politica industriale e della ricerca che la Commissione europea ha varato nel corso del tempo, da ultimo con il più volte richiamato "pacchetto" di interventi del 24 gennaio scorso. Inoltre, è importante segnalare che quest'analisi avrà tre diversi livelli "geografici" di approfondimento: l'Europa, l'Italia, la dimensione locale del nostro Paese. Ciò in linea con l'impostazione di fondo della collaborazione di ricerca tra Astrid LED e iFAB.

Un secondo terreno di approfondimento riguarda la relazione tra l'AI Act e le altre discipline di carattere orizzontale che hanno un rilievo importante per lo sviluppo dei Big Data, dell'Intelligenza artificiale e del supercalcolo. Ci si riferisce ai già richiamati regolamenti varati negli ultimi anni: in particolare, il GDPR, il Data Governance Act ed il Data Act, oltre al DSA e DMA.

Come pure assume importanza il tema della governance dell'AI Act. Sia con riguardo alla relazione tra gli Uffici della Commissione europea e le autorità nazionali che vigileranno sul rispetto delle regole in materia di IA, sia con riferimento al grado di autonomia ed indipendenza delle autorità nazionali rispetto all'Esecutivo.

Un'altra direttrice di analisi riguarderà gli impatti che le misure europee – regolamentari e di politica industriale – potranno avere con riguardo alle PMI. In effetti, lo sviluppo e la diffusione delle tecnologie digitali e, tra questa dell'intelligenza artificiale, mentre dimostrano la capacità di propagazione estesa a tutti i settori dell'industria e dei servizi, si scontrano con il diverso grado di preparazione al digitale da parte delle imprese, a seconda delle loro dimensioni produttive. In estrema sintesi, ci si chiederà in quale misura, ed attraverso quali strumenti, sia possibile consentire alle PMI di sfruttare le potenzialità delle tecnologie digitali nella promozione di una maggiore efficienza produttiva, di un arricchimento dell'offerta all'utenza finale, di un migliore posizionamento – insomma – nel contesto competitivo nazionale ed internazionale[123].

Da ultimo, si pone il problema degli adempimenti previsti dall'AI Act, con riguardo, soprattutto agli sviluppatori di sistemi di IA, ma anche alle aziende che utilizzano questi sistemi. Queste ultime già scontano una arretratezza tanto nell'adozione di sistemi di IA (solo il 5% delle imprese li ha finora adottati), quanto una "strutturale" difficoltà a realizzare i benefici dell'introduzione di tecnologie innovative[124].

[123] Un tema affine ma distinto rispetto al rapporto tra tecnologie digitali e PMI è rappresentato dal ruolo che le start up possono svolgere nell'ecosistema digitale, anche con riferimento al contesto italiano, nazionale e locale.
[124] I ritardi delle imprese italiane nell'adozione delle nuove tecnologie e la scarsa capacità a sfruttarne pienamente i vantaggi è un fenomeno da tempo esaminato dalla letteratura economica: per tutti, si rimanda ai contributi di ricerca del prof. Sergio Mariotti (Politecnico di Milano), nella seconda metà degli anni Ottanta.

A questo punto, sia pure nella consapevolezza del livello iniziale dell'analisi fin qui svolta, e quindi tenuto conto che il seguito della ricerca fornirà elementi di valutazione ulteriori e più sistematici, si sottopongono alcune preliminari indicazioni[125] di policy, sulla base di quanto fin qui rappresentato e sulla scorta dei risultati della letteratura in materia, con riguardo al tema della mitigazione dei rischi legati alla cybersicurezza, come *sample* di quelle che potrebbero essere le conclusioni di policy della ricerca Astrid LED.

In sintesi, emerge la necessità di:

1. individuare un sempre crescente numero di risorse umane specializzate;
2. prendere parte a forum e comunità di multistakeholder per la condivisione di *best-practices*;
3. stabilire meccanismi e processi di coordinamento con tutti gli attori governativi rilevanti;
4. valutare, revisionare e migliorare regolarmente la strategia aziendale e le politiche interne in base a precedenti incidenti (accaduti o evitati), feedback ricevuti da regolari controlli esterni e nuovi rischi identificati dalla ricerca scientifica;
5. integrare un modello di gestione del rischio umano per garantire una sicurezza continua, considerando le persone come possibile punto di partenza di problemi legati alla sicurezza digitale;
6. promuovere l'utilizzo della c.d. "*people analytics*"[126] per ottimizzare la formazione individuale, identificando e collegando i bisogni formativi personali ai profili di rischio specifici;
7. trasformare la formazione in strumento di riduzione del rischio, migliorando così la resilienza e la consapevolezza individuale riguardo alla sicurezza informatica;
8. accertare l'affidabilità dei fornitori di servizi gestiti o di servizi di sicurezza gestiti;
9. coinvolgere esperti in comunicazioni elettroniche per migliorare la preparazione e la risposta agli attacchi informatici in tale settore;
10. promuovere una condivisione immediata di eventuali incidenti per garantire una risposta tempestiva di possibili altri enti interessati;
11. estendere i test di stress fisici alle infrastrutture digitali.

[125] Da 1 a 5 ispirate a OECD, *Recommendations of the Council on National Digital Security Strategies*, OECD/Legal/0480; da 6 a 8 ispirate a Cefriel, *Sicurezza informatica ed elemento umano. Rischi e interventi di mitigazione, ripartendo dalle persone*, febbraio 2024; da 9 a 11 ispirate a Commissione europea, *Report on the cybersecurity and resiliency of the EU communications infrastructures and networks*, 21 febbraio 2024.

[126] R. Ghatak, *People Analytics: Data to Decisions*, Springer Nature, Singapore, 2022.

Allegato – Ricostruzione recenti documenti UE in materia di IA e strategie/tecnologie abilitanti

In questo allegato vengono riportati documenti recenti in materia di intelligenza artificiale (e strategie/tecnologie abilitanti) prodotti dall'Unione europea.

Versione aggiornata al 27 marzo 2024.

I collegamenti ipertestuali riportano prevalentemente a documenti in lingua italiana. Se non presenti, si rinvia a documenti in lingua inglese.

Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione

Final version.

Trilogo

- AIA Final Draft (26 January 2024).
- *Consolidated version*.
- AI Mandates (20 June 2023).

Commissione Europea

- AIA – COM – Draft Standardisation Request (5 December 2022).
- AIA – COM – Proposal (21 April 2021).
- AIA – COM – Annexes (21 April 2021).
- AIA – COM – Impact Assessment 1 (21 April 2021).
- AIA – COM – Impact Assessment 2 (21 April 2021).
- AIA – COM – Impact Assessment 3 (21 April 2021).

Consiglio dell'Unione Europea

- AIA – CZ – General Approach (25 November 2022).
- AIA – CZ – Draft General Approach (11 November 2022).
- AIA – CZ – Draft for Coreper (3 November 2022).
- AIA – CZ – 4th Proposal (19 October 2022).
- AIA – CZ – 3rd Proposal (23 September 2022).
- AIA – CZ – 2nd Proposal (16 September 2022).
- AIA – CZ – 1st Proposal (15 July 2022).
- AIA – CZ – Options Paper (17 June 2022).
- AIA – FRA – Consolidated Version (15 June 2022).

- AIA – FRA – Progress Report (16 May 2022).
- AIA – FRA – Art 3+4 (13 May 2022).
- AIA – FRA – Art 56-58 and 63-69 (6 May 2022).
- AIA – FRA – Art 70-85 (3 May 2022).
- AIA – FRA – Art 30-39 and 59-62 (25 April 2022).
- AIA – FRA – JHA (4 April 2022).
- AIA – FRA – Art 53-55a (7 March 2022).
- AIA – FRA – Art 40-52 (15 February 2022).
- AIA – FRA – Art 16-29 (3 February 2022).
- AIA – FRA – Art 8-15 (13 January 2022).
- AIA – SLO – Art 1-7 (29 November 2021).
- AIA – SLO – Progress Report (22 November 2021).

Parlamento Europeo

- AIA – IMCO-LIBE Report – Adopted (14 June 2023).
- AIA – IMCO-LIBE Report – All Amendments (14 June 2022).
- AIA – IMCO-LIBE Report – Draft (20 April 2022).
- AIA – JURI – Rule 57 Opinion – Adopted (12 September 2022).
- AIA – JURI – Rule 57 Opinion – Amendments (24 March 2022).
- AIA – JURI – Rule 57 Opinion – Draft (2 March 2022).
- AIA – ITRE – Rule 57 Opinion – Adopted (14 June 2022).
- AIA – ITRE – Rule 57 Opinion – Amendments (31 March 2022).
- AIA – ITRE – Rule 57 Opinion – Draft (3 March 2022).
- AIA – CULT – Rule 57 Opinion – Adopted (16 June 2022).
- AIA – CULT – Rule 57 Opinion – Amendments (1 April 2022).
- AIA – CULT – Rule 57 Opinion – Draft (21 February 2022).
- AIA – ENVI – Rule 56 Opinion – Adopted (22 April 2022).
- AIA – ENVI – Rule 56 Opinion – Amendments (25 January 2022).
- AIA – ENVI – Rule 56 Opinion – Draft (10 December 2021).
- AIA – TRAN – Rule 56 Opinion – Adopted (12 July 2022).
- AIA – TRAN – Rule 56 Opinion – Amendments (4 May 2022).
- AIA – TRAN – Rule 56 Opinion – Draft (29 March 2022).

Altre istituzioni

- AIA – ECB – Opinion I (29 Dec 2021).
- AIA – ECB – Opinion II (29 Dec 2021).
- AIA – CoR – Opinion (2 Dec 2021).
- AIA – EESC – Opinion (22 Sept 2021).
- AIA – EDPB+EDPS – Opinion (18 June 2021).

Ufficio europeo per l'intelligenza artificiale:

- Decisione della Commissione del 24.1.2024 che istituisce l'Ufficio europeo per l'intelligenza artificiale - C (2024)390.

Artificial Intelligence in the European Commission (AI@EC) Communication:

- https://commission.europa.eu/document/download/601a9e64-cdb9-4545-becb-1079ba8c457c_en?filename=EN%20Artificial%20Intelligence%20in%20the%20European%20Commission.PDF&prefLang=it

Politica industriale

- European Critical Raw Materials Act
- Proposal for a Directive of the European Parliament and of the Council amending Directives 2009/102/EC and (EU) 2017/1132 as regards further **expanding and upgrading the use of digital tools and processes in company law**.
- Regolamento (UE) 2021/1173 del Consiglio del 13 luglio 2021 relativo all'istituzione dell'impresa comune per il **calcolo ad alte prestazioni europeo** e che abroga il regolamento (UE) 2018/1488.
- Regolamento (UE) 2023/1781 del Parlamento europeo e del Consiglio del 13 settembre 2023 che istituisce un **quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori** e che modifica il regolamento (UE) 2021/694 (regolamento sui chip).
- Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio del 14 dicembre 2022 che istituisce il programma strategico per il **decennio digitale 2030**.
- Risoluzione legislativa del Parlamento europeo del 15 febbraio 2023 sulla proposta di regolamento del Consiglio recante modifica del regolamento (UE) 2021/2085 che istituisce le **imprese comuni nell'ambito di Orizzonte Europa** per quanto riguarda l'impresa.
- Regolamento (UE) 2021/523 del Parlamento europeo e del Consiglio del 24 marzo 2021 che istituisce il **programma InvestEU** e che modifica il regolamento (UE) 2015/1017.
- Emendamenti del Parlamento europeo, approvati il 21 novembre 2023, alla proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro di misure per rafforzare l'ecosistema europeo di produzione di prodotti delle **tecnologie a zero emissioni nette.**
- Establishing the **Strategic Technologies for Europe Platform** ('STEP').
- Regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio, del 14 giugno 2023, relativo alle **macchine** e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio.
- Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio del 10 maggio 2023 relativo alla **sicurezza generale dei prodotti**, che modifica il regolamento (UE) n. 1025/2012.
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on **boosting startups and innovation** in trustworthy artificial intelligence - COM(2024) 28 final.
- Proposal for a COUNCIL REGULATION regulation amending Regulation (EU) 2021/1173 as regards an **EuroHPC initiative for start-ups** to boost European leadership in trustworthy Artificial Intelligence - COM(2024).

- Recommendations and roadmap for **European sovereignty on open source hardware, software and RISC-V Technologies**.
- First **regulatory sandbox on Artificial Intelligence** presented.
- The European Union and the United States of America strengthen **cooperation** on research in **Artificial Intelligence and computing** for the Public Good.
- TTC Joint Roadmap for Trustworthy **AI and Risk Management**.
- Hiroshima Process **International Guiding Principles for Advanced AI system**.
- Hiroshima Process **International Code of Conduct for Advanced AI Systems**.
- DIGITAL Europe - **High Performance Computing** (managed by the EuroHPC Joint Undertaking).
- Strategia sul web 4.0 e i **mondi virtuali** per guidare la prossima transizione tecnologica.
- Norme armonizzate dell'UE in materia di **brevetti** promuovono l'innovazione, gli investimenti e la competitività nel mercato unico.
- Joint Communication: An EU Approach for **Space Traffic Management** - An EU contribution addressing a global challenge.
- Strategia europea in materia di **sicurezza economica**.
- Raccomandazione sui settori tecnologici critici per la sicurezza economica dell'UE: semiconduttori avanzati, intelligenza artificiale, quantistica, biotecnologie.
- Consorzio europeo per le infrastrutture digitali.
- Nuovo **sistema brevettuale unitario.**

Connettività

- Raccomandazioni sulla promozione normativa della connettività gigabit.
- Regolamento (UE) 2023/588 del Parlamento europeo e del Consiglio del 15 marzo 2023 che istituisce il programma dell'Unione per una **connettività sicura per il periodo 2023-2027.**
- Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'**identità digitale europea.**

Dati

- Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il **programma Europa digitale** e abroga la decisione (UE) 2015/2240.
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni: **"Bussola per il digitale 2030: il modello europeo per il decennio digitale".**
- Dichiarazione europea sui diritti e i principi digitali.
- Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 **(Regolamento sulla governance dei dati)**.
- Proposta di regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo **(normativa sui dati).**

- Emendamenti del Parlamento europeo, approvati il 13 dicembre 2023, alla proposta di regolamento del Parlamento europeo e del Consiglio sullo **spazio europeo dei dati sanitari**.
- Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (**normativa su un'Europa interoperabile**).
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa al rafforzamento della politica del **settore pubblico in materia di interoperabilità**: "Collegare i servizi pubblici verso un'Europa interoperabile".
- Regolamento (UE) 2018/1724del Parlamento europeo e del Consiglio, del 2 ottobre 2018, che istituisce uno **sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi**.
- **Commission staff working document on Common European Data Spaces**.
- **New Cloud Strategy.**
- 'Report on the **state of the Digital Decade**'.

Cybersecurity

- Recommendation on the security and resilience of submarine cable infrastructures.
- Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della **cibersicurezza basato sui criteri comuni (EUCC).**
- Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il **Centro europeo di competenza per la cibersicurezza nell'ambito industriale**, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.
- Relazione sulla proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza.
- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di **cibersicurezza nell'Unione**, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972.
- Regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, che stabilisce misure per un livello comune elevato di **cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione**.
- Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020.
- Relazione sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza.
- Comunicazione congiunta al Parlamento europeo e al Consiglio: **"La politica di ciberdifesa dell'UE".**
- Comunicazione congiunta al Parlamento europeo e al Consiglio: **"Piano d'azione sulla mobilità militare 2.0".**
- DIGITAL Europe - Amended **Cybersecurity Work Programme** 2023-2024 (.pdf).
- The European **Digital Infrastructure Consortium**.
- Quadro di certificazione della cibersicurezza dell'UE.

Media

- Emendamenti del Parlamento europeo, approvati il 3 ottobre 2023, alla proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno (**legge europea per la libertà dei media).**
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni: "**I media europei nel decennio digitale**: un piano d'azione per sostenere la ripresa e la trasformazione".
- Relazione sulle **prospettive dell'industria europea dei media.**

Finanza

- Risoluzione legislativa del Parlamento europeo del 22 novembre 2023 sulla proposta di direttiva del Consiglio che modifica la direttiva 2006/112/CE per quanto riguarda le **norme IVA per l'era digitale**.
- Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla **resilienza operativa digitale** per il settore finanziario.
- Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai **mercati delle cripto-attività** e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.
- Commission's legislative proposal on a **digital euro** for the EU adopted in June 2023

Protezione del consumatore e concorrenza

- Direttiva (UE) 2023/2673 del Parlamento europeo e del Consiglio, del 22 novembre 2023, che modifica la direttiva 2011/83/UE per quanto riguarda i **contratti di servizi finanziari conclusi a distanza** e abroga la direttiva 2002/65/CE.
- New **liability rules on products to protect consumers** and foster innovation.
- Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (**regolamento sui servizi digitali**)
- Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (**regolamento sui mercati digitali**)
- Emendamenti del Parlamento europeo, approvati il 21 novembre 2023, alla proposta di direttiva del Parlamento europeo e del Consiglio recante norme comuni che promuovono la **riparazione dei beni** e che modifica il regolamento (UE) 2017/2394 e precedenti direttive.
- Regolamento (UE) n. 316/2014 della Commissione, del 21 marzo 2014, relativo all'applicazione dell'articolo 101, paragrafo 3, del trattato sul funzionamento dell'Unione europea a categorie di **accordi di trasferimento di tecnologia**.