DE IUSTITIA

Rivista scientifica Maggio 2024

DIRITTO DELL'UNIONE EUROPEA ISSN 2974-7562

IL QUADRO NORMATIVO UE SULL'INTELLIGENZA ARTIFICIALE: GLI ASPETTI IN-NOVATIVI DEL NUOVO REGOLAMENTO

di **Mario BARBAJA***

ABSTRACT

Il presente contributo si propone di esaminare la Proposta di Regolamento [COM (2021) 206 final], presentata il 21 aprile 2021 dalla Commissione europea e da ultimo approvata il 13 marzo 2024 nella sua versione consolidata dal Parlamento europeo, che mira a introdurre regole armonizzate sull'Intelligenza Artificiale. La regolamentazione proposta prevede un edificio regolatorio che possa bilanciare l'innovazione tecnologica con la protezione dei diritti individuali, garantendo che le intelligenze artificiali siano utilizzate in modo etico e responsabile: questo rispecchia la consapevolezza crescente del bisogno di mettere in atto misure preventive per affrontare le sfide che potrebbero affiorare con lo sviluppo continuo dell'Intelligenza Artificiale.

Nell'arco dell'intero elaborato, si presterà, particolare attenzione, alla disciplina normativa, esaminando le disposizioni contenute nella Proposta sull'IA presentata dalla Commissione e le principali modifiche apportate; considerando che, attualmente, la formalizzazione del testo normativo si trova nelle fasi finali del processo legislativo. Prima di addentrarci nell'analisi dettagliata della disciplina, sarà svolta una premessa introduttiva sul compromesso raggiunto in sede europea in merito all'IA, mettendo in luce le nette divergenze tra il Parlamento e il Consiglio su alcune tematiche di fondamentale importanza. Successivamente, si effettuerà una necessaria disamina dei fondamenti giuridici e degli atti prodromici all'iniziativa legislativa adottata dalla Commissione, al fine di comprendere appieno il contesto di riferimento. L'analisi, si concentrerà quindi sui vari aspetti del quadro legislativo in materia, iniziando con il Titolo

I che riguarda l'oggetto, il campo di applicazione e la definizione di "sistema di Intelligenza Artificiale". Successivamente, verranno approfonditi i vari livelli

di rischio associati all'impatto delle diverse categorie di sistemi di IA classificabili in sistemi che comportano un rischio inaccettabile, un rischio alto, un rischio medio o basso.

Saranno analizzate dettagliatamente le pratiche proibite dettate dall'articolo 5 della Proposta che comportano un rischio inaccettabile, tra cui la manipolazione, lo sfruttamento di gruppi vulnerabili, il social scoring e l'uso di sistemi di identificazione biometrica a distanza.

Un ampio spazio sarà dedicato al Titolo III, che regolamenta i sistemi di IA ad alto rischio, trattando i criteri di identificazione e gli obblighi per fornitori, utenti e altri attori coinvolti nel ciclo di vita di tali sistemi. Ulteriormente, saranno esaminate le procedure di valutazione di conformità e le disposizioni relative al monitoraggio post-immissione sul mercato: questa analisi includerà gli obblighi informativi e le misure di vigilanza previste per i sistemi di Intelligenza Artificiale, nonché gli obblighi meno stringenti previsti per i sistemi a basso rischio. Infine gli ultimi due paragrafi saranno dedicati all'esame dell'assetto istituzionale delineato dal Regolamento e alle conseguenze sanzionatorie previste in caso di mancata osservanza delle misure sancite dal dettato regolamentare. In conclusione, si cercherà, senza alcuna pretesa di esaustività, di evidenziare i tratti salienti di questa nuova regolamentazione europea sull'Intelligenza Artificiale sottolineando la necessità non più rinviabile di un quadro normativo adatto a promuovere lo sviluppo dei dispositivi di IA e l'uso responsabile di tali tecnologie nell'Unione.

SOMMARIO

* Consulente in ambito *compliance e risk management* ex d.lgs. n. 231/2001 nonché abilitato all'esercizio della professione forense.

1. UNA SVOLTA STORICA: CONSIGLIO EUROPEO E PARLAMENTO SIGLANO UN ACCORDO RIGUARDANTE LE NORME ARMONIZZARE SULL'INTELLIGENZA ARTIFICIALE

Dopo ben 36 ore di estenuanti negoziati, il 9 dicembre 2023 il Consiglio ed il Parlamento europeo, nell'ambito della procedura legislativa ordinaria, hanno raggiunto un'intesa politica sull'atteso quadro normativo che disciplinerà l'Intelligenza Artificiale (*AI ACT*) e nello specifico sulla Proposta [*COM(2021) 206 final*] - (d'ora in avanti definita Proposta, Proposta di Regolamento o Proposta normativa) contenente norme armonizzate sull'Intelligenza Artificiale e di modifica di alcuni atti legislativi dell'Unione avanzata dalla Commissione il 21 aprile del 2021[1].

L'ampia portata di applicazione, la diversità e il dinamismo dell'*IA*, insieme al suo margine di imprevedibilità, opacità e autonomia rendono complesso definire un ambito regolatorio che ponderi tutti gli elementi e gli interessi coinvolti in modo efficace, pertanto è da salutare con favore lo sforzo legislativo delle Autorità Europee[2].

Le complesse negoziazioni hanno evidenziato l'enorme difficoltà nel cercare di addivenire ad un consenso tra le varie entità istituzionali[3]. Il dibattito si è polarizzato principalmente su un paio di punti significativi e nevralgici della disciplina: gli utilizzi ammessi *IA* e le pratiche vietate che comportano rischi insostenibili per l'essere umano[4].

Uno dei temi più controversi per quanto concerne gli usi ammessi, è stato l'utilizzo dell'Intelligenza Artificiale da parte delle forze dell'ordine, in particolare per quanto riguarda il riconoscimento biometrico in tempo reale e l'applicazione dei dispositivi di c.d. polizia predittiva per identificare il potenziale autore di

[1] F.META, *Intelligenza artificiale, la Ue trova la quadra. Scatta la corsa al rush finale* in www.corrierecomunicazioni.it, Corcom, 9 dicembre 2023; 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, COM(2021) 206 final del 21/4/2021; Si ricorda che il Parlamento aveva approvato, a larga maggioranza, diversi emendamenti nella seduta plenaria del 14 giugno 2023 alla Proposta di Regolamento della Commissione mentre il Consiglio in data 6 dicembre 2022 aveva adottato un orientamento generale contente la propria opinione sui singoli profili toccati dalla proposta; a tal proposito si veda M.FOTI, *AI Act: con il voto del Parlamento l'UE traccia il futuro dell'Intelligenza Artificiale,www.altalex.com*, 23 giugno 2023; M. MARTORANA,R.SAVELLA, *Intelligenza artificiale: orientamento del Consiglio europeo e ultimi sviluppi nella definizione del Regolamento, www.altalex.com*, 15 febbraio 2023.

[2] G. PROIETTI, *Intelligenza artificiale: una prima analisi della proposta di regolamento europeo in www.dirittobancario.it.*

[3] L. ZORLONI, *Con l'Ai Act l'Europa approva il primo decreto al mondo sull'intelligenza artificiale, in www.wired.it*, 9 dicembre 2023.

[4] L.ZORLONI, *I 2 ostacoli che bloccano l'accordo sull'AI Act, il regolamento europeo sull'intelligenza artificiale* in www.wired.it, 4 dicembre 2023.

una condotta illecita e il luogo di consumazione del reato. Il Parlamento Europeo si è opposto con fermezza all'utilizzo di queste applicazioni, mentre il Consiglio, in virtù della necessità di potenziare le condizioni di sicurezza interne agli Stati, si è mostrato pienamente favorevole. Durante le negoziazioni, 60 accademici e ricercatori nel campo della privacy e dei diritti digitali hanno condiviso la posizione del Parlamento, scrivendo una lettera che esortava l'Organo Legislativo a non cedere sui divieti relativi all'utilizzo dell'Intelligenza Artificiale.

Un altro profilo di tensione, nel quale si è evidenziata una diversità di posizioni tra le due Istituzioni, ha riguardato i sistemi generativi ossia quelle tecnologie capaci di riprodurre nuovi contenuti ed addestrate attraverso un'enorme mole di dati. Sul punto, i due co-legislatori hanno adottato una logica dualistica, focalizzandosi, in primo luogo, sulle intelligenze artificiali ad alto impatto (come *GPT-4* di *Open AI*) richiedendo agli sviluppatori adeguamenti formali preliminari ed, in secondo luogo, invece, imponendo per gli altri modelli fondamentali meno dirompenti la sola conformità agli standard regolamentari al momento dell'ingresso sul mercato.

Il varo della normativa sull'Intelligenza Artificiale rappresenta una pietra miliare nel contesto giuridico globale[5]. Da un lato, la nuova regolamentazione euro-unitaria si impegna a preservare i diritti fondamentali, la democrazia e lo stato di diritto, nonché a puntellare la sostenibilità ambientale. Dall'altro, si propone di stimolare l'innovazione e di posizionare l'Europa al centro di un settore così impattante, il quale ha già notevolmente permeato la vita quotidiana di tutti destando non solo stupore ma anche dubbi e incertezze sul piano applicativo. In futuro, ed è in questa prospettiva che si pongono le novità regolatorie del Regolamento, ci si aspetta che tale settore acquisisca sempre maggiore importanza, diventando il perno principale dell'economia mondiale. La Presidente del Parlamento Europeo Roberta Metsola definisce pionieristico l'accordo siglato in quanto garantisce una sorta di legislazione responsabile e all'avanguardia. Allo stesso modo, Ursula Von Der Leyen, Presidente della Commissione europea, afferma che questa regolamentazione fa acquisire all'Europa una posizione di *leadership* industriale e tecnologica[6]. L'ambizione, neanche troppo velata delle Istituzioni Europee, è che le esigenze del mercato possano indurre anche potenze con regolamentazioni differenti ad allinearsi alla disciplina normativa che l'Unione Europea sta tratteggiando. L'idea di fondo che sta dietro al raggiungimento di questo accordo preliminare è quella di garantire che i dispositivi di Intelligenza Artificiale immessi sul mercato europeo siano sicuri e rispettino i diritti fondamentali e i valori dell' Unione, tanto è vero che il testo così come è stato approvato distingue i prodotti "intelligenti" che sono suscettibili di causare gravi danni o comunque di innescare rischi significativi da quelli che invece non hanno nessuna ricaduta. In questo senso il quadro normativo in oggetto definisce una scala di rischio nella quale le pratiche e gli impieghi di *IA* vengono classificati sulla base di diversi livelli di rischio: da sistemi di Intelligenza Artificiale caratterizzati da un rischio inaccettabile, a un rischio alto, fino a un rischio basso o minimo. Questa normativa parte dal presupposto che l'impiego dell'Intelligenza Artificiale possa comportare rischi per i diritti, difatti mira, a instaurare un controllo umano solido sull'Intelligenza Artificiale, impedendo

[5] *Intelligenza artificiale, l'Ue approva la prima normativa al mondo in* www.euronews.com, *Euronews*, 9 dicembre 2023.

[6] La proposta della Commissione è correlata ad un Piano di investimenti e ad un Piano di innovazione tecnologica (Coordinated Plan on Artificial Intelligence 2021 Review (COM[2021] 205 final); Per una panoramica circa l'orientamento politico dell'UE per fronteggiare le sfide future dettate dall' *IA* si faccia riferimento alla Comunicazione della Commissione(COM[2021]), al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Promuovere un approccio europeo all'intelligenza artificiale, 24/4/2021.

che essa sfugga completamente dal dominio umano e si traduca in scelte pregiudizievoli.

Tuttavia, si muove, altresì, nella ferma convinzione che non si debba sopravvalutare il fattore rischio, al fine di non ostacolare lo sviluppo di una tecnologia decisiva per la competitività del mercato interno.

Pertanto, si è cercato di conciliare queste due esigenze opposte, ovvero caldeggiare lo sviluppo dei sistemi di Intelligenza Artificiale e contenere il rischio, attraverso una disciplina teleologicamente orientata a ricondurre l'Intelligenza Artificiale a una dimensione antropocentrica. Alla luce di questo scenario, consapevole dell'importanza sempre più significativa nel panorama globale di questo settore, l'Unione Europea, sfruttando le dinamiche del mercato, si propone di dominare e plasmare gli sviluppi futuri delle tecnologie legale all'*IA.*

L'accordo preliminare, come si evince, riconoscendo l'importanza della protezione dei diritti umani si propone di equilibrare lo sviluppo tecnologico con la tutela delle libertà fondamentali mediante dei presidi normativi volti a minimizzare i rischi associabili all'uso dell'Intelligenza Artificiale. In base a questa prospettiva, la normativa è proiettata a prevenire le violazioni dei diritti fondamentali e ad assicurare, al contempo, il controllo umano sull'Intelligenza Artificiale. Il pacchetto normativo sull'*IA*, concordato dai negoziatori delle due Istituzioni, a seguito della lunga gestazione, rispetto alla primigenia Proposta, include vari aspetti di rilievo: nuove disposizioni sui modelli di di *IA* a carattere generale ad alto impatto; ridistribuzione dei poteri a livello istituzionale, con una maggiore centralizzazione a livello sovranazionale delle decisioni esecutive; introduzione di nuove pratiche vietate legate all'*IA*; precisazioni in ordine alle situazioni nelle quali l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico si rende strettamente necessario per il contrasto alla criminalità; valutazione d'impatto prima di attivare un sistema di Intelligenza Artificiale[7].

Venendo più nel dettaglio, il presente contributo intende esaminare le principali novità introdotte nell' accordo di compromesso, confermate tra l'altro, nella recente approvazione parlamentare del 13 marzo 2024, per, poi, successivamente, nel prosieguo della trattazione, affrontare gli elementi più significativi dell'iniziativa legislativa adottata dalla Commissione.

Con riferimento alla nozione di *IA* l'accordo allineandosi all'approccio tenuto in materia dall'Ocse, definisce un sistema di *IA* "*un apparato basato su macchina progettato per funzionare con diversi livelli di autonomia che, può mostrare capacità di adattamento dopo l'implementazione e che per obiettivi espliciti o impliciti, deduce dagli input ricevuti come generare output come previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*"[8]. Questa definizione ha il pregio di enunciare dei criteri sufficientemente chiari per distinguere l'*IA* da sistemi software più semplici.

Pertanto assumono rilevanza ai fini della cornice normativa sull' *IA* tutti quei sistemi che devono: 1) essere basati su dispositivi computazionali capaci di generare output, e che siano progettati con diversi livelli di autonomia, in grado di operare anche senza l'ausilio umano; 2) disvelare una grande capacità di adattamento e una notevole capacità di apprendimento che consente loro di evolversi durante l'uso; 3) essere indirizzati alla risoluzione di obiettivi espliciti e impliciti ; 4) essere in grado di dedurre gli output dagli input ricevuti ; 5) essere

[7] D.MAISTO, *Ai act gli impatti dell'accordo sull'intelligenza artificiale*, Qui finanza, 12 dicembre 2023.
[8] B. CALDERINI, *Ai Act, il punto sui risultati raggiunti e i dubbi sul futuro in www.agendadigitale.eu*, Agenda Digitale, 12 dicembre 2023; si veda *Raccomandazione del Consiglio dell'Organizzazione per la cooperazione e lo sviluppo economici (OCSE), del 22 maggio 2019, sull'Intelligenza Artificiale*.

in grado di interagire con l'ambiente circostante e influenzarlo[9].

La bozza di Regolamento è stata poi innervata da disposizioni che riguardano sia l'utilizzo dei sistemi di Intelligenza Artificiale (*IA*) per finalità generali, sia le tecnologie con scopi generali annesse ad altri sistemi ad alto rischio[10]. Sono state poi introdotte, regole sulla trasparenza per i grandi sistemi, che attraverso l'immissione di grandi quantità di dati, sono in grado di svolgere con competenza una varietà di compiti (modelli informatici di base ad un suo generale) ivi inclusa la creazione di contenuti e configurati regimi giuridici più restrittivi per i modelli di base addestrati con grandi quantità di dati in grado di svolgere prestazioni avanzate ben al di sopra della media e che possono alla luce di queste potenzialità diffondere rischi sistemici (modelli informatici di base "ad alto impatto"). In tale ottica vengono classificati come sistemi a rischio sistemico quei modelli che presentano un impatto significativo sul mercato interno a causa della loro portata e con effetti negativi reali o ragionevolmente prevedibili su salute pubblica, sicurezza, diritti fondamentali o sulla società nel suo insieme, che possono essere propagati su larga scala lungo tutta la catena del valore[11].

Per quanto attiene alla *governance*, è stato istituito presso la Commissione un Ufficio per l'*IA* con compiti di supervisione dei sistemi di Intelligenza Artificiale, di monitoraggio, di direzione e di controllo sulla corretta applicazione da parte dei soggetti incisi delle disposizioni normative contenute nel Regolamento[12]. Inoltre, ai fini di una visione sistemica ed olistica sull'*IA*, quest'organo sarà affiancato da un gruppo scientifico di esperti, rappresentanti delle varie componenti della società civile che agirà come organo consultivo. Per di più, è stato istituito un forum consultivo dalla composizione mista che avrà il compito di fornire competenze tecniche al Comitato tecnico sull'*IA* ed alla Commissione, [13].

In considerazione della capacità lesiva dell'Intelligenza Artificiale, il nuovo testo rivisto prevede che i fornitori debbano svolgere una valutazione d'impatto del sistema di *IA* prima che lo stesso venga inserito nel circuito economico.

L'accordo provvisorio riconoscendo ancor di più rispetto alla Proposta della Commissione il primato dell'essere umano sulla tecnologia amplia il novero delle pratiche di *IA* vietate: assume rilievo il divieto di riconoscimento delle emozioni mediante l'utilizzo di Intelligenza Artificiale in ambienti lavorativi e nelle istituzioni educative; è vietata l'acquisizione massiva e indiscriminata di immagini facciali provenienti da internet, piattaforme social o registrazioni di telecamere; è istituito il divieto della cosiddetta "polizia predittiva" ovvero non si potrà avviare un'indagine penale a carico di un individuo basandosi unicamente sulle

[9] I.DE FEO e A.AFFERNINI, *Ai Act: il Regolamento sull'Intelligenza Artificiale adottato dal Parlamento UE* in *www.dirittobancario.it.*

[10] *Raggiunto l'accordo politico sull'Artificial Intelligence Act* in *www.federprivacy.it*,11 dicembre 2023; Il testo normativo, recentemente approvato dal Parlamento in data 13 marzo, espone in modo minuzioso gli obblighi di trasparenza in capo ai fornitori sia per i modelli di base generici che per quelli a rischio sistemico. Riguardo ai primi, i fornitori devono: garantire la disponibilità di una documentazione esaustiva che descriva chiaramente il funzionamento dei sistemi; fornire un elenco dettagliato dei contenuti utilizzati per l'addestramento del sistema; designare un rappresentante autorizzato per interagire con le autorità competenti. Per quanto riguarda, invece, i modelli a rischio sistemico, i fornitori devono: condurre una valutazione del modello mediante strumenti all'avanguardia ed in accordo ai protocolli standardizzati; individuare e attenuare eventuali rischi sistemici che potrebbero sorgere a livello dell'Unione Europea per lo sviluppo, l'immissione sul mercato o l'uso di tali modelli; registrare e notificare tempestivamente alle autorità competenti eventuali incidenti gravi congiuntamente alle misure correttive adottate; garantire un adeguato livello di sicurezza informatica per il modello e le relative infrastrutture; adottare codici di condotta per comprovare il rispetto degli obblighi imposti. Si vedano gli emendamenti alla proposta di *AI Act* del Parlamento europeo approvati il 13 marzo 2024.

[11] Per una migliore comprensione del tema, si suggerisce di fare riferimento agli emendamenti alla Proposta di AI Act del Parlamento europeo approvati il 13 marzo 2024.

[12] *Raggiunto l'accordo politico sull'Artificial Intelligence Act* in www.federprivacy.it,11 dicembre 2023.

[13] D.MAISTO, op. cit., *Qui finanza*, 12 dicembre 2023.

indicazioni fornite dai sistemi di Intelligenza Artificiale, tuttavia sarà possibile utilizzare i sistemi di analisi dei reati che operano su informazioni anonimizzate, al fine di fornire tendenze sulla scena criminale.

Tra le novità introdotte nel testo di compromesso, si osserva, infine, un inasprimento delle sanzioni rispetto a quanto previsto nella Proposta originale della Commissione. In particolare, le nuove soglie edittali sono le seguenti: per le violazioni delle pratiche vietate stabilite dall'*AI Act*, le sanzioni possono arrivare fino a 35 milioni di euro o al 7% del fatturato mondiale annuo dell'anno precedente; per le violazioni di altri obblighi e requisiti stabiliti dalla stessa legge sull'Intelligenza Artificiale, le sanzioni possono raggiungere fino a 15 milioni di euro o al 3% del fatturato mondiale annuo dell'anno precedente; per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità competenti, la sanzione può essere fino a 7,5 milioni di euro o all'1% del fatturato mondiale annuo dell'anno precedente[14]. Per quanto riguarda l'iter normativo, dopo l'intesa raggiunta in esito alle negoziazioni interistituzionali, il testo è stato inizialmente sottoposto al *Coreper* e, successivamente, è stato approvato con una votazione "quasi plebiscitaria" (con 523 voti favorevoli, 46 contrari e 49 astenuti) lo scorso13 marzo 2024 dal Parlamento europeo. Sul punto, occorre evidenziare che, dalla disamina della recente versione approvata dell'*AI ACT*, si evince un quadro sistemico che conferma l'impostazione di fondo introdotta nel disegno di legge della Commissione europea, unitamente al correlato approccio regolativo basato sul rischio. Tornando al percorso normativo attualmente in corso, in seguito, il testo approvato in sede parlamentare richiederà, prima della sua adozione definitiva, l'avallo formale, a norma del procedimento legislativo UE, da parte del Consiglio[15]. Tuttavia, il Regolamento dispiegherà i suoi effetti dopo due anni dalla sua entrata in vigore, ad eccezione dei divieti, i quali avranno effetto dopo 6 mesi, e delle norme inerenti l'uso dell'Intelligenza Artificiale per scopi generali, che produrranno effetto dopo 12 mesi[16].

2. BREVE EXURSUS STORICO SULLA GENESI DELLA NUOVA DISCIPLINA IN MATERIA DI IA

Prima che la Commissione europea formulasse una Proposta normativa inerente un apposito assetto giuridico sull' *IA,* nell'ordinamento comunitario alle decisioni automatiche assunte attraverso l'impiego di sistemi di intelligenza Artificiale poteva essere applicato quanto disposto dal Regolamento Generale sulla protezione dei dati (2016/679) con riguardo ai processi automatizzati[17]. Sul punto, la previsione normativa dell'art 22 Reg. (UE) 2016/679 dispone che l'interessato ha il diritto di non essere assoggettato unicamente ad una decisione fondata esclusivamente sul trattamento automatizzato compresa la profilazione[18] che produca decisioni capaci di

[14] I.DE FEO e A. AFFERNINI, op. cit., *in www.dirittobancario.it.*
[15] L. DI GIACOMO, *Regolamento europeo sull' ia (ai act): il testo aggiornato al 21 gennaio, Diritto europeo e internazionale,22 gennaio 2024*; Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
[16] *Ai Act 2023: accordo sul nuovo Regolamento Ue sull'intelligenza artificiale* in www.dirittobancario.it, non solo diritto bancario, 14 dicembre 2023; Per superare questo biennio di stallo del Regolamento la Commissione intende proporre un "Patto per l'IA con lo scopo di convogliare gli sviluppatori europei e internazionali, che prima della sua effettiva attuazione vogliano su base volontaria impegnarsi ad attuare le norme cogenti del nuovo assetto normativo, si veda *Plasmare il futuro dell'Europa* in www.digitalstrategy.ec.europa.eu.
[17] A. LONGO e G. SCORZA. *Intelligenza artificiale. L'impatto sulle nostre vite, diritti, libertà,* Milano, 2020, p. 206 e ss.
[18] Per profilazione deve intendersi ai sensi dell' art. 4 n. 4 del Regolamento (UE) 2016/679: «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il

generare effetti giuridicamente rilevanti o che incidano in modo equipollente sulla sua persona. La vigente disciplina europea in materia di privacy, tenendo conto del potenziale margine di errore e delle possibili inesattezze nelle indicazioni dei sistemi di Intelligenza Artificiale, non proibisce le decisioni automatizzate, ma richiede che le determinazioni non siano prese senza un ravvisabile coinvolgimento umano, a meno che non si rientri nelle eccezioni di utilizzo stabilite nell'articolo 22 del Reg. (*UE*) n.2016/679 relative alle ipotesi in cui il trattamento automatizzato dei dati sia necessario per la conclusione o l'esecuzione di un contratto, sia autorizzato dal diritto dell'Unione o di uno Stato membro o si basi sul consenso esplicito dell'interessato.

La disposizione richiamata al comma 3 prescrive tra l'altro al titolare del trattamento, nel caso in cui vengano adottati procedimenti decisionali automatizzati, compresa la profilazione, l'obbligo di adottare "misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato".

La peculiare forza propulsiva dell'*IA* e la sua diffusione capillare in ogni ambito della vita umana hanno indotto il legislatore ad introdurre una disciplina specifica, disgiunta dalla normativa sulla protezione dei dati personali, la quale si rivela non più compatibile con l'urgenza dei problemi da affrontare e non più idonea a cogliere le nuove opportunità.

L'inadeguatezza del quadro normativo descritto, in precedenza, ha stimolato il Regolatore a riannodarsi su due principali aree di intervento : la prima connessa alla novella di diverse disposizioni attualmente in vigore, in particolare in materia di sicurezza dei prodotti e di protezione dei dati personali; la seconda volta alla costituzione di un apparato normativo di carattere tecnico relativo alla fase di addestramento dei sistemi di intelligenza artificiale, alla tenuta dei dati e dei registri, alla trasparenza e alla precisione degli stessi sistemi ed alla sorveglianza umana[19].

Come precedentemente enunciato, si evidenzia a livello comunitario un innovativo impegno, volto all'inserimento in seno alla Legislazione Europea di una disciplina organica ed unitaria sull'*IA* che possa diventare un cogente punto di riferimento per le altre legislazioni degli Stati membri e un prototipo normativo cui ispirarsi per i paesi extra Ue. Pertanto, la scelta del legislatore europeo cade in modo inequivocabile sul Regolamento, quale strumento legislativo immediatamente applicabile, uniforme su tutto il territorio dell'Unione Europea e insuscettibile di adattamenti a livello nazionale[20]. Com'è noto, il Regolamento ai sensi dell'art 288 TFUE è l'atto di diritto derivato sovranazionale che produce direttamente effetto negli Stati membri senza che sia necessario alcuna misura di recepimento a differenza della Direttiva che vincola gli Stati membri a realizzare gli scopi in essa previsti entro una scadenza temporale [21]. La preferenza accordata al Regolamento anziché alla Direttiva è in linea con l'adozione effettuata anteriormente dal Legislatore con il Regolamento 2016/679 in materia di protezione dei dati personali[22].

Il principale obiettivo della normativa è regolare l'accesso dei prodotti di Intelligenza Artificiale al mercato comune europeo, concentrandosi, in particolare, sugli utilizzi

rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

[19] N.ABRIANI e G.SCHNEIDER, *Diritto delle imprese e intelligenza artificiale, Dalla Fintech alla Corptec,* Bologna , Editore il Mulino, p.145.

[20] A. PAJNO, F.DONATI, A.PERRUCCI*, Intelligenza artificiale e diritto: una rivoluzione? << Diritti Fondamentali, Dati Personali e Regolazione Vol.1 >>,* Bologna , Editore il Mulino, p. 217.

[21] G. TESAURO, *Diritto dell'Unione Europea, settima edizione*, Cedam,2012,p.139 e ss.

[22] C. SCHEPISI*, Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione* in www.aisdue.eu, 28 marzo 2022,p.7.

considerati più a rischio, ovvero quegli usi dell'*IA* che potrebbero lambire il catalogo dei diritti fondamentali enunciati nella Carta di Nizza [23]. Parimenti, vengono identificati e proibiti quei specifici impieghi dell'Intelligenza Artificiale correlati ad un rischio insostenibile[24]. A tal riguardo è importante rilevare che il Legislatore nel disciplinare l'*IA* adotta una tecnica regolativa incentrata sulla significatività del rischio: in cui tenta di minimizzare i pregiudizi più rilevanti per i diritti fondamentali[25] delle persone fisiche derivanti dall'uso dei sistemi di *IA* mediante norme di natura procedimentale idonee ad accertare, prevenire e ridurre il rischio[26]. Inoltre, a ciò si aggiunga che in tale modello normativo, si prevede una distribuzione delle responsabilità graduata al concreto rischio connesso alle attività poste in essere dai principali attori della filiera produttiva dell'*IA*. A questo punto della trattazione, sorge l'obbligo però di condurre un'analisi storica, completa ed esaustiva, sul percorso che ha portato i due co-legislatori europei, ossia il Parlamento e il Consiglio, e la Commissione come iniziale istante, a negoziare reciprocamente e a giungere a un'intesa sull'*IA.*

Tutto ha inizio il 21 aprile 2021, quando la Commissione Europea presenta al Consiglio europeo ed al Parlamento una Proposta di Regolamento sull'Intelligenza Artificiale, un documento composto da 85 articoli, disseminati in 12 Titoli, preceduti da 89 considerando. A completamento del testo, sono stati redatti 9 allegati [27]. L'atto proposto dalla Commissione si fonda su due basi giuridiche: l'articolo 114 del TFUE e l'articolo 16 TFUE[28]. L'articolo 114 TFUE conferisce alle istituzioni dell'Unione Europea la competenza per adottare misure di ravvicinamento delle normative nazionali che influiscono sul funzionamento o sull'instaurazione del mercato comune. Parallelamente, l'articolo 16 TFUE attribuisce alle istituzioni il potere di adottare norme relative alla protezione delle persone in relazione al trattamento dei dati personali. La scelta di questi due fondamenti normativi evidenzia la duplice finalità dell'atto normativo prescelto: promuovere l'armonizzazione normativa per il corretto funzionamento del mercato comune e garantire la protezione delle persone in un contesto europeo in cui si vuole progressivamente liberalizzare la circolazione

[23] A. ALAIMO, *Il Regolamento sull'intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico*? *In www.federalismi.it,* 18 Ottobre 2023, p.4.

[24] C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di Intelligenza artificiale, in Biolaw Journal*, 2021.

[25] Diritti fondamentali quali la dignità umana, la libertà, l'uguaglianza, la democrazia, il diritto alla non discriminazione, alla protezione dei dati, la salute, la sicurezza, etc.

[26] P. LOI, *Il rischio proporzionato nella proposta di regolamento sull'IA e i suoi effetti nel rapporto di lavoro*, *in* F*ederalismi*, n.4, 2023.

[27] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, *Il regolamento europeo sull'intelligenza artificiale Analisi informatico- giuridico in www.i-lex.it*, Dicembre 2021,p.7; E' da segnalare che per la presentazione del quadro normativo sull'*IA*sono state condotte ampie consultazioni con i portatori di interessi. Nella proposta sono riportati i contributi ricevuti dai vari portatori di interesse "*sono pervenuti 1 215 contributi, di cui 352 da imprese od organizzazioni/associazioni di imprese, 406 da persone fisiche (92 % persone fisiche dell'UE), 152 a nome di istituzioni accademiche/di ricerca e 73 da autorità pubbliche. I pareri della società civile sono stati rappresentati da 160 partecipanti (tra cui 9 organizzazioni di consumatori, 129 organizzazioni non governative e 22 sindacati); 72 partecipanti hanno invece contribuito classificandosi come "altri". Dei 352 rappresentanti di imprese e dell'industria, 222 sono stati imprese e rappresentanti di imprese, il 41,5 % delle quali apparteneva alla categoria delle micro, piccole e medie imprese. Nel resto dei casi si è trattato di associazioni di imprese. Complessivamente l'84 % delle risposte ricevute da imprese e dall'industria è pervenuto dall'UE-27. A seconda della domanda, tra 81 e 598 partecipanti hanno utilizzato l'opzione di testo libero per inserire osservazioni. Oltre 450 documenti di sintesi sono stati presentati tramite il sito web EUSurvey, in aggiunta alle risposte al questionario (oltre 400) oppure sotto forma di contributi indipendenti (oltre 50)".*

[28] A. PAJNO, F.DONATI, A.PERRUCCI, op. cit., Bologna , Editore il Mulino, pp 135 e ss; 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 (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 (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.

dei dati. Questo ambizioso progetto normativo, giunto quasi al termine con l' approvazione del Parlamento Europeo del 13 marzo 2024, rappresenta una tessera all' interno di un mosaico più ampio, nel quale si inserisce la c.d. Agenda Digitale Europea la quale comprende non solo il Regolamento in questione, ma anche altri importanti atti legislativi come il *Digital Service Act* (normativa europea sui servizi digitali), il *Digital Market Act* (normativa europea sui mercati digitali) e il *Data Governance Act* (normativa in materia di trattamento dei dati personali). L' obiettivo congiunto di tali discipline è favorire lo sviluppo del mercato unico digitale, per agevolare la crescita e il progresso economico[29].

Accanto a questi assetti normativi, si pone l'iniziativa della Commissione Europea che si incastona, a sua volta, nell'ambito di una serie di atti di impulso programmatici sull'*IA*[30]. Tra di essi, spiccano le risoluzioni del Parlamento europeo, adottate il 20 ottobre 2020, che affrontano i principi etici dell'Intelligenza Artificiale (*IA*)[31], della robotica[32] e delle tecnologie correlate, oltre al regime di responsabilità civile per l'*IA*[33]. Ulteriori risoluzioni più recenti sull'uso dell'*IA* datate 20 gennaio 2021[34], che hanno ulteriormente arricchito questo multiforme contesto. In merito all'antropocentrismo dell'IA, si segnala la Comunicazione della Commissione europea del 2019 intitolata "*Creare fiducia nell'Intelligenza Artificiale antropocentrica*"[35]. Inoltre non si può non menzionare la pubblicazione nel 19 febbraio 2020 del Libro Bianco sull'Intelligenza Artificiale[36] con il quale la Commissione ha dettato delle indicazioni per un approccio specifico nell'ambito dell'Intelligenza Artificiale volto a combinare l'eccellenza e la fiducia. Infine, un contributo, altrettanto significativo, è emerso dal lavoro svolto *dall'High-Level Expert Group on AI* e dalle linee guida elaborate datale gruppo in materia di affidabilità dell'*IA*[37]. Tornando al progetto normativo proposto dalla Commissione, questo si staglia nell'orizzonte comunitario con lo scopo ambizioso di posizionare l'Unione Europea, come leader indiscussa nel settore dell'Intelligenza Artificiale in un contesto globale caratterizzato dalla sostanziale assenza di discipline organiche[38]. Dietro questa esplicita volontà vi è la spinta derivante da diversi soggetti istituzionali in seno all'UE di voler affermare mediante questa regolamentazione una sovranità digitale. Alla luce di ciò, va ricordato che, parallelamente al processo legislativo

[29] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., in www.i-lex.it, Dicembre 2021, p.4.
[30] C. CASONATO, B. MARCHETTI, op. cit., in *Biolaw Journal*, 2021.
[31] Risoluzione del Parlamento europeo del 20/10/2020 recante
Raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012 [INL]; In tale contesto merita di essere segnalata anche la Risoluzione del 20/10/2020 sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di tecnologie di intelligenza artificiale, 2020/2015 (INI).
[32] Risoluzione del 2018/C 252/25, recante Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL).
[33] Il Parlamento europeo ha approvato una risoluzione recante Raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014 [INL]); Si veda, tra l'altro, la Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di
sicurezza e di responsabilità, adottata dalla Commissione il 19/2/2020, COM[2020] 64 def.
[34] Risoluzione del Parlamento europeo del 19 maggio 2021 sull'intelligenza artificiale nell'istruzione, nella cultura e nel settore audiovisivo (2020/2017(INI)); Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)).
[35] COMMISSIONE, Comunicazione dell'8 aprile 2019 rubricata "Creare fiducia nell'intelligenza artificiale antropocentrica" (COM (2019) 168).
[36] COMMISIONE EUROPEA, Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia (COM(2020) 65 final).
[37] C. CASONATO, B. MARCHETTI, op. cit., in Biolaw Journal, 2021; Si veda il Draft Ethics Giudelines for Trustworthy AI (Orientamenti etici per un'IA affidabile) predisposto dall'High Level Expert Group on Artificial Intelligence della Commissione Europea del 18 dicembre 2018 (The European Commission's High Level Expert Group on Artificial Intelligence).
[38] G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale* in Rivista Trimestrale di diritto pubblico *Anno LXXII, Fasc.4, 2022, p.6.*

sull'*IA*, la Commissione europea e gli Stati membri hanno lanciato nel dicembre 2018 un Piano coordinato sull'Intelligenza Artificiale, con il precipuo 'obiettivo non solo di massimizzare l'impatto degli investimenti, ma anche di potenziare la collaborazione e la cooperazione reciproca[39]. In questo contesto, l'introduzione normativa e l'affermazione sul piano regolatorio, costituiscono anche una risposta ai timori della crescente competitività da parte di nazioni come la Cina e gli Stati Uniti[40], che hanno allocato ingenti risorse finanziarie in questo campo. L'articolata disciplina sull'*IA*, rappresenta, da ultimo, una reazione normativa all'eterogeneità regolamentare esistente tra gli Stati europei nell'affrontare le problematiche derivanti dall'applicazione dell'Intelligenza Artificiale[41]. A fronte di ciò la Proposta di Regolamento, articolata e robusta, fissa un assetto normativo omogeneo che possa governare in maniera uniforme le questioni normative legate a questa tecnologia emergente. Il sistema delineato risente di un elevato tasso di tecnicità nonché dell'imprescindibile esigenza di contemperare una pluralità di interessi spesso tra loro confliggenti. La Proposta, nell'ottica di voler essere al passo con l'incessante divenire imposto del mercato globale, vuole creare uno spazio normativo che, incentivando le imprese ad investire nell'innovazione tecnologica, agevoli lo sviluppo di prodotti legati all'intelligenza. Questo implica la nascita di un sostrato normativo che faciliti il riconoscimento e la valorizzazione delle innovazioni basate sull'*IA* in tutto il territorio dell'Unione Europea.

Dalle indicazioni emerse circa la sconfinata mole di opportunità e di criticità derivanti dall'implementazione dell'Intelligenza Artificiale, la Commissione si è posta una serie di obiettivi[42]. Questi includono garantire la sicurezza dei sistemi immessi sul mercato, rispettare la legislazione esistente sui diritti fondamentali e i valori dell'Unione, assicurare la certezza del diritto per favorire gli investimenti e l'innovazione nell'ambito dell'Intelligenza Artificiale, migliorare la *governance* e l'effettiva applicazione delle leggi esistenti sui diritti fondamentali e sui requisiti di sicurezza applicati ai sistemi di *IA*, agevolare lo sviluppo di un mercato unico e prevenirne la frammentazione[43]. Al fine di raggiungere tali obiettivi, il legislatore adotta, all'interno della cornice normativa, un approccio regolatorio proporzionato all'Intelligenza Artificiale (IA), che si limita ai requisiti minimi necessari per gestire i rischi e le problematiche riconducibili ad essa, senza imporre eccessivi ostacoli allo sviluppo tecnologico e senza aumentare spropositatamente i costi di commercializzazione degli algoritmi di *IA*[44]. Sulla scorta di questa prospettiva, la

[39] COMMISSIONE, Piano coordinato sull'intelligenza artificiale licenziato il 7 dicembre del 2018 COM (2018) 237; Inoltre, in risposta alla pubblicazione della Strategia europea sull'IA, è stato proposto nel 2021 un Nuovo Piano coordinato sull'intelligenza artificiale, che aggiorna il precedente Piano, presentato nel dicembre 2018.

[40] C. CASONATO, B. MARCHETTI, op. cit., *in Biolaw Journal*, 2021; Si vedano, a tal riguardo, l' Executive Order n.13859 intitolato "Maintaining American Lea dership in Artificial Intelligence" emanato l'11 febbraio 2019 dal Presidente degli Stati Uniti, l' Executive Order presidenziale n.13960 del 3 dicembre 2020, rubricato "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government" e l'Executive Order (n. 14110) del 30 ottobre 2023 sulla Safe, Secure, and Trustworthy Artificial Intelligence (decreto per un'intelligenza artificiale sicura e affidabile); Per quanto riguarda la politica normativa della Cina in materia di IA, la Cyberspace Administration of China, ente responsabile della supervisione della rete internet, ha pubblicato il 13 Luglio 2024 una serie di linee guida per regolamentare il settore dell'intelligenza artificiale generativa, le cd. "Misure provvisorie per la gestione dei servizi di intelligenza artificiale generativa", promulgate il 10 luglio 2023 ed entrate in vigore il successivo 15 agosto 2023.

[41] *G.* MARCHIANO', *Proposta di Regolamento della Commissione europea del 21 aprile 2021 sull'Intelligenza artificiale con particolare riferimento alle IA ad alto rischio* in www.ambientediritto.it, Cyberlaws, 2021,p.6.

[42] COM/2021/206 final, https://eur-lex.europa.eu.

[43] Solo una normativa avente una dimensione europea è appropriata per evitare la formazione di quello che la Proposta di regolamento apostrofa come "*un mosaico di norme nazionali*" che potrebbero ostacolare la circolazione dei prodotti e dei servizi di intelligenza artificiale con conseguente rischio per la sicurezza e la tutela dei diritti fondamentali, si veda COM/2021/206 final, https://eur-lex.europa.eu.

[44] COM/2021/206 final, https://eur-lex.europa.eu.

Commissione sviluppa un'impalcatura normativa proporzionata incentrata su un approccio basato sul rischio (*risk based approach*) che non crea restrizioni inutili al commercio, motivo per cui l'intervento normativo è adattato alle situazioni concrete in cui sussiste una preoccupazione "di rischio" giustificato o nelle quali tali preoccupazioni "di rischio" può essere ragionevolmente prevista. Allo stesso modo, include nell' assetto normativo sull'*IA* meccanismi flessibili, come vedremo, che consentono un continuo aggiornamento del dato normativo in ragione della repentina evoluzione tecnologica in grado di dischiudere scenari di volta in volta diversi. Deve essere, inoltre, evidenziata la coerenza dell'impianto normativo con le altre normative vigenti applicabili ai settori nei quali i sistemi di *IA* ad alto rischio sono già utilizzati o saranno probabilmente utilizzati in un prossimo futuro[45]. I profili su cui la normativa si concentra e che vivisezionerò sono molteplici, ma sicuramente tra i più rilevanti si annoverano: la definizione di *IA*; le pratiche di Intelligenza Artificiale bandite per il loro potenziale rischio in considerazione dell'approccio antropocentrico perseguito; i sistemi ad alto rischio ammessi sul mercato subordinatamente al rispetto di determinati requisiti previsti *ex ante* e di una valutazione di conformità; l'istituzione delle cosiddette '*sandboxes*'; infine, le previsioni concernenti il sistema di *governance*."

3. *L'AMBITO DI APPLICAZIONE SOGGETTIVO E OGGETTIVO*

Dopo aver sottolineato la logica sottesa all'iniziativa legislativa bisogna passare in rassegna gli aspetti essenziali della disciplina normativa in materia di *IA*. Occorre partire, in *primis*, dall'esame dell'ambito di applicazione soggettivo della disciplina per poi affrontare in un secondo momento il versante oggettivo di applicazione. L'articolo 2 del Regolamento sull'*IA* disciplina il perimetro di applicazione soggettiva del Regolamento, stabilendo i soggetti impattati da quest'ultimo[46]. La norma ha una valenza extraterritoriale in quanto non mira a raggiungere i soli programmatori, sviluppatori, produttori e fornitori situati in Paesi europei ma si focalizza sulla localizzazione del prodotto facendo riferimento a tutti i sistemi di Intelligenza Artificiale che generano un *output* con effetti nel territorio dell'Unione Europea. Questa soluzione definitoria onnicomprensiva, che coinvolge anche soggetti esterni all'Unione, è concepita per includere nello spettro normativo del Regolamento tutte le tecnologie basate sull'Intelligenza Artificiale che producono effetti nell'Unione Europea. Alla luce di quanto detto, emerge la *ratio* sottesa a questa misura protettiva che è quella di prevenire l'introduzione e la commercializzazione nel mercato unionale di sistemi di Intelligenza Artificiale esteri con caratteristiche aliene alla normativa dell'UE che potrebbero rilevarsi pericolosi per la cittadinanza.

Esaminando le definizioni soggettive ai sensi della presente disposizione, emergono come principali figure il fornitore (*provider*), definito come qualsiasi entità, fisica o giuridica, che introduce sul mercato a titolo oneroso o

[45] Nel quadro normativo sull'*IA*: viene garantita la coerenza con la Carta dei diritti fondamentali dell'Unione europea e con il diritto derivato dell'UE in vigore per quanto riguarda la protezione dei dati, la tutela dei consumatori, la non discriminazione e la parità di genere; non vengono meno le disposizioni del regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) e della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva (UE) 2016/680), bensì vengono integrate con una serie di disposizioni armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di specifici sistemi di IA ad alto rischio, nonché con restrizioni relative a specifici utilizzi dei sistemi di identificazione biometrica remota; si integrano gli atti normativi dell'Unione n vigore in materia di non discriminazione, con requisiti specifici mirati a ridurre al minimo il rischio di discriminazione algoritmica, specialmente in relazione alla progettazione e alla qualità dei set di dati utilizzati nello sviluppo dei sistemi di IA.

[46] C. CASONATO, B. MARCHETTI, op. cit.., *in Biolaw Journal*, 2021.

gratuito una tecnologia basata sull'Intelligenza Artificiale, indipendentemente dalla sua sede geografica, e l'utente (*user*), ossia colui che utilizza la tecnologia per svolgere attività personali[47]. Esulano dal perimetro d'applicazione del Regolamento i fornitori che producono sistemi di Intelligenza Artificiale da usare in situazioni legate alla sicurezza nazionale o a scopi militari[48]. Allo stesso modo, il Regolamento non si estende, poi, alle autorità pubbliche di paesi terzi e alle organizzazioni internazionali che impieghino sistemi di Intelligenza Artificiale in consonanza agli accordi internazionali dedicati all'applicazione della legge e alla cooperazione giudiziaria con l'Unione Europea e uno o più stati membri. Va, peraltro, osservato, che la sfera di applicabilità del Regolamento in virtù del Considerando 12 non pregiudica l'applicabilità del regime di responsabilità dei prestatori intermediari di cui alla direttiva 2000/31/CE del Parlamento europeo e del Consiglio[49]. Con riferimento, invece, all'ambito oggettivo, lo si ricava dall'art 1, il quale, dispone che il Regolamento si applica all' l'immissione sul mercato da intendersi quale prima messa a disposizione di un sistema di *IA* sul mercato dell'Unione, alla messa a disposizione sul mercato da qualificarsi come qualsiasi fornitura di un sistema di *IA* per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale, a titolo oneroso o gratuito ed, infine, alla messa in servizio da intendersi quale fornitura di un sistema di *IA* direttamente all'utente per il primo uso o per uso proprio sul mercato dell'Unione per la finalità prevista[50].

Si colloca nell'orizzonte applicativo della disciplina *de qua* la creazione di spazi di sperimentazione normativa, noti come "*sandboxes*", finalizzati ad agevolare l'accesso al mercato delle *start-up*, promuovere l'innovazione per sostenere le piccole e medie imprese e massimizzare la competizione. In questo contesto favorevole supervisionato dalle autorità nazionali competenti, i sistemi di Intelligenza Artificiale possono essere attentamente testati e convalidati prima di essere ufficialmente introdotti sul mercato europeo[51]. Si fa uso, ad esempio, delle *sandboxes* per addestrare ed implementare i sistemi di Intelligenza Artificiale mediante l'utilizzo di dati biometrici, assicurandosi contemporaneamente che l'impiego di tali dati avvenga nel pieno rispetto del diritto alla protezione dei dati personali.

4. LA NOZIONE ISTITUZIONALE DI INTELLIGENZA ARTIFICIALE CONTENUTA NEL REGOLAMENTO

E' necessario, ai fini di questa trattazione, dare una definizione di Intelligenza Artificiale

[47] G. PROIETTI, *op. cit., in www.dirittobancario.it.*

[48] COM/2021/206 final, https://eur-lex.europa.eu; rientrano nel novero soggettivo di applicazione del regolamento anche le seguenti figure: il rappresentante autorizzato identificabile con qualsiasi persona fisica o giuridica stabilita nell'Unione, autorizzata mediante un mandato scritto da un fornitore di un sistema di intelligenza artificiale (IA), incaricata di eseguire gli obblighi e seguire le procedure stabilite da questo regolamento per conto del fornitore; l'importatore definibile come ogni soggetto fisico o giuridico nell'Unione che introduce sul mercato o mette inservizio un sistema di IA portando il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione; infine, da ultimo, troviamo il distributore da intendersi come qualsiasi persona fisica o giuridica all'interno della catena di approvvigionamento diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione senza apportarne modifiche alle proprietà ; Per quanto concerne l'utilizzo dell'intelligenza artificiale per finalità militari si rinvia alla Risoluzione parlamentare del 12/9/2018 sui sistemi d'arma autonomi (2018/2752 [RSP]). Si veda in proposito anche la Risoluzione del Parlamento europeo del 20/1/2021 (2020/2013 [INI]) sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale.

[49] *G.* MARCHIANO', *op. cit..,* in www.ambientediritto.it, Cyberlaws,2021, p.7.

[50] G. PROIETTI, *op. cit., in www.dirittobancario.it; si vedano altresi' i Considerando 71 e 72 della Proposta normativa sull'IA*

[51] C. DELLA GIUSTINA, *Il Regolamento Europeo sull' intelligenza artificiale Ai Act 2023 in Cammino Diritto*, 18 Dicembre 2023.

per comprendere appieno il campo di applicazione attorno al quale ruota l'intera disciplina del Regolamento. In termini generici, l'Intelligenza Artificiale (*IA*) può essere definita una forma di intelligenza non biologica, in grado di apprendere e migliorarsi nel tempo, e che, in certi aspetti, opera in modo simile a quella umana, ancorché presenti diversi profili di divergenza[52]. Dal punto di vista scientifico, nonostante un fervente dibattito in corso e l'assenza di un consenso unanime sul suo significato, l'*IA* è solitamente definita come una disciplina informatica che studia i fondamenti teorici, le metodologie e le tecniche per progettare sia sistemi hardware sia sistemi software capaci di fornire prestazioni all'elaboratore elettronico che, a prima vista, sembrerebbero essere esclusive dell'intelligenza umana. È, invero, opinione condivisa nella comunità informatica che l'intelligenza artificiale si riveli attraverso la capacità di svolgere varie funzioni, tra cui: adattamento all'ambiente, in particolare a nuove situazioni, apprendimento dall'esperienza, percezione, intuizione, pensiero astratto, utilizzo efficiente di risorse limitate, comunicazione e etc[53].

Nella Relazione di accompagnamento alla Proposta di Regolamento, si intende per Intelligenza Artificiale una famiglia di tecnologie in rapida evoluzione che può portare un'ampia gamma di vantaggi economici e sociali[54]. Questi benefici includono il miglioramento della previsione, l'ottimizzazione delle operazioni e dell'allocazione delle risorse, nonché la personalizzazione dell'erogazione dei servizi.

A tal proposito, l'uso dell'Intelligenza Artificiale è considerato in grado di generare risultati benefici a livello sociale e ambientale, fornendo nel contempo vantaggi competitivi chiave alle aziende e all'economia europea. All'interno del Titolo I del Regolamento, dedicato alle definizioni, l'articolo 3 dispone che rientra nel perimetro definitorio dei sistemi di Intelligenza Artificiale ogni software sviluppato con una o più delle tecniche degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono[55].

Le prescrizioni del Regolamento si applicano ad alcuni di tali sistemi durante la fase di progettazione e sviluppo; nel corso della fase di immissione sul mercato; e infine, durante la fase di messa in funzione, per mitigare le conseguenze dannose che possono insorgere. Questa nozione di sistema di Intelligenza Artificiale, delineata all'articolo 3, viene esplicata ulteriormente nell'allegato 1[56], fornendo esempi paradigmatici di quelli che possono essere considerati sistemi di Intelligenza Artificiale.

Questi includono approcci di apprendimento automatico *machine learning*, e apprendimento profondo *deep learning*, che consentono ai sistemi di elaborare dati e assumere decisioni autonome. Inoltre, l'allegato

[52] A. LONGO e G. SCORZA, op. cit., 2020, p.14 e ss.
[53] G. SARTOR, *L'Intelligenza artificiale e il diritto*, Torino , Editore Giappichelli, 2022, p.16.
[54] COM/2021/206 final, https://eur-lex.europa.eu; Nella Risoluzione del Parlamento europeo sulla responsabilità civile in materia di IA" del 20/10/202066 veniva definita come ": «un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici», si veda Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale P9_TA(2020)0276.
[55] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it*, Dicembre 2021, p.10.
[56] L'Allegato I, intitolato " tecniche e approcci di intelligenza artificiale" definisce gli approcci specifici che caratterizzano l'intelligenza artificiale: a) approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (deep learning); b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.

menziona approcci basati sulla logica, sulla conoscenza, la rappresentazione della conoscenza e la programmazione induttiva, oltre a metodi statistici[57]. Tutte queste categorie, dettagliate nell'allegato 1, definiscono l'Intelligenza Artificiale nell'Unione Europea e, pertanto, devono conformarsi alle disposizioni di questo Regolamento.

Il legislatore comunitario ha introdotto una definizione ampia dei sistemi basati sull'Intelligenza Artificiale, includendo software che si avvalgono del *machine learning*, del *logic learning*, e di sistemi di conoscenza basati su dati statistici[58]. Un aspetto di fondamentale importanza, derivante direttamente dalla definizione di Intelligenza Artificiale adottata dal Legislatore Europeo, è che questa tecnologia deve sempre generare un output corrispondente a un risultato predeterminato dall'essere umano[59]. Questo punto rappresenta un elemento ineludibile del Regolamento, poiché il legislatore comunitario, nell'ottica di allocare la responsabilità sui rispettivi produttori, vuole che le tecnologie *AI* producano risultati predefiniti e prevedibili. Allargando lo scenario tratteggiato notiamo che la cornice normativa prevede che elenco di tecnologie sopra richiamate sarà soggetto a una continua evoluzione, poiché una delle principali caratteristiche della normativa è la periodica revisione dell'Allegato 1, che riguarda gli approcci e le tecniche per lo sviluppo dell'*IA*[60]. Nella prospettiva della normativa sull'*IA* questa modernizzazione del sistema è indirizzata a prevenire l'obsolescenza normativa in ragione del costante progresso tecnologico che influisce per forza di cose sull'armamentario normativo rendendolo inadeguato. Alla stregua di ciò, ne discende che è stato previsto che la Commissione Europea, a mente dell'art 290 TFUE , possa modificare, mediante atti delegati, gli allegati aggiornandoli per tener conto dell'evoluzione tecnologica in atto[61].

5. ANALISI, VALUTAZIONE E GESTIONE DEL RISCHIO

In premessa, è fondamentale sottolineare come il Regolamento riponga la massima priorità nel rafforzare la sicurezza nell'utilizzo dell'Intelligenza Artificiale per i cittadini, le imprese e le istituzioni pubbliche[62]. Tale obiettivo viene concretizzato attraverso la previsione di una scala di rischio multilivello, che prevede regolamentazioni più restrittive per le applicazione dell'Intelligenza Artificiale in contesti particolarmente delicati e sensibili. Diversamente, si individuano e vietano alcune modalità d'uso, sebbene tecnicamente possibili, in quanto ritenute perniciose per l'essere umano[63]. Proseguendo con il vaglio del Regolamento, è evidente che le disposizioni mirano a garantire un utilizzo responsabile dell'Intelligenza Artificiale, bilanciando efficacemente le esigenze di innovazione con la protezione dei diritti e la tutela dell'ordine pubblico[64].

Il Regolamento classifica le tecnologie dell'Intelligenza Artificiale in base al rischio[65]. Nel primo gruppo, rientrano i sistemi vietati, generalmente proibiti salvo rare eccezioni normative. Nel secondo gruppo, si collocano i sistemi ad alto rischio, per i quali sono definiti precisi precetti e misure organizzative, riconoscendo l'intrinseca pericolosità associata. Infine, nel terzo gruppo sono inclusi i sistemi di

[57] G. PROIETTI, *op. cit., in www.dirittobancario.it.*
[58] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, i op. cit.., *in www.i-lex.it*, Dicembre 2021, p.10.
[59] C. CASONATO, B. MARCHETTI, op. cit., *in Biolaw Journal*, 2021.
[60] Legge sull'intelligenza artificiale, Dossier n° 57 - 12 novembre 2021, Camera dei deputati - Ufficio Rapporti con l'Unione Europea, in https://documenti.camera.it.
[61] La norma di cui all'art. 4 del Regolamento legittima la Commissione a rivedere l'Allegato I adattando flessibilmente l'ambito di applicazione del quadro normativo.
[62] COM/2021/206 final, https://eur-lex.europa.eu.
[63] C. CASONATO, B. MARCHETTI, op. cit., *in Biolaw Journal,* 2021.
[64] C. SCHEPISI, op. cit ., in www.aisdue.eu, 28 marzo 2022, p.8.
[65] *CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit.., in www.i-lex.it, Dicembre 2021.pp.7 e ss.*

medio e basso rischio, che comportano livelli inferiori di regolamentazione e controllo. Questa suddivisione in gruppi di rischio fornisce un quadro chiaro per l'adozione di misure proporzionate alle caratteristiche e alle implicazioni di ogni tipo di tecnologia, garantendo un approccio differenziato e mirato.

È indispensabile, sin d'ora, sottolineare che per i sistemi a rischio minimo, la portata normativa, e di conseguenza tutti gli adempimenti di carattere formale, sono chiaramente ridotti. Per questi ultimi sistemi, le diverse società, non essendo in pericolo i diritti dei cittadini, potranno definire regole comportamentali da inserire in un apposito Codice di Condotta che dovrà ispirare le attività di tutti coloro che operano con l'ausilio dell'*IA*[66]. In una prospettiva di gestione proattiva del rischio (r*isk management*), l'impianto regolatorio sottolinea l'esigenza di implementare un robusto sistema di gestione del rischio derivabile dalle applicazioni di *IA*[67]. Questo sistema di gestione del rischio, costituito da un processo interattivo e continuo, dovrebbe essere applicato lungo l'intero ciclo di vita del sistema, con aggiornamenti regolari, e deve essere strutturato in quattro fasi: (a) identificazione e analisi iniziale dei rischi noti e prevedibili associati a ciascun sistema ad alto rischio; (b) stima e valutazione dei rischi che possono emergere durante l'utilizzo del sistema in conformità allo scopo previsto e in condizioni d'uso improprio ragionevolmente prevedibili; (c) valutazione di ulteriori rischi basata sull'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato; (d) adozione di adeguate misure di gestione dei rischi, in grado di rendere accettabile qualsiasi rischio residuo, sempre che il sistema sia utilizzato secondo le intenzioni previste. Alla stregua di ciò, per gestire al meglio il rischio, il Regolamento detta poi una serie di precetti: a) eliminazione o contenimento dei rischi per quanto possibile mediante una progettazione e uno sviluppo adeguati; b) attuazione di adeguate misure di mitigazione e controllo in relazione a quei rischi che non possono essere eliminati; c) trasmissione di informazioni adeguate all'utente e, se opportuno, fornitura della necessaria formazione[68].

In conclusione, la scelta di tali criteri operativi all'interno del corpus normativo evidenzia l'impostazione metodologica adottata dal legislatore, il quale struttura il processo di gestione del rischio in modo sistematico ed efficiente: da una parte vuole eliminare o ridurre i rischi attraverso un'adeguata progettazione e fabbricazione e dall'altro vuole fornire dati adeguati, unitamente, ove necessario a una formazione degli utenti.

6. LE PRATICHE DI IA VIETATE

Il quadro regolatorio oggetto del presente contributo si incardina su alcuni principi europei, quali il rispetto dei diritti costituzionali, della dignità e della democrazia liberale, pilastri basilari dell'ordinamento europeo[69]. Pertanto, il Regolamento impone un divieto categorico su alcune pratiche di utilizzo dell'Intelligenza Artificiale, considerate a priori compromettenti per l'essere umano[70]. Si ritiene che tali sistemi siano in contrasto con i valori europei e i diritti fondamentali dell'Unione Europea. In ottemperanza con il contesto valoriale europeo, il sistema normativo cerca di coniugare la tutela dell'integrità di tali valori essenziali con le logiche del mercato, sempre più indirizzate all'implementazione di sistemi basati sull'Intelligenza Artificiale[71]. Analizzando attentamente questo apparato normativo,

[66] F.A. NANNI, *Analisi della proposta di Regolamento sull'intelligenza artificiale pubblicata dalla Commissione Europea il 21 aprile 202*1 *in www.cyberlaws.it*, 16 giugno 2021.
[67] G. PROIETTI*, op. cit., in www.dirittobancario.it*.
[69] *G.* MARCHIANO'*, op. cit., in www.ambientediritto.it*, Cyberlaws,2021, p.10.
[70] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit.., *in www.i-lex.it,* Dicembre 2021.
[71] *G.* MARCHIANO'*, op. cit., in www.ambientediritto.it*, Cyberlaws,2021, p.10.

emerge chiaramente l'accento posto sulla intangibilità dei diritti e delle libertà fondamentali, tanto è vero che è richiesta un'osservanza alle disposizioni molto stringente nei vari contesti di uso dell'Intelligenza Artificiale. L'*Ai Act*, conformemente ai principi fondanti dell'*UE* ed ai propri tratti identitari, regolamenta in modo accurato e dettagliato non solo i sistemi di *IA* che possono comportare seri rischi fisici e psicologici, ma anche quei sistemi che se utilizzati sfociano in modo immediato ed esplicito nella lesione di diritti e interessi costituzionalmente protetti. A questo punto, occorre scandagliare i vari divieti previsti dal Regolamento, e, nello specifico, il dettato normativo di cui all'art. 5 del Titolo II stabilisce alcuni divieti per diverse pratiche realizzate con l'uso dell'Intelligenza Artificiale[72]. Il Regolamento europeo proibisce diverse pratiche, adottando un approccio garantista ed antropocentrico[73]. Vieta l'utilizzo di tecniche subliminali (*subliminal manipulation*) che sfruttano elementi inconsci della mente al fine di indurre e condizionare subdolamente gli utilizzatori dei sistemi di Intelligenza Artificiale ad adottare comportamenti che possano cagionare agli stessi o ad altre persone un nocumento fisico o psicologico[74].È stata proibita la categorizzazione e la targhetizzazione biometrica degli utenti considerati vulnerabili (*exploitation of vulnerability)* in ragione dell'età, della disabilità o della situazione sociale ed economica, e che abusa di questa circostanza personale per alterare materialmente il comportamento di una persona che appartiene a tale gruppo, provocandole un danno fisico o psicologico. Questo divieto si configura come un baluardo a difesa delle persone dalle pratiche di utilizzo dell'*IA* indirizzate a sfruttare le loro fragilità. Sulla scia di questa disamina concernente le proibizioni, risalta all'occhio l'impronta fortemente protettiva impressa dal Legislatore per prevenire l'abuso delle informazioni biometriche per fini discriminatori o pregiudizievoli. E' stato bandito l'utilizzo di sistemi di AI che valutano o classificano l'affidabilità delle persone sulla base del loro comportamento sociale, noto come "*social scoring o social credit sistem*"[75].In particolare, è stata vietata la pratica concernente l'introduzione sul mercato, la messa in funzione o l'utilizzo di dispositivi utilizzati dalle Autorità Pubbliche per la raccolta di dati senza il consenso degli interessati e l'assegnazione di un punteggio numerico o categorico in base a una determinata condotta sociale. A tal proposito, la pratica in questione può produrre uno o entrambi i seguenti risultati: (i) un trattamento dannoso o sfavorevole per determinate persone fisiche o per interi gruppi di persone in contesti sociali estranei rispetto a quelli in cui i dati sono stati originariamente generati o raccolti; (ii) un trattamento dannoso o sfavorevole per determinate persone fisiche o per interi gruppi di appartenenza non giustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità. La previsione legislativa di cui all'art 5 al punto c) norma questa proibizione poiché un eventuale utilizzo determinerebbe trattamenti discriminatori nei confronti di alcune persone o favoritismi nei confronti di altre[76]. Dall'analisi della formula della norma si evince l'intento del Legislatore europeo di preservare l'equità e impedire qualsiasi forma di valutazione basata su criteri sociali che potrebbe portare a disparità e penalizzazioni[77]. Tra le applicazioni vietate dell'Intelligenza Artificiale, che ricadono nel livello di rischio inaccettabile, rientrano i sistemi di riconoscimento facciale a distanza e di identificazione biometrica remota in luoghi

[72] *G. PROIETTI*, op. cit., *in www.dirittobancario.it.*
[73] A. ALAIMO*, op. cit.., in www.federalismi.it,* 18 Ottobre 2023, p.4.
[74] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it*, Dicembre 2021,pp 13 e ss.
[75] G. PROIETTI*, op. cit., in www.dirittobancario.it*
[76] *G.* MARCHIANO', *op. cit.., in www.ambientediritto.it,* Cyberlaws,2021,p.10.
[77] C. CASONATO, B. MARCHETTI*, op. cit..,* *in Biolaw Journal*, 2021.

pubblici, utilizzati dalle forze dell'ordine(*real-time remote biometric identification for law enforcement purpose in publicly accessible spaces*)[78]. Per inquadrare correttamente questo divieto occorre prima definire il concetto di riconoscimento biometrico e poi operare un distinguo tra riconoscimento *real time* e riconoscimento *ex post*[79]. Ai sensi dell'ottavo Considerando della bozza di Regolamento, per sistema di identificazione biometrica basato sull'uso dell'*IA*, il termine "sistema di identificazione biometrica" identifica tutti quei mezzi progettati per riconoscere le persone fisiche a distanza mediante il confronto dei loro dati biometrici con quelli già inclusi in un *database* di riferimento. Da questa definizione si evince che nei sistemi "*real-time*", l'acquisizione dei dati biometrici, il confronto e l'identificazione avvengono simultaneamente o con ritardi insignificanti, mentre, al contrario, nei sistemi che consentono un'identificazione "*ex post*", i dati biometrici sono acquisiti in un momento precedente e il confronto, così come l'identificazione, si verificano successivamente, in un secondo momento. Tornando alla disamina del divieto, si rileva che l'articolo 5 concede alle autorità pubbliche la possibilità di utilizzare tali sistemi di riconoscimento biometrico in determinati contesti e circostanze specifiche[80]. Il Regolamento traccia, specificamente, per esigenze pubblicistiche e preventive, una serie di casi eccezionali per l'utilizzo di sistemi di riconoscimento biometrico da parte delle forze dell'ordine. Queste ipotesi predeterminate tassativamente dalla legge sono: la situazione di minaccia terroristica imminente, la ricerca di vittime di gravi crimini o l'individuazione, la localizzazione, l'identificazione o il perseguimento dell'autore o del sospettato delle fattispecie di reato indicate nel paragrafo secondo dell'art 2 della decisione quadro 2002/584/GAI del Consiglio qualora però in tali ipotesi di reato la pena edittale nel massimo o una misura di sicurezza previste siano superiori di almeno tre anni nella legislazione dello Stato membro. A tal riguardo, il Regolamento precisa che l'uso di un sistema di identificazione biometrica in tempo reale in spazi accessibili al pubblico, a fini di attività di contrasto e persecuzione dei crimini, è subordinato a dei limiti di carattere temporale, geografico e personale[81] Per rientrare, inoltre, nel raggio di applicazione delle eccezioni previste per il contrasto alla criminalità, è necessaria un'autorizzazione preventiva (*ex ante*) da parte di un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'utilizzo. Il rilascio di questa autorizzazione, a mente del secondo comma dell'articolo 5, comporta una serie di valutazioni, che includono l'analisi della natura della situazione che ha motivato il suo possibile utilizzo[82]. In particolare, si considerano la gravità, la probabilità e l'entità del danno, nonché le conseguenze dell'uso del sistema sui diritti e le libertà di tutte le persone interessate, con particolare attenzione alla gravità, probabilità e portata di tali conseguenze. In situazioni di impellente necessità, debitamente e congruamente motivate, è consentita l'adozione del sistema di identificazione biometrica senza il rilascio preventivo dell'autorizzazione, con la possibilità di richiedere l'autorizzazione in concomitanza o successivamente al suo utilizzo[83]. Tuttavia l'Autorità competente, tenendo conto di un compendio probatorio solido e sulla scorta di

[78] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it*, Dicembre 2021,p.19.
[79] G. PROIETTI, op. cit., *in www.dirittobancario.it*.; L'impiego generalizzato di tale tecnologia aprirebbe le porte a una sorveglianza di massa, poiché comporterebbe la scansione dei passanti, consentendo, in violazione della loro riservatezza, l'associazione dei loro volti o dei loro tratti somatici.
[80] *G.* MARCHIANO', *op. cit..,* in www.ambientediritto.it, Cyberlaws,2021, p.11.
[81] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it*, Dicembre 2021, p.20.
[82] . CASONATO, B. MARCHETTI*, op. cit.., in Biolaw Journal*, 2021.
[83] A. LONGO, *Italia primo Paese a vietare il riconoscimento facciale (con eccezioni),* il sole24 ore, 2 dicembre 2021.

indicazioni chiare presentate dal richiedente, valuterà il rilascio dell'autorizzazione, determinando se il sistema di identificazione biometrica risulti necessario e proporzionato al conseguimento di uno degli obiettivi contrassegnati nella lettera d) dell'articolo 5.L'ultimo paragrafo dell'articolo 5 lascia degli spazi di manovra agli Stati membri, consentendo loro di autorizzare l'uso di sistemi di identificazione biometrica nei casi previsti nei paragrafi 1, lettera (d), 2 e 3[84]. Nell'ambito della propria legislazione, lo Stato membro può stabilire le modalità operative necessarie per richiedere, emettere e esercitare le autorizzazioni. Queste prescrizioni normative dovrebbero in aggiunta anche dettagliare per quali ipotesi di reato è accordato l'utilizzo dell'identificazione biometrica e inquadrare le autorità autorizzate all'applicazione di tali sistemi, cosa che non risulta evincersi dalle disposizioni nel Regolamento.

7. SISTEMI DI IA AD ALTO RISCHIO

Il nucleo centrale dell'intero Regolamento riguarda i sistemi di Intelligenza Artificiale (*AI*) ad alto rischio (*high-risk systems*), al quale il Regolamento riserva il titolo III[85]. La normativa contempla numerose disposizioni applicabili a tali sistemi ad alto rischio, e, va sottolineato che tali sistemi dovranno attenersi a procedure specifiche e soddisfare determinati requisiti prima di poter essere introdotti nel mercato dell'Unione.

Secondo l'impianto normativo del Regolamento questi sistemi devono essere sottoposti a una valutazione meticolosa per garantire che le loro operazioni non compromettano i diritti umani fondamentali: difatti il prodotto prima di essere immesso sul mercato deve transitare attraverso un necessario vaglio di conformità, atto a comprovare l'assenza di rischi inaccettabili.

In base all'articolo 6 del Regolamento, rientrano nella categoria dell'alto rischio tutti quei sistemi destinati ad essere utilizzati come componente di sicurezza di prodotti o rappresentano essi stesso un prodotto soggetto ad una valutazione di conformità secondo le normative armonizzate *UE*, contenute nell'allegato n. II, corrispondenti ,quasi pedissequamente, all'ampio pacchetto di misure del c.d *new legislative framework*[86]: tra le regolamentazioni menzionate risaltano la direttiva 2009/48/CE sulla sicurezza dei giocattoli e il Regolamento (UE) 2017/745 sui dispositivi medici[87].

Inoltre, quando si fa riferimento ai sistemi di Intelligenza Artificiale ad alto rischio, è opportuno prestare particolare attenzione, all'allegato III il quale contiene un elenco puntuale di diverse aree critiche nelle quali il rischio di utilizzo potrebbe essere di una certa portata, potendo impattare direttamente sulla vita delle persone[88]. Si pensi ad esempio ai sistemi di valutazione per la selezione del personale, ai sistemi di previsione della solvibilità degli individui, nonché ai sistemi inerenti la gestione delle pratiche migratorie ecc. Nello specifico le aree contemplate sono: l'accesso ai servizi pubblici e privati, l'attività di contrasto e amministrazione della giustizia, la categorizzazione biometrica delle persone

[84] *G.* MARCHIANO', *op. cit., in www.ambientediritto.it*, Cyberlaws,2021,pp.11 e ss ; I casi previsti per poter autorizzare l'uso di sistemi di identificazione biometrica da parte degli Stati sono segnatamente la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; e il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro."

[85] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., in www.i-lex.it, Dicembre 2021, p.2.

[86] È un insieme di misure normative tese ad uniformare e migliorare gli standard di conformità richiesti per la commercializzazione nel mercato unico europeo di determinati prodotti.

[88] C. CASONATO, B. MARCHETTI, op. cit.., *in Biolaw Journal*, 2021.

fisiche, il funzionamento delle infrastrutture critiche, l'istruzione e la formazione professionale, l'occupazione e la gestione dei lavoratori[89]. Questo allegato, che enumera le diverse aree in cui l'utilizzo di sistemi di *IA* si presume ad alto rischio, sarà soggetto a aggiornamenti progressivi in base ai nuovi sviluppi tecnologici. All'interno del Regolamento infatti, è stato previsto, per far fronte a una tecnologia in continuo divenire, un meccanismo di aggiornamento delle aree considerate ad alto rischio mediante l'emanazione di atti delegati ai sensi dell'art 290 TFUE da parte della Commissione. Questa modifica, consentendo una periodica evoluzione normativa, viene attivata quando sono soddisfatti requisiti precisi: (a) l'uso dei sistemi di Intelligenza Artificiale rientra in uno dei settori elencati nei punti da 1 a 8 dell'allegato III; (b) i sistemi comportano un rischio di danno alla salute e alla sicurezza o un rischio di impatto negativo sui diritti fondamentali, con una gravità e probabilità di accadimento equivalenti o superiori al rischio associato ai sistemi indicati nell'allegato III[90].

La Commissione per poter ricorrere a tale procedura che elude l'ordinario iter legislativo deve scrutinare i seguenti aspetti: (a) lo scopo perseguito dal sistema di *IA ;* (b) l'ambito di utilizzo del sistema di Intelligenza Artificiale; (c) se il sistema di *IA* abbia già cagionato un nocumento alla salute e alla sicurezza o comunque abbia avuto una ricaduta negativa sui diritti fondamentali o abbia sollecitato preoccupazioni significative in relazione alla verificazione di tale danno o impatto negativo; (d) l' entità del danno o di tale impatto negativo, in particolare in termini di intensità e capacità di colpire una pluralità di persone; (e) la misura in cui le persone potenzialmente lese dipendono dal risultato prodotto con un sistema di *IA*; (f) l'entità della posizione di debolezza dei danneggianti rispetto all'utente del sistema, in particolare a causa di uno squilibrio di potere, asimmetria informativa, circostanze economiche o sociali, o di età; (g) il grado di reversibilità del risultato prodotto dal sistema in questione; (h) l'eventuale previsione di apposite misure in relazione ai rischi presentati da un sistema di *IA* dalla legislazione europea; (i) l'esistenza di misure efficaci per prevenire o ridurre al minimo tali rischi. È precisato, altresì, all'art 84 che la Commissione, a seguito dell'entrata in vigore dell'atto legislativo, valuta la necessità di modificare l'elenco di cui allegato III una volta l'anno e, successivamente, ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame del presente Regolamento [91].

8. UN CORRETTO MODELLO DI GOVERNANCE DEI DATI

Esaminati i criteri per classificare un sistema di Intelligenza Artificiale come ad alto rischio, pare doveroso definire i requisiti obbligatori consacrati nel Capo II del Titolo III della normativa, a cui, specialmente i fornitori, devono fare riferimento per l'immissione sul mercato o la messa in servizio[92]. In tal senso, questi requisiti possono essere compendiati come segue: gestione dei dati di alta qualità (art. 10); conservazione delle registrazioni (art. 12); trasparenza e fornitura di informazioni agli utenti (art. 11). Nella trattazione di questo paragrafo si farà esclusivo riferimento ai requisiti relativi alla qualità dei dati.

Secondo quanto dispone il Regolamento, visti gli errori e le discriminazioni associabili all'impiego di dati non sufficientemente curati, assume rilievo centrale ai sensi dell'art.10, la qualità dei dati inseriti nei sistemi di Intelligenza Artificiale i quali devono soddisfare

[89] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., in www.i-lex.it, Dicembre 2021, p.22.
[90] G. PROIETTI*, op. cit., in www.dirittobancario.it*
[91] Cfr.art.84.
[92] F.C.LA VATTIATA, *Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale*, *Diritto Penale e Uomo*, p.12.

precisi criteri di qualità, specialmente per quanto riguarda i dati utilizzati nell'addestramento (*data set*), nella convalida (*validation set*) e nella prova (*test set*)[93]. Queste attività di preparazione dei dati sono predisposte per garantire che l'algoritmo operi in conformità alle previsioni programmate dagli sviluppatori, in linea con la destinazione d'uso e in modo sicuro, al fine di raggiungere il risultato prefigurato[94]. Il Regolamento dettaglia le caratteristiche che il *dataset* deve possedere nelle fasi di *training, validation* e *testing*: è essenziale che il dato sia innanzitutto pertinente rispetto all'*output* desiderato, completo, rappresentativo e privo di errori, conformemente agli standard di qualità richiesti[95] Per minimizzare il rischio di esiti discriminatori, è fondamentale che i *dataset* siano rappresentativi, statistici e eticamente corretti in relazione al contesto di utilizzo dell'algoritmo. L'adattamento degli algoritmi al contesto d'uso grazie alle proprietà statistiche immesse nel sistema è una pratica di *goverernance* essenziale, specialmente considerando il preaddestramento su *dataset* ampi. Sulla scia di questa prospettiva, si pone il tema della robustezza del sistema, ovvero della sua capacità di resistere ai rischi connessi ai limiti del sistema stesso, tra cui errori, guasti e incongruenze che possono dispiegarsi soprattutto a causa delle interazioni con persone fisiche o altri dispositivi (art 15)[96]. Per affrontare tali rischi, al fine di ridurli e mitigarli, si rende necessario implementare soluzioni come *backup* o meccanismi *fail-safe*. È, altresì, necessario ai sensi del par.4 dell'art 15 garantire la resilienza contro azioni e minacce di sicurezza informatica di terzi che potrebbero compromettere la sicurezza del sistema e, di conseguenza, innescare comportamenti dannosi nell'Intelligenza Artificiale[97]. Queste misure di carattere tecnico, che sono state poc'anzi richiamate, hanno come fine quello di assicurare un risultato dei sistemi di *IA* accurato e, soprattutto, immune da distorsioni provocate da minacce, che possono originare tanto da attacchi informatici di terzi quanto da alterazioni impreviste consustanziali alle limitazioni del sistema[98]. Prima della commercializzazione di un sistema di Intelligenza Artificiale ad alto rischio, è obbligatorio redigere un documento tecnico secondo gli standard presenti nell'Allegato IV del Regolamento[99]. Tale documentazione non solo fornisce una descrizione del processo di sviluppo dell'algoritmo, ma consente anche di tracciare la sua evoluzione durante l'intero ciclo di vita. Il sistema documentale prescritto agevola la tracciabilità del sistema e facilita il monitoraggio *post-market* (*monitoring post market*), consentendo di valutare gli output e le performance dell'algoritmo anche dopo la sua introduzione sul mercato. Infine, per garantire sempre un monitoraggio attivo il Regolamento, al paradigma normativo di cui all'art 12, prevede un meccanismo di *logging,* ovvero è necessario che i dispositivi vengano programmati e sviluppati in maniera tale da consentire la registrazione degli eventi nel corso del loro impiego. Il meccanismo, ora esposto, favorisce la tracciabilità dei dispositivi durante il loro ciclo di vita e agevola il monitoraggio degli *output* e delle *performance* anche in una fase successiva all'emissione nel circuito economico[100].

[93] C. CASONATO, B. MARCHETTI, *op. cit.., in Biolaw Journal,* 2021.
[94] F.C.LA VATTIATA, op. cit.., *Diritto Penale e Uomo*, p.12.
[95] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it*, Dicembre 2021,p.24
[96] C. CASONATO, B. MARCHETTI, op. cit., in *Biolaw Journal*, 2021.
[97] F.A. NANNI, op. cit., *in www.cyberlaws.it*, 16 giugno 2021.
[98] F.C.LA VATTIATA, op. cit., *Diritto Penale e Uomo*, p.12.
[99] G. PROIETTI, *op. cit., in www.dirittobancario.it*
[100] F.C.LA VATTIATA, op. cit., *Diritto Penale e Uomo*, p.12; ai sensi dell'art. 20 del Regolamento, la conservazione dei log generati automaticamente dai sistemi di IA ad alto rischio avviene per un periodo di tempo limitato quando tali log sono sotto il controllo dei fornitori in virtù di accordo stipulato con l'utente o in conformità alla legge in COM/2021/206 final, https://eur-lex.europa.eu.

9. *TRASPARENZA E COMPRENSIBILITÀ DEI RISULTATI*

Una questione a cui il Regolamento dedica particolare attenzione è l'opacità legata al funzionamento dei sistemi di Intelligenza Artificiale[101]. I problemi che sorgono a causa dall'opacità delle indicazioni algoritmiche si traducono in una estrema difficoltà dell'essere umano nell'identificare l'iter logico alla base di un certo risultato finale generato dai sistemi di *IA.*

Questa incomprensibilità, nel saper interpretare la macchina in gergo, si chiama '*blackbox*', e, più precisamente, corrisponde alla sostanziale incapacità di comprendere la correttezza del processo decisionale e all'impossibilità di decifrare i dati utilizzati. Il problema dell'opacità e dell'incapacità di mappare i passaggi eseguiti dagli algoritmi per generare il risultato finale è principalmente associato al settore dei sistemi di apprendimento automatico, caratterizzati dalla loro intrinseca natura adattativa e da una complessità computazionale tale da rendere inaccessibile la comprensione delle modalità di funzionamento attraverso le quali optano per una decisione anziché un'altra. In considerazione di questa significativa complessità nel conoscere le singole fasi del processo interno del dispositivo di Intelligenza Artificiale, i sistemi ad alto rischio, a norma dell'art 13, devono essere progettati e sviluppati garantendo un livello adeguato di trasparenza (*transparency)*[102]. Ciò significa che gli utenti devono essere in grado di comprendere il funzionamento del sistema, la logica sottesa alle operazioni che effettua il sistema di Intelligenza Artificiale e, di conseguenza, i motivi che stanno dietro a una decisione automatizzata. La trasparenza si configura all'interno del panorama normativo sull'*IA* come fattore determinante per promuovere la fiducia degli utenti nei confronti dei sistemi di Intelligenza Artificiale e assicurare una comprensione chiara(*explainability*) del processo decisionale dei sistemi di *IA.* Il Regolamento non richiede necessariamente la completa conoscenza dell'insieme di istruzioni appartenenti all'algoritmo, ma indica la necessità di fornire informazioni chiare, concise e comprensibili agli utenti, conformemente alle disposizioni del Regolamento. A tal riguardo, ogni sistema di *IA* ad alto rischio deve essere corredato di istruzioni per l'uso, contenenti le seguenti indicazioni; la finalità prevista; il livello di accuratezza, robustezza e *cyber*sicurezza[103] rispetto al quale il sistema è stato sottoposto; qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di *IA* ad alto rischio in conformità alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali; le prestazioni inerenti le persone e i gruppi di persone sui quali il sistema è destinato ad essere utilizzato; le informazioni pertinenti in termini di dati di addestramento convalida e prova ; le eventuali modifiche apportate al sistema di *IA* ad alto rischio; le misure di sorveglianza; delineate dall'articolo 14; le misure di manutenzione e cura necessarie per garantire il

[101] F. PASQUALE., *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, 2015. Per l'autore i sistemi decisonali algortmici sono come scatole nere inintellegibili in cui gli imput e gli output sono riconoscibili dall'utente ma il suo funzionamento o meglio l'iter decisionale prescelto non lo è.

[102] C. CASONATO, B. MARCHETTI, op. cit.., in *Biolaw Journal*, 2021.

[103] A proposito delle tematiche legate alla sicurezza informatica, si consiglia di fare riferimento alla Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione; Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013 («Regolamento sulla cybersicurezza»).

corretto funzionamento di tale sistema. Si coglie, con estrema evidenza, la necessità per il Regolamento di garantire per quanto possibile un diritto per i soggetti ad una spiegazione dei risultati. Un obiettivo, quello della trasparenza, evidenziato anche dal Considerando 70 che enuncia un obbligo di trasparenza per tutti sistemi di Intelligenza Artificiale ad alto rischio.

10. UN EFFICACE SUPERVISIONE UMANA SULL'IA

Nell'ottica di conferire una centralità alla supervisione umana nella progettazione, nello sviluppo e nel controllo dei sistemi di Intelligenza Artificiale, il Regolamento all'art.14 statuisce che i sistemi ad alto rischio devono essere concepiti in modo tale da consentire, anche attraverso idonei strumenti di interfaccia uomo-macchina, una sorveglianza efficace da parte delle persone fisiche nel corso dell'utilizzo del sistema di Intelligenza Artificiale (*Human oversight*)[104].Per il Regolamento, la supervisione umana è considerata indispensabile per prevenire i rischi, alla salute, alla sicurezza o altri diritti fondamentali, che potrebbero manifestarsi, anche quando il sistema è utilizzato in conformità ai requisiti della Proposta o in modo comunque ragionevolmente prevedibile[105]. Alla luce di ciò, l'aspetto del controllo umano assume grande rilevanza all'interno del reticolato normativo del Regolamento poiché è strettamente connesso alla gestione attiva dei rischi. Pertanto, il Legislatore prevede che sia il fornitore, anche dopo l'emissione in commercio del bene, sia l'utilizzatore che utilizza il sistema di Intelligenza Artificiale per la propria attività, debbano mantenere una sorveglianza continua attraverso alcune metodologie operative, tra cui: a) comprendere appieno le capacità e i limiti del sistema di *IA* ed essere in grado di monitorarne il funzionamento; b) mantenere un atteggiamento consapevole rispetto al rischio di *bias* ;c) essere in grado di interpretare correttamente l'*output* del sistema; d) essere in grado di decidere di non utilizzare il sistema o di ignorare, annullare o ribaltare il suo *output*; e) essere in grado di intervenire sul funzionamento del sistema o di interromperlo mediante un pulsante di "arresto" o una procedura analoga[106]. In aggiunta, all'interno del dettato normativo di cui all'art 29 è previsto che gli utenti dei sistemi ad altro rischio devono monitorare il funzionamento degli algoritmi sulla scorta delle istruzioni per l'uso. Questa previsione normativa abilita gli utenti a: garantire la pertinenza dei dati rispetto alla destinazione d'uso del sistema; informare il fornitore o il distributore, sospendendo contestualmente l'uso del sistema, nell'ipotesi in cui rilevi che l'osservanza delle istruzioni accluse al sistema possa comportare un rischio di cui all'art. 65 del Regolamento; informare attraverso attività di *reporting* il fornitore o il distributore in caso di gravi sinistri o malfunzionamenti; detenere, per un congruo periodo di tempo commisurato allo scopo del sistema, le registrazioni automatiche generate dal sistema nell'ipotesi in cui fossero nella sua disponibilità[107].

Tanto premesso, appare evidente che l'esercizio consapevole del controllo umano è un presidio fondamentale affinché l'Intelligenza Artificiale non intraprenda percorsi rischiosi ed incontrollati. Ad ogni modo, la comprensione totale delle capacità e dei limiti del sistema da parte dell'essere umano rimane comunque un compito arduo poiché l''Intelligenza Artificiale, sfruttando il suo apprendimento automatico basato sull'esperienza, si discosta da previsioni predicabili ex ante, generando soluzioni originali man mano che acquisisce conoscenze.

[104] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it*, Dicembre 2021, p.27.
[105] C. CASONATO, B. MARCHETTI, op. cit., *in Biolaw Journal*, 2021.
[106] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it,* Dicembre 2021, p.27
[107] G. PROIETTI, op. cit., *in www.dirittobancario.it.*

11. PROCEDURA DI VALUTAZIONE DELLA CONFORMITÀ

In ossequio a un approccio basato sulla gestione del rischio (*risk approach*), l'introduzione nello spazio economico europeo e la creazione di sistemi di Intelligenza Artificiale ad alto rischio è ammessa subordinatamente al rispetto dei requisiti contemplati nel Regolamento e a seguito di una attenta valutazione di conformità *ex ante* condotta dal fornitore[108].

Innanzitutto, in primo luogo, occorre determinare se il sistema di Intelligenza Artificiale può essere classificato effettivamente come ad alto rischio o meno. Successivamente, è necessario garantire che la progettazione e lo sviluppo del sistema siano conformi alle disposizioni del Regolamento non solo in fase di sviluppo ma anche durante l'utilizzo continuato del sistema.

In altre parole, è necessario implementare una procedura di *testing* e verifica che assicuri che il sistema, ideato con una determinata funzionalità, produca l'*output* desiderato in risposta all'*input* programmato, secondo quanto stabilito dalle normative. L'articolo 43, in un'ottica di *accountability,* stabilisce in via generale che la conformità a determinati standard è di spettanza del fornitore e consiste nel valutare la corrispondenza del loro sistema di gestione dei dati e della documentazione tecnica specifica ai canoni normativi predeterminati nel Capo 5, rubricato "Norme, valutazione della conformità, certificati, registrazioni [109]. All'esito dell'esecuzione delle procedure di conformità, i sistemi di Intelligenza Artificiale ad alto rischio beneficiano di una presunzione di osservanza ai requisiti a mente dell'articolo 40[110]. Per i dispositivi di categorizzazione biometrica delle persone fisiche, la valutazione di conformità effettuata dal fornitore deve ricevere la preventiva omologa da parte di organismi di controllo accreditati presso le Autorità di sorveglianza previste dal Regolamento. In relazione ai sistemi ad alto rischio destinati ad essere usati come componenti di sicurezza di un prodotto o come prodotto, secondo le normative europee in materia di sicurezza dei prodotti elencate all'Allegato 2 del Regolamento, seguono, per evitare un inutile sdoppiamento procedurale, la procedura di conformità di cui alla relativa normativa[111].

Al di fuori di queste situazioni, una volta conclusa con successo la valutazione della *compliance*, i sistemi di Intelligenza Artificiale ad alto rischio devono essere contrassegnati con l'apposizione della marcatura CE. La funzione del contrassegno è quello di certificare l'ottemperanza del sistema di Intelligenza Artificiale, ai fini della sua commercializzazione, alle norme previste nell'ambito del Regolamento. Secondo quanto stabilito dall'art 49 il produttore deve appore il logo CE sul sistema in modo visibile, leggibile e indelebile[112].

Completato tale adempimento, è , altresì, necessario, emettere una dichiarazione di conformità responsabilizzante, prima della commercializzazione o dell'utilizzo del sistema, a norma dell'articolo 48[113]. Alcuni sistemi, invece, prima di poter essere immessi sul mercato devono essere registrati in un apposito database accessibile al pubblico.

A tal guisa l'Allegato VIII cristallizza le informazioni necessarie che i provider, prima di collocare il prodotto sul mercato, devono 'inserire nel database, quali: identificazione e tracciabilità del sistema, obiettivi perseguiti, stato corrente del sistema (attivo o inattivo), copie conformi o indicazioni puntuali delle

[108] C. CASONATO, B. MARCHETTI, op. cit., in *Biolaw Journal*, 2021.
[109] Cfr.art..43
[110] Cfr.art.40
[111] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it,* Dicembre 2021, p.32
[112] Cfr.art.40.
[113] G. PROIETTI, *op. cit., in www.dirittobancario.it*

certificazioni e delle dichiarazioni di conformità, istruzioni elettroniche sul funzionamento[114].

L'obiettivo del Regolamento è configurare un sistema in cui chiunque, almeno in via di prima approssimazione, possa verificare, sia attraverso la marcatura CE sia mediante l'accesso al suddetto database, se un determinato sistema di Intelligenza Artificiale sia in linea con la cornice normativa del Regolamento dettata in materia di conformità. La procedura preliminare di controllo della conformità, tuttavia, non costituisce l'unico momento di controllo dei rischi[115]. Il Regolamento prevede anche un monitoraggio successivo alla messa in commercio (monitoraggio *post marketing*) che tiene conto dei singoli eventi avversi associabili alle variabili attività dei prodotti di Intelligenza Artificiale. A tal riguardo, viene istituito un meccanismo che consente di registrare tutte le informazioni di interesse durante il periodo di tempo in cui i dispositivi sono operativi[116]. In particolare vi è una raccolta sistematica di dati pertinenti forniti dagli utenti o raccolti tramite altre fonti[117]. Nell'ipotesi in cui dovessero palesarsi difetti sopravvenuti e storture non prevedibili in relazione all'assetto del bene secondo la scienza del momento in cui è stato messo in commercio, i fornitori devono segnalare tali problematiche alle autorità competenti. Su tale punto, l'art 62 testualmente recita "*I fornitori di sistemi di IA ad alto rischio immessi sul mercato dell'Unione segnalano qualsiasi incidente grave o malfunzionamento di tali sistemi che costituisca una violazione degli obblighi previsti dal diritto dell'Unione intesi a tutelare i diritti fondamentali alle autorità di vigilanza del mercato degli Stati membri in cui tali incidenti o violazioni si sono verificati…*"[118].Come precisato dal secondo comma dell'art 62 qualsiasi malfunzionamento o incidente relativo ai dispositivi di *IA* deve essere segnalato immediatamente dopo l'accertamento del nesso causale o dalla ragionevole probabilità ti tale collegamento eziologico ed in ogni caso non oltre il termine perentorio di 15 giorni dalla sua scoperta[119].

12. SISTEMI DI IA A RISCHIO LIMITATO O MINIMO

Nel corso di questa disamina, il *focus* principale è stato posto sulle pratiche proibite di utilizzo dell'Intelligenza Artificiale che contravvengono ai valori europei nonché sui prodotti ad alto rischio che possono essere introdotti sul mercato a condizione che rispettino gli obblighi di gestione dei dati usati per l'addestramento, la validazione e la verifica e siano osservanti dei requisiti di trasparenza e supervisione.

Il Regolamento affronta in modo residuale i sistemi a basso rischio caratterizzati da una limitata capacità manipolativa o a rischio minimo che non comportano rischi rilevanti. A tal riguardo, l'articolo 52, Titolo IV del Regolamento, stabilisce che alcuni sistemi non a rischio limitato, ovvero con un livello di rischio minimo, appartenenti a specifici settori, sono esentati da una rigida griglia di obblighi burocratici[120]. Per i sistemi a rischio limitato la normativa richiede che il fornitore debba adempiere esclusivamente a obblighi informativi e di trasparenza, garantendo che i sistemi di Intelligenza Artificiale destinati a interagire con persone fisiche come *chatbo*t siano progettati e sviluppati in modo tale rendere gli utenti consapevoli del fatto di stare interagendo con un sistema di *IA*. Viene meno questa forma di trasparenza quando è evidente

114 P. SEVERINO, *Intelligenza artificiale. Politica,economia,diritto,tecnologia,* Roma, Editore Luiss, 2022, p.164.
115 C. CASONATO, B. MARCHETTI, op. cit., *in Biolaw Journal*, 2021
116 Cfr.art.61
118 Cfr.art.62
119 Legge sull'intelligenza artificiale, Dossier n° 57 - 12 novembre 2021, Camera dei deputati - Ufficio Rapporti con l'Unione Europea, in https://documenti.camera.it.
120 G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it*, Dicembre 2021, p.27.

dalle circostanze e dal contesto che si tratta di un dispositivo di Intelligenza Artificiale e anche quando un sistema di *IA* è autorizzato dalla legge per accertare, prevenire, indagare e perseguire i reati[121]. Gli utenti che utilizzano un sistema di Intelligenza Artificiale per generare o manipolare immagini, contenuti audio o video che ritraggono persone, oggetti, luoghi o riproducono altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ("deep fake") sono tenuti a garantire l'immediata identificazione dei contenuti generati e manipolati artificialmente[122].La disposizione, in esame, che è stata prevista per combattere la disinformazione e contrastare la produzione, oramai pervasiva, di materiale illegale non si applica se l'uso è autorizzato dalla legge per rilevare, prevenire, indagare e perseguire reati o è necessario per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantite nella Carta dei diritti fondamentali dell'UE, fatte salve le adeguate garanzie per i diritti e le libertà di terzi. Da ultimo, per i sistemi a rischio minimo non rientranti pertanto nelle altre fasce di rischio dovranno essere sviluppati e utilizzati in osservanza della Legislazione vigente senza ulteriori obblighi giuridici[123].

13. ASSETTO ORGANIZZATIVO

Un aspetto fondamentale della nuova normativa è l'istituzione di un articolato e complesso sistema di *governance*[124]. Questo nuovo assetto istituzionale incardinato nel titolo VI del Regolamento è caratterizzato da due organismi distinti: uno di carattere sovranazionale ed un altro avente una connotazione nazionale. In sede comunitaria, viene istituito un Comitato europeo per l'Intelligenza Artificiale (*Board*), con funzioni analoghe al Comitato europeo per la protezione dei dati (*European Data Protection Board*), composto da rappresentanti degli Stati membri e dalla Commissione, al quale vengono attribuite diverse funzioni tra cui: favorire l'attuazione in modo agevole, efficace ed armonizzato del Regolamento; contribuire all'efficace cooperazione delle autorità nazionali e della Commissione; fornire un utile contributo consulenziale alla Commissione; mettere a disposizione della Commissione le proprie capacità tecniche; promuovere la raccolta e la condivisione delle migliori *best practices* tra gli stati membri[125]. Al livello nazionale, gli Stati membri saranno tenuti a designare una o più Autorità nazionali competenti e, tra queste, l'Autorità di controllo nazionale che sarà investita del potere di garantire l'applicazione e l'attuazione del Regolamento. L'istituita Autorità, dovrà disporre di risorse finanziarie adeguate per poter svolgere i compiti assegnati e dovrà avvalersi di personale altamente competente che abbia una comprensione approfondita in vari aspetti multidisciplinari, tra cui: tecnologie, dati e calcolo dei dati relativi all'Intelligenza Artificiale; diritti fondamentali legati all'uso dell'Intelligenza Artificiale; rischi per la salute e la sicurezza derivanti dall'utilizzo di sistemi basati sull'Intelligenza Artificiale; conoscenza delle norme e dei requisiti giuridici esistenti relativi all'Intelligenza Artificiale[126].

Tra le sue competenze rientrano, oltre quelle citate, anche il fornire orientamenti e consulenze sull'attuazione del presente Regolamento ai fornitori di piccole dimensioni ed inoltre è di sua spettanza interloquire con altre Autorità nazionali nel caso in cui intendano fornire proprie interpretazioni in settori in cui l'Intelligenza Artificiale si interseca con altre normative. All'interno del sistema di *governace* viene attribuita al Garante europeo per la

[121] Cfr.art.52
[122] G. PROIETTI, op. cit., *in www.dirittobancario.it.*
[123] F.A. NANNI, *op. cit.., in www.cyberlaws.it,* 16 giugno 2021.
[124] C. CASONATO, B. MARCHETTI, op. cit., *in Biolaw Journal*, 2021.
[125] F.A. NANNI, *op. cit..*, in www.cyberlaws.it, 16 giugno 2021
[126] Cfr.art.49.

protezione dei dati la competenza per sindacare l'operato delle Istituzioni, delle Agenzie, degli organi dell'Unione quando rientrano nella portata applicativa del Regolamento[127]. In caso di eventuali situazioni di inadempienza e di irregolarità il Garante europeo per la protezione dei dati personali è titolato a elevare sanzioni pecuniarie nei loro confronti[128]. Come ulteriore strumento di controllo la normativa prevede la configurazione e l'istallazione di una banca dati centrale, gestita dalla Commissione, al fine di raccogliere una serie di informazioni rilevanti riguardanti le caratteristiche dei sistemi, le certificazioni pertinenti e l'identità del fornitore[129]. In riferimento al tema dei controlli, la disciplina sull'*IA* promuove gli strumenti di autodisciplina, quali espressione di forme di cooregolazione e sussidarietà orizzontale, per tutti quei sistemi che non comportano un rischio inaccettabile per l'essere umano.

A tal proposito, il Regolamento all'art 69 rubricato "Codici di condotta" dispone l'intervento della Commissione e degli Stati membri per incoraggiare le parti interessare ad applicare su base volontaria i requisiti di cui al titolo III, Capo 2, inerenti i sistemi di *IA* ad alto rischio[130]. E' interessante notare, in conclusione, che il quadro normativo nel Titolo III, Capo IV, prevede l'istituzione di "organismi notificati" i quali devono essere edotti dell'introduzione dei sistemi di *IA* prima del loro utilizzo[131]. Secondo le disposizioni del Regolamento, per verificare effettivamente la conformità del sistema di *IA* alle prescrizioni, il fornitore è tenuto a inviare una notifica all'organismo notificato[132] deputato a valutare la corrispondenza rispetto agli standard e ai requisiti di sicurezza sanciti[133]. A tal fine, ogni Stato membro ha il compito di designare un'autorità di notifica che sarà responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per valutare le attività poste in essere dagli organismi poc'anzi citati.

14. TRATTAMENTO SANZIONATORIO

A norma del Regolamento, è prevista l'applicazione di sanzioni pecuniarie a carico di chi viola determinate prescrizioni o non rispetta le obbligazioni sancite nel Regolamento. Gli importi delle sanzioni possono raggiungere fino a 30 milioni di euro o corrispondere al 6% del fatturato annuo dell'azienda[134]. Questo regime sanzionatorio si applica specificamente nel caso di introduzione sul mercato o messa in funzione di sistemi di IA vietati (art. 5) o in caso di violazione delle disposizioni stabilite nell'art. 10, riguardanti *data* e *data governance* dei dati. Nell'ipotesi in cui vengano disattesi altri requisiti stabiliti per i sistemi ad alto rischio, è invece previsto un regime sanzionatorio più tenue, con una sanzione pecuniaria che può raggiungere fino ai 20 milioni di euro o corrispondere al 4% del fatturato totale dell'azienda. Nel caso di violazione degli obblighi informativi da parte dei fornitori (ai sensi dell'art. 71, comma 5) il Regolamento prevede un trattamento ancora meno incisivo e più di favore per il trasgressore, con una sanzione che ammonta a 10 milioni di euro o corrisponde al 2% del fatturato. Allo scopo di adattare il trattamento sanzionatorio al fatto concreto la normativa stabilisce che la concreta determinazione della sanzione pecuniaria si fondi su molteplici criteri: la natura, la gravità e la durata della violazione insieme alle sue

[127] F.A. NANNI, *op. cit.,* in www.cyberlaws.it, 16 giugno 2021.
[128] P.SEVERINO, op. cit., Roma, Editore Luiss, 2022, p.165.
[129] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, op. cit., *in www.i-lex.it*, Dicembre 2021, p.32.
[130] Cfr.art.69.
[131] *G.* MARCHIANO', *op. cit., in www.ambientediritto.it*, Cyberlaws,2021, p.20.
[132] Ai sensi dell'art 35 della Proposta "*La Commissione mette pubblicamente a disposizione l'elenco degli organismi notificati a norma del presente regolamento, inclusi i numeri di identificazione loro assegnati e le attività per le quali sono stati notificati. La Commissione garantisce che l'elenco sia tenuto aggiornato"*
[133] Quest' organo deve essere terzo ed indipendente rispetto rispetto al fornitore del sistema ad alto rischio, ai potenziali concorrenti e nei confronti di qualsiavoglia soggetto che abbia una cointeressenza economica nel bene.
[134] F.A. NANNI, *op. cit., in www.cyberlaws.it*, 16 giugno 2021.

postume conseguenze; si tiene conto della circostanza che l'operatore sia recidivo, avendo commesso la stessa violazione per la quale è stata già comminata una sanzione da un'altra autorità di sorveglianza; si considera, per l'irrogazione della sanzione, anche la dimensione e la quota di mercato dell'operatore che ha posto in essere la violazione[135].

Per garantire l'aderenza ai requisiti prescritti dal Regolamento, l'Autorità di sorveglianza, dopo che ha preso contezza della difformità del sistema di Intelligenza Artificiale agli standard richiesti dalla normativa, può ingiungere al soggetto interessato l'adozione di idonee misure correttive per porre fine alla violazione[136]. Inoltre, il Regolamento prevede, altresi, che l'autorità di sorveglianza può impartire al suddetto soggetto un ordine di ritiro definitivo del sistema di Intelligenza Artificiale dal mercato o di ritiro temporaneo per un periodo ragionevole, il quale sarà commisurato alla natura del rischio (art. 65, comma.2.

A seguito di queste iniziative repressive ritenute indispensabili per ristabilire lo *status quo ante* si deve notiziare la Commissione e le Autorità Nazionali competenti degli Stati membri nei quali il sistema è stato introdotto affinchè si adoperino per attivare delle misure equipollenti di salvaguardia.

È importante notare che il dettato normativo dell'articolo 72 prevede sanzioni amministrative anche per le amministrazioni pubbliche dell'Unione Europea che violano il Regolamento. L'importo massimo della misura punitiva è fissato fino a 500.000 euro per le violazioni più gravi, che riguardano la messa in servizio di Intelligenza Artificiale vietata o in contrasto con le disposizioni sulla gestione dei dati, e fino a 250.000 euro per altre non conformità rispetto ai parametri previsti per i sistemi ad alto rischio[137].

[135] Cfr.art.71.
[136] C. CASONATO, B. MARCHETTI, op. cit., *in Biolaw Journal,* 2021.
[137] Cfr.art.72.