Maggio 2021

Intelligenza artificiale: una prima analisi della proposta di regolamento europeo

Giuseppe Proietti, dottorando di ricerca, Università di Roma Tor Vergata

1. Premessa

Nel corso degli ultimi anni l'Unione Europea ha emanato una serie di atti non vincolanti volti alla definizione dell'approccio alle nuove tecnologie, in modo particolare all'intelligenza artificiale (di seguito anche IA). La premura principale – a fronte dei vantaggi, ed al contempo dei rischi, derivanti dalla sua diffusione dell'IA – risiede nella creazione di un ecosistema di fiducia per gli utenti-consumatori garantendo la sicurezza e i diritti umani, senza pregiudicare gli investimenti e la ricerca. Ciò con l'intento di preservare l'unità del mercato interno, evitando quindi una sua frammentazione. Si inserisce esattamente in questa dimensione tattica l'ultima iniziativa della Commissione europea nell'ambito della strategia sull'innovazione, la quale risalta per la sua importanza giacché costituisce la prima iniziativa con cui si concretizza quell'approccio che fino al 21 aprile scorso veniva stilato solamente a livello programmatico.

L'emanazione della proposta di regolamento sull'intelligenza artificiale – o *artificial intelligence act* – rappresenta la prima iniziativa legislativa al mondo con la quale si ambisce ad una regolamentazione generale di tale tecnologia[1] e uno degli

[1] "*Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*". COM(2021) 206 final. Reperibile su: https://ec.europa.eu/transparency/regdoc/rep/1/2021/EN/COM-2021-206-F1-EN-MAIN-PART-1.PDF
La proposta di Regolamento in questione, anche per la sua complementarità, è stata accompagnata dalla proposta di "Regolamento macchine" reperibile su: https://ec.europa.eu/docsroom/documents/45508
Durante la conferenza di presentazione della proposta di regolamento, il commissario europeo T. Breton, cogliendo un delicato aspetto dell'era della tecnica, ha dichiarato che «*l'intelligenza artificiale è un mezzo, non un fine*»; un assunto che rientra nella *ratio* della proposta legislativa, ma che rischia di sottovalutare «*l'autonomia della tecnica dalle finalità che gli uomini si propongono, per cui gli uomini diventano sempre più appendici della strumentazione che producono* (…) *Con l'autonomizzarsi del mezzo, infatti, con il suo assurgere a condizione universale per la realizzazione di qualsiasi fine, si assiste alla subordinazione di ogni fine all'incremento dell'apparato dei mezzi in cui la tecnica consiste*.». U. GALIMBERTI, *Psiche e techne. L'uomo nell'età della tecnica*, Feltrinelli, 2019, p.330.

obiettivi è quello di ridurre il divario esistente con altri Stati in termini di sviluppo e investimenti[2].

Il perimetro applicativo che l'IA già oggi occupa, la sua multiformità ed il suo dinamismo - oltre al margine di imprevedibilità – manifestano limpidamente la difficoltà di prefigurare un quadro legislativo capace di rintracciare un equilibrio a tutti gli elementi e gli interessi di volta in volta in gioco. In uno scenario simile, perciò, in un contesto interdisciplinare, qualsiasi iniziativa legislativa si presterebbe ad inevitabili critiche e dibattiti.

I profili che la proposta di regolamento affronta sono copiosi e per molti aspetti controversi e delicati. Tra i vari temi v'è quello della definizione dell'IA, la sua classificazione a seconda della tipologia di rischio, i requisiti che alcuni sistemi, ad alto rischio, debbono rispettare, nonché l'iter di convalida e certificazione, sino agli obblighi in capo ad alcuni soggetti facenti parte della catena del valore e al sistema di *governance*. Il profilo attinente alla responsabilità (*rectius*, alla natura o al grado di responsabilità) non viene affrontato in modo diretto, richiamando un futuro intervento della Commissione sul punto, benché il contenuto della proposta fornisca inevitabilmente indicazioni indirette.

Dunque, ancorché il percorso di regolamentazione si presenti ai suoi arbori, sia per i lunghi tempi di approvazione di un testo legislativo, ma ancor più per i suoi riflessi applicativi, ci si presta ad una prima analisi di alcune delle principali questioni sollevate dalla proposta in commento.

2. Il lungo percorso europeo

La prima iniziativa europea nel settore può essere individuata nella risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica[3]. Tale risoluzione, sebbene sembri riferirsi esclusivamente alla robotica, si dedica in senso lato alle più recenti realtà tecnologiche. Con tale atto, il Parlamento si prefigge lo scopo europeo di individuare un equilibrio che sostenga l'innovazione e la competitività industriale mantenendo al contempo un'elevata sicurezza e tutela dei diritti e libertà dei cittadini.

Nei mesi di febbraio - aprile del 2018 la Commissione europea dal canto suo emanava la relazione *Re-finding industry, Report from the High-Level Strategy Group on Industrial*

[2] Negli stessi giorni - ossia il 19 aprile 2021 - negli USA la Federal Trade Commission emanava raccomandazioni in materia di utilizzo di strumenti IA. Si veda *Aiming for truth, fairness, and equity in your company's use of AI.* reperibile su: https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai

[3] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), Reperibile su: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52017IP0051

Technologies, con cui delineava una ridefinizione dell'industria europea alla luce delle nuove sfide emergenti dalle tecnologie[4].

Nello stesso periodo del 2018, con l'istituzione dell'*European Group on Ethics in Science and New Technologies*, la Commissione europea emanava la relazione *Artificial Intelligence, Robotics and 'Autonomous' Systems*, con l'intento di descrivere le problematiche derivanti dai più recenti sviluppi tecnologici, esaminando e ponendo in risalto le implicazioni etiche e morali[5].

Con la comunicazione del 25 aprile del 2018 dal titolo "L'intelligenza artificiale per l'Europa" la Commissione europea delineava gli obiettivi di investimento, legislativi ed etici nell'ambito del quadro dell'innovazione europea e nel mondo[6].

Il 7 dicembre 2018 veniva invece pubblicato "il piano coordinato sull'intelligenza artificiale"[7] con cui si è elaborato un piano di ampio respiro, focalizzato in particolare sul tema degli investimenti europei per lo sviluppo di nuove tecnologie in virtù delle loro peculiarità e dell'attuale svantaggio competitivo rispetto ad altri Stati mondiali.

Ancora. Gli ulteriori atti che meritano menzione riguardano gli aspetti di natura etica ineluttabilmente coinvolti. Ci si riferisce in particolare agli orientamenti etici per una IA affidabile, elaborati dal gruppo di esperti ad alto livello[8] e la conseguente comunicazione della Commissione europea "Creare fiducia nell'intelligenza artificiale antropocentrica" con la quale venivano fatti propri tali orientamenti[9], la relazione elaborata dal centro comune di ricerca della Commissione europea *Artificial Intelligence: a European*

---

[4] *Re-finding industry, Report from the High-Level Strategy Group on Industrial Technologies*, relazione reperibile su: https://op.europa.eu/en/publication-detail/-/publication/28e1c485-476a-11e8-be1d-01aa75ed71a1

[5] *Artificial Intelligence, Robotics and 'Autonomous' Systems*, documento Reperibile su: https://op.europa.eu/en/publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1

[6] *L'intelligenza artificiale per l'Europa*, Comunicazione Reperibile su: https://ec.europa.eu/transparency/regdoc/rep/1/2018/IT/COM-2018-237-F1-IT-MAIN-PART-1.PDF
Nelle conclusioni, pag. 20, si legge che: «*L'approccio all'IA descritto nel presente documento mostra la strada da seguire ed evidenzia la necessità di unire le forze a livello europeo, per assicurare che tutti i cittadini europei partecipino alla trasformazione digitale, che risorse adeguate siano dedicate all'IA e che i valori e i diritti fondamentali dell'Unione siano in primo piano nel contesto dell'IA.*»

[7] *Il piano coordinato sull'intelligenza artificiale*, reperibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018DC0795
Su questo piano si è altresì pronunciato il Consiglio d'Europa con il documento "*Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption 6177/19*", 201, reperibile su: https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf

[8] *Orientamenti etici per una IA affidabile*, documento pubblicato l'8 aprile 2019 e reperibile su: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[9] *Creare fiducia nell'intelligenza artificiale antropocentrica*, Comunicazione Reperibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019DC0168&from=GA

Perspective e la relazione *Liability for artificial intelligence and other emerging digital technologies*[10].

L'ultimo atto importante della Commissione europea - che ha rappresentato il preludio all'emanazione della proposta di regolamento in commento - è il "libro bianco sull'intelligenza artificiale - un approccio europeo all'eccellenza e alla fiducia" pubblicato il 19 febbraio 2020[11].

Le ultime sollecitazioni alla Commissione per un intervento legislativo nella materia sono intervenute da parte del Parlamento europeo e dal Consiglio d'Europa. Quest'ultimo, con il documento pubblicato il 2 ottobre 2020 ha sottolineato l'importanza – in un quadro legislativo - di determinare quelle IA da considerare ad alto rischio[12]. In un secondo documento, del 21 ottobre 2021, *The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, il Consiglio d'Europa ha posto l'attenzione sulle problematiche e i rischi derivanti dall'opacità, dalla complessità dei sistemi di IA e dai pregiudizi che generano un ampio grado di imprevedibilità affinché sia garantita la compatibilità degli stessi con i diritti fondamentali[13].

Il Parlamento Europeo, invece, è recentemente intervenuto con la risoluzione del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate[14]

---

[10] *Artificial Intelligence: a European Perspective e la relazione Liability for artificial intelligence and other emerging digital technologies*, relazione reperibile su: https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en/format-PDF

[11] *White paper* reperibile su: https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en
Sui temi affrontati nel documento si veda quanto esposto dallo scrivente in *Il libro bianco sull'intelligenza artificiale. L'approccio europeo tra diritto ed etica*, in Giustiziacivile.com, 24 giugno 2020.

[12] Documento reperibile su: https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf

[13] Council of the European Union, Presidency conclusions - *The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 11481/20, 2020. Reperibile su: https://www.consilium.europa.eu/media/46496/st11481-en20.pdf

[14] Risoluzione reperibile su: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_IT.html#title1
Il Parlamento, al paragrafo 12 della risoluzione, rileva in particolare che: «(…) *qualsiasi regolamentazione futura dovrebbe seguire un approccio basato sui rischi e orientato al futuro, onde regolamentare l'intelligenza artificiale, la robotica e le tecnologie correlate, tra cui norme tecnologicamente neutre trasversali a tutti i settori e, se del caso, norme settoriali specifiche; osserva che, al fine di garantire un'attuazione uniforme del sistema di valutazione del rischio e il rispetto dei relativi obblighi giuridici per garantire parità di condizioni tra gli Stati membri ed evitare la frammentazione del mercato interno, è necessario un elenco esaustivo e cumulativo di settori ad alto rischio e di usi o scopi ad alto rischio; sottolinea che tale elenco deve essere oggetto di una rivalutazione periodica e osserva che, data la natura evolutiva di tali tecnologie, il modo in cui viene effettuata la loro valutazione del rischio potrebbe dover essere rivalutato in futuro*».

e, in pari data, con la Risoluzione recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale[15].

Gli interventi, costituiti da relazioni, comunicazioni e risoluzioni da parte delle istituzioni europee sono stati numerosi ed hanno condotto alla proposta di regolamento in commento.

3. L'*Artificial Intelligence Act*

3.1 Il quadro generale

L'obiettivo della Commissione è quello di procedere in questo settore mediante un'azione comune europea che assicuri il buon funzionamento del mercato interno e governi adeguatamente i rischi e i benefici dell'IA.

L'oggetto del regolamento proposto, ovvero il suo ambito oggettivo, lo si ricava dall'art. 1. Tale disposizione prescrive che il regolamento sancisce norme riguardanti l'immissione sul mercato, la messa in servizio e l'utilizzo di sistemi di intelligenza artificiale, il divieto di alcune pratiche mediante l'utilizzo di specifici sistemi IA, particolari requisisti per i sistemi ad alto rischio e gli obblighi per i loro operatori, nonché le regole di trasparenza per alcuni sistemi IA progettati per interagire con persone fisiche.

Dunque, gli scopi perseguiti risiedono nel garantire che i sistemi di IA utilizzati e immessi sul mercato europeo siano sicuri e rispettosi dei diritti fondamentali e valori europei, assicurando la certezza del diritto in modo da agevolare gli investimenti in materia di innovazione. Stando a quanto affermato dalla Commissione, il quadro normativo che si intende costruire riguarda un sistema proporzionato e incentrato su un approccio fondato sul rischio che non crei restrizioni inutili al commercio, per cui l'intervento legislativo sarebbe previsto per quelle situazioni in cui sussista un giustificato motivo o laddove tale motivo possa essere ragionevolmente previsto per il prossimo futuro. Allo stesso tempo, il quadro giuridico intende includere meccanismi flessibili che consentirebbero un adattamento dinamico, a seconda dell'evoluzione della tecnologia[16].

Le norme che vengono proposte verrebbero applicate tramite un sistema di *governance* a livello di Stati membri, sulla base di strutture già esistenti, e un meccanismo di cooperazione a livello di Unione con l'istituzione di un Comitato europeo per l'intelligenza artificiale simile al comitato già esistente in materia di dati personali[17]. Va

[15] Risoluzione reperibile su: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html
[16] Proposta regolamento, p. 3.
[17] Tale Comitato, come previsto dal titolo VI della proposta di regolamento, fornirebbe assistenza alla Commissione per (a) contribuire all'efficace cooperazione tra le autorità nazionali di controllo e la Commissione per quanto concerne la materia disciplinata dal regolamento; (b) coordinare e contribuire all'orientamento e all'analisi da parte della Commissione, nonché delle autorità nazionali di vigilanza e di altre autorità competenti, sule questioni emergenti nel mercato interno per quanto riguarda le questioni disciplinate dal regolamento; (c) assistere le autorità nazionali di vigilanza e la Commissione nel garantire una coerente applicazione del regolamento.

da sé che il sistema di *governance* stabilito nella proposta ha carattere generale ed astratto e per la sua attuazione ci si potrebbe interrogare su una sua composizione multidisciplinare.

Vengono inoltre proposte misure aggiuntive a sostegno dell'innovazione, in particolare attraverso c.d. *regulatory sandbox*[18] – ossia spazi di sperimentazione normativa- in materia di intelligenza artificiale e altre misure per ridurre gli oneri e sostenere le piccole e medie imprese e le start-up[19].

La Commissione evidenzia altresì la necessità di mantenere un impianto normativo coerente con la legislazione europea vigente ed applicabile ai settori dove i sistemi di IA ad alto rischio vengono già utilizzati o verranno utilizzati nel prossimo futuro. Una connessione e integrazione normativa viene operata anche in relazione alla legislazione macchine, talché la proposta di regolamento è stata adottata simultaneamente alla proposta in materia di regolamento macchine.

La compatibilità del regolamento viene assicurata anche in ordine ad una serie di iniziative legislative in corso o già pianificate da parte della Commissione che perseguono l'obiettivo di affrontare, tra gli altri, le questioni riguardanti la responsabilità in relazione alle nuove tecnologie, inclusi i sistemi di intelligenza artificiale. Inoltre, la promozione dell'innovazione basata sull'intelligenza artificiale è strettamente collegata al *Data Governance Act*[20], alla direttiva sui dati aperti[21] e ad altre iniziative nell'ambito della strategia dell'UE per i dati[22], che istituiranno meccanismi e servizi affidabili per il riutilizzo, la condivisione e la messa in comune dei dati essenziali per lo sviluppo di modelli di intelligenza artificiale basati sui dati di alta qualità[23].

La disciplina principale – in cui si incentra il regolamento proposto – concerne i sistemi di IA ad alto rischio. La suddivisione del rischio, sebbene non esplicitata nella proposta,

[18] Il Titolo V del regolamento è dedicato a tali misure di supporto. L'art. 53 prevede che le *sandbox* normative per l'IA, istituite dalle autorità competenti di uno o più Stati membri o dal garante europeo della protezione dei dati, devono fornire un ambiente controllato che faciliti lo sviluppo, la verifica e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o messa in servizio secondo uno specifico piano. Ciò avviene sotto la diretta supervisione delle autorità competenti per garantire la conformità ai requisiti del regolamento.
[19] Proposta regolamento, p. 3.
[20] Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767
[21] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83
[22] Commission Communication, A European strategy for data COM/2020/66 final
[23] Proposta regolamento, p. 5.

viene convenzionalmente operata con un discernimento in quattro differenti livelli. Il rischio inaccettabile, l'alto rischio, il rischio limitato[24] e il rischio minimo[25].

La proposta legislativa è stata pubblicata congiuntamente all'aggiornamento completo del piano coordinato del 2018 il quale ha come obiettivo programmatico quello di creare le condizioni favorevoli allo sviluppo e all'adozione dell'IA mediante lo scambio di informazioni strategiche, la condivisione dei dati, la promozione dell'eccellenza in materia di IA istituendo un partenariato pubblico-privato, costruendo e mobilitando capacità di ricerca, sviluppo e innovazione e mettendo a disposizione delle PMI e delle pubbliche amministrazioni strutture di prova e sperimentazione nonché poli dell'innovazione digitale[26].

3.2 La disciplina normativa

Il titolo I della proposta è dedicato alle disposizioni generali. Secondo l'art. 2, il regolamento trova applicazione in riferimento a quei fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, indipendentemente dal fatto che essi siano stabiliti nell'Unione europea o in un paese terzo; agli utilizzatori di sistemi di intelligenza artificiale situati all'interno dell'UE; ai fornitori e agli utenti di tali sistemi che si trovano in un paese terzo quando gli effetti di ciò che viene prodotto si ripercuotono nell'UE. Viene esclusa l'applicazione del regolamento per quei sistemi sviluppati o utilizzati esclusivamente per scopi militari, oltreché per le autorità pubbliche di un paese terzo e le organizzazioni internazionali se utilizzano sistemi di IA nel quadro di accordi internazionali.

L'art. 3, invece, è particolarmente delicato in quanto stabilisce le definizioni rilevanti ai fini del regolamento. Tra le più importanti rientra proprio quella di intelligenza artificiale. Viene stabilito che per "sistema di intelligenza artificiale" si intende quel software sviluppato in una o più delle modalità e approcci di cui all'Allegato I del Regolamento e che sia in grado di generare risultati come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce alla luce degli obiettivi definiti dall'uomo. L'allegato in questione riporta tre gruppi di tecnologie. Alla lettera a) viene riportato il *machine learning* e *deep learning*; la lett. b) individua quelle tecnologie basate sulla logica e sulla conoscenza, sulla programmazione (logica) induttiva, le basi della conoscenza, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti, la lett. c) fa riferimento invece agli approcci statistici, di ricerca e alla stima Bayesiana.

[24] Sistemi di IA per i quali ci si limita a prevedere specifici obblighi di trasparenza.
[25] È consentito il libero utilizzo di tali applicazioni (videogiochi o filtri spam basati sull'IA). Non è previsto alcun intervento per queste ipotesi in quanto tali sistemi di IA presentano solo un rischio minimo o nullo per i diritti o la sicurezza dei cittadini.
[26] Il cd. *Coordinated Plan on Artificial Intelligence 2021 Review* è reperibile su: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

Il considerando 6 prevede che la nozione di IA dovrebbe essere definita in modo da garantire la certezza del diritto e fornendo allo stesso tempo la flessibilità necessaria per accogliere i futuri sviluppi tecnologici. Essa dovrebbe fondarsi sulle caratteristiche funzionali del software, in particolare sulla capacità, per un dato insieme di obiettivi definiti dall'uomo, di generare *output* quali contenuti, previsioni, raccomandazioni o decisioni in grado di influenzare l'ambiente con cui il sistema interagisce, sia in una dimensione fisica che digitale. I sistemi di intelligenza artificiale – prosegue il considerando - possono essere progettati per funzionare con diversi livelli di autonomia ed essere utilizzati in modo autonomo o come componente di un prodotto, indipendentemente dal fatto che il sistema sia fisicamente integrato come parte del prodotto finale (incorporato) o serva la funzionalità del prodotto senza essere integrato (non incorporato).

Viene offerta anche la definizione di fornitore ("*provider*"), il quale sarebbe il soggetto, persona fisica o giuridica, che sviluppa un sistema di IA o che lo possiede e che ha come obiettivo quello di immetterlo sul mercato sotto il proprio nome o marchio, sia a titolo oneroso che gratuito. L'assenza del *developer*, ossia dello sviluppatore, lascerebbe intendere la volontà di considerare nell'unica figura del fornitore colui che sviluppa il sistema o che – sebbene sviluppato da altri –si appresti ad immetterlo sul mercato sotto il proprio nome. L'utente, o l'utilizzatore, ("*user*") viene identificato nel soggetto, persona fisica o giuridica, che utilizza il sistema di IA quando esso è sotto la sua autorità (o custodia), ad eccezione dell'ipotesi in cui tale utilizzo avvenga per uno scopo esclusivamente personale e non di natura professionale.

3.2.1 Il rischio inaccettabile

Il titolo II è particolarmente delicato in quanto definisce quel primo livello di rischio in cui viene operato il discernimento, ossia il rischio inaccettabile. All'art. 5, vengono stabiliti quei divieti per alcune pratiche realizzate con alcune tecnologie di intelligenza artificiale.

Vengono sostanzialmente proibite quattro pratiche. La prima, dal tenore vago, concerne l'immissione sul mercato, la messa in servizio o l'uso di un sistema di intelligenza artificiale che attua tecniche subliminali con il fine di falsare inconsciamente il comportamento di una persona in un modo che provochi o possa provocare danni a quella o altra persona. Una pratica contemplata nell'ambito di un contenitore normativo che probabilmente necessiterebbe una definizione più circoscritta.

La seconda, anch'essa vaga, concerne l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA capace di sfruttare una vulnerabilità legata ad un gruppo particolare di persone per la loro età, disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona appartenente a quel gruppo e in modo tale da provocare potenziali danni fisici o psicologici.

La terza, fondamentale nella sua previsione, riguarda il divieto del cd. *Social scoring* o *Social credit system*. La pratica proibita concerne l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche per la valutazione o la classificazione dell'affidabilità delle persone in un determinato periodo di tempo e sulla base del loro comportamento sociale o della personalità, prevedendo quindi un punteggio sociale che porta a 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. L'intento è meritevole ed è chiaramente quello di evitare che si possa giungere al fenomeno di *social scoring* già presente in alcuni Stati. Nel considerando 17 vengono puntualizzati i rischi che potrebbero derivare da un sistema di tal fatta, ossia le conseguenze discriminatorie e l'esclusione sociale di alcune minoranze o gruppi, violando quindi la dignità umana[27].

La quarta e ultima pratica vietata riguarda l'uso di sistemi di identificazione biometrica remota e "in tempo reale", in spazi accessibili al pubblico, ad eccezione di quei casi in cui l'uso sia strettamente necessario per alcuni obiettivi: (i) la ricerca mirata di specifiche e potenziali vittime di reati, compresi bambini scomparsi; (ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o per l'incolumità fisica delle persone o in caso di attacco terroristico; (iii) per l'individuazione, la localizzazione, l'identificazione o il perseguimento di un autore o sospettato di alcuni reati in particolare punibile nello Stato membro interessato con una pena detentiva per un periodo massimo di almeno tre anni.

Nell'ambito delle possibilità di utilizzo di questi sistemi di identificazione, il paragrafo successivo prevede la necessità di considerare la natura della situazione che ha dato origine al suo possibile utilizzo, in particolare la gravità, la probabilità e l'entità del danno che verrebbe causato senza l'utilizzo del sistema; le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, e in particolare la gravità, la probabilità e la portata di tali conseguenze.

L'ultimo paragrafo dell'art. 5 concede inoltre la facoltà agli stati membri di determinare specifiche ipotesi e situazioni in cui l'utilizzo di tali sistemi sarebbe lecito e quindi consentito.

Nel considerando n. 8 si tenta di fornire una nozione di sistema di identificazione biometrica a distanza e di operare il discernimento tra identificazione in tempo reale e

[27] Il considerando prosegue rilevando come tali sistemi di IA verrebbero utilizzati per valutare o classificare l'affidabilità delle persone in base al loro comportamento sociale in più contesti o secondo le caratteristiche personali. Il punteggio sociale ottenuto da tali sistemi di IA può causare un trattamento dannoso o sfavorevole nei confronti di soggetti o di interi gruppi in contesti sociali non correlati al contesto in cui i dati sono stati originariamente generati o raccolti.

identificazione *ex post*. Si tratta sostanzialmente di un sistema IA teso a identificare persone fisiche a distanza mediante il confronto dei suoi dati biometrici con quelli già contemplati all'interno di una banca dati di riferimento. Va da sé che nel caso di sistemi "*real-time*", l'acquisizione dei dati biometrici, il confronto e l'identificazione avvengono tutti istantaneamente o comunque senza ritardi significativi. Nel caso dei sistemi che consentono una identificazione "*ex post*", invece, i dati biometrici sono già stati acquisiti e il confronto e l'identificazione avvengono solo in un secondo momento. Nello stesso considerando, si precisa che si tratta di materiale, come immagini o riprese video generate da telecamere a circuito chiuso o dispositivi privati, acquisito prima dell'uso del sistema nei confronti delle persone fisiche interessate[28].

La disciplina dettata per la tecnologia dei sistemi di identificazione biometrica a distanza è la prima ad aver suscitato critiche immediate. In particolare, l'EDPS, salutando con favore l'iniziativa europea volta a regolare la materia dell'IA, rileva la necessità di un divieto assoluto dell'identificazione biometrica[29]. Nel comunicato si legge infatti che *«(…) the EDPS regrets to see that our earlier calls for a moratorium on the use of remote biometric identification systems - including facial recognition - in publicly accessible spaces have not been addressed by the Commission.*

The EDPS will continue to advocate for a stricter approach to automated recognition in public spaces of human features - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - whether these are used in a commercial or administrative context, or for law enforcement purposes. A stricter approach is necessary given that remote biometric identification, where AI may contribute to unprecedented developments, presents extremely high risks of deep and non-democratic intrusion into individuals' private lives.».

La tecnologia di cui si discetta – già utilizzata in molte parti del mondo con diversi gradi di pervasività[30] – è una delle più dibattute, costituendo il nucleo centrale anche in precedenti comunicazioni europee come nel caso del Libro bianco sull'IA.

3.2.2 I sistemi ad alto rischio

Il titolo III è dedicato specificatamente ai sistemi IA ad alto rischio e costituisce il nucleo centrale dell'intero regolamento.

[28] Le nozioni di Sistema di identificazione remota, nonché di sistema di identificazione in tempo reale ed ex post vengono formulate nell'art. 3 della proposta ai n. 36, 37 e 38.
[29] "*Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*", 23 Apr 2021, reperibile su: https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en
[30] Per un quadro tangibile sulla diffusione della tecnologia del riconoscimento facciale (ed altri strumenti) da parte delle forze dell'ordine negli USA, e della loro applicazione geografica, si veda la piattaforma *Atlas Surveillance*: https://atlasofsurveillance.org/

Il soggetto che intende immettere sul mercato un sistema appartenente a tale categoria è tenuto a rispettare ed osservare determinate e rigorose fasi prestabilite. Infatti, il prodotto deve essere sottoposto ad una valutazione di conformità e deve soddisfare requisiti specifici e per alcuni sistemi è coinvolto un apposito organismo. Per alcuni sistemi di IA autonomi è prevista la registrazione in una banca dati dell'UE accessibile al pubblico. È necessario altresì sottoscrivere una dichiarazione di conformità e il sistema deve riportare la marcatura CE.

È considerato ad alto rischio, ai sensi dell'art. 6, quel sistema di IA che (a) viene utilizzato come componente di un prodotto, o che è esso stesso un prodotto rientrante in una delle discipline normative europee di cui all'allegato II del regolamento; (b) il prodotto che, per l'immissione sul mercato o per la messa in servizio, viene sottoposto ad una valutazione di conformità da parte di soggetti terzi. Inoltre, al par. 2, è previsto che debbono essere considerati ad alto rischio quei sistemi di cui all'allegato III del regolamento.

Quest'ultimo allegato contiene un elenco di ambiti in cui potrebbe essere utilizzata la tecnologia in questione. Viene menzionata ad esempio l'area della pubblica sicurezza, dell'accesso ai servizi pubblici e privati essenziali[31], dei trasporti[32], dell'occupazione[33],

[31] Ci si riferisce in particolare all'accesso al credito e alla valutazione dell'affidabilità creditizia che può negare ai cittadini la possibilità di ottenere un prestito. Tali sistemi, come specificato nel considerando 37, possono causare forme di discriminazione tra persone o gruppi di persone fondate sulle origini razziali o etniche, disabilità, età, orientamento sessuale o generare nuove forme di discriminazione. Nello stesso considerando si rileva la necessità di esentare da tali limitazioni – per il loro minimo impatto sul mercato e per la disponibilità di alternative – per l'uso proprio da parte di fornitori di piccole dimensioni. Nell'ambito dei servizi pubblici erogati da autorità pubbliche, se i sistemi di IA vengono utilizzati per determinare se ammettere, negare ridurre o negare tali benefici e servizi potrebbe verificarsi un impatto significativo sul sostentamento delle persone e potrebbero essere violati i loro diritti. Tali sistemi dovrebbero pertanto essere classificati come ad alto rischio. Tuttavia, come precisato nel considerando, il regolamento non dovrebbe ostacolare lo sviluppo e l'uso di approcci innovativi nella p.a., a condizione che tali sistemi non comportino un rischio elevato per le persone. Infine, i sistemi di IA utilizzati per inviare o stabilire priorità nell'invio di servizi di pronto intervento di emergenza dovrebbero essere classificati come ad alto rischio poiché prendono decisioni in situazioni molto critiche per la vita e la salute delle persone e dei loro beni.

[32] Nell'ambito delle infrastrutture critiche, come precisato anche nel considerando 34, vengono classificati ad alto rischio tutti quei sistemi che costituiscono delle componenti di sicurezza nella gestione della circolazione stradale, così come nella fornitura di acqua, gas ed elettricità. La ragione della classificazione risiede nel pericolo derivante agli interessi e diritti primari delle persone.

[33] Il considerando 36 prevede che i sistemi IA utilizzati nel settore del lavoro, in particolare per l'assunzione e la selezione di persone, ovvero per assumere decisioni sulla promozione e assegnazione di posizioni, per il monitoraggio o per la valutazione dei compiti dei lavoratori, debbono essere classificati ad alto rischio, poiché possono avere un impatto significativo sulle prospettive di carriera futura e sui mezzi di sussistenza di queste persone. Durante il processo di reclutamento e nella valutazione o promozione di persone nei rapporti di lavoro, tali sistemi possono attuare modelli di discriminazione, ad esempio contro donne, determinate fasce di età, persone con disabilità o persone di determinate razze o origini etniche o orientamento sessuale. I sistemi di intelligenza artificiale utilizzati per monitorare le prestazioni e il comportamento di queste persone possono anche influire sui loro diritti alla protezione dei dati e alla privacy.

dell'asilo ed immigrazione, dell'istruzione[34] e dell'amministrazione della giustizia[35]. All'interno di ciascuna delle aree menzionate viene specificato lo scopo per il quale potrebbe essere utilizzato il sistema di IA.

L'art. 7 della proposta conferisce alla Commissione europea il potere di adottare atti delegati volti all'aggiornamento della lista di cui all'allegato III allorché vengano soddisfatti due requisiti: (a) che l'uso dei sistemi di IA rientri in uno dei settori elencati ai punti da 1 a 8 dell'allegato III; (b) che i sistemi comportino un rischio di danno alla salute e alla sicurezza, o un rischio di impatto negativo sui diritti fondamentali, vale a dire, in relazione alla sua gravità e probabilità di accadimento, equivalente o superiore al rischio di impatto negativo posto dai sistemi contemplati nell'allegato III. La Commissione è tenuta a considerare diversi criteri per questa valutazione: (a) lo scopo perseguito dal sistema di IA; (b) il perimetro di utilizzo del sistema di intelligenza artificiale; (c) se il sistema di IA abbia già causato un danno alla salute e alla sicurezza o comunque un impatto negativo sui diritti fondamentali o abbia dato adito a preoccupazioni significative in relazione alla verificazione di tale danno o impatto negativo; (d) la portata 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.

Il capo II è dedicato alla disciplina dei requisiti che i sistemi ad alto rischio devono soddisfare.

È prevista l'implementazione di un sistema di gestione del rischio proveniente dall'IA per l'intero ciclo di vita dello stesso, sistematicamente aggiornato e strutturato in quattro fasi: (a) identificazione e analisi dei rischi noti e prevedibili associati a ciascun sistema ad alto rischio; (b) stima e valutazione dei rischi che possono emergere quando il sistema

[34] Come precisato nel considerando 35, debbono essere considerati ad alto rischio quei sistemi IA utilizzati nell'istruzione o nella formazione professionale, in particolare quei sistemi volti a determinare l'accesso all'istruzione e il percorso professionale di una persona. Se progettati e utilizzati in modo improprio, tali sistemi possono violare il diritto all'istruzione e alla formazione, nonché il diritto a non essere discriminati.
[35] Il considerando 40 prevede che alcuni sistemi di IA destinati all'amministrazione della giustizia e dei processi democratici debbono essere classificati come ad alto rischio in virtù del loro impatto potenzialmente significativo sulla democrazia, sullo Stato di diritto e sulle libertà individuali, nonché sul diritto a un ricorso effettivo e a un processo equo. In particolare, per affrontare i rischi di potenziali pregiudizi, errori ed opacità, è opportuno qualificare come ad alto rischio quei sistemi progettati per assistere le autorità giudiziarie nella ricerca e nell'interpretazione dei fatti e della legge. Tale classificazione, tuttavia, non dovrebbe tuttavia riguardare i sistemi di IA destinati ad attività amministrative puramente accessorie che non incidono sull'effettiva amministrazione della giustizia in casi particolari.

è utilizzato in conformità allo scopo previsto e in condizioni d'uso improprio che possano essere ragionevolmente previste; (c) valutazione di altri rischi che possono sorgere sulla base dell'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato; (d) adozione di misure di gestione dei rischi adeguate. Tali misure devono essere tali da far qualificare accettabile qualsiasi rischio residuo, a condizione che il sistema venga utilizzato in conformità allo scopo previsto. Siffatti rischi residui devono in ogni caso essere comunicati all'utente.

Nell'individuazione delle più appropriate misure di gestione del rischio, occorre garantire: a) l'eliminazione o la riduzione dei rischi per quanto possibile mediante una progettazione e uno sviluppo adeguati; b) l'attuazione di adeguate misure di mitigazione e di controllo in relazione a quei rischi che non possono essere eliminati; c) la trasmissione di adeguate informazioni all'utente e, se opportuno, la loro formazione.

Nella valutazione dell'attuazione di misure di riduzione o di eliminazione dei rischi occorre tenere in considerazione la conoscenza tecnica, l'esperienza, l'istruzione e la formazione che ci si può attendere da parte dell'utente.

I sistemi ad alto rischio debbono essere sottoposti a specifici test. Le procedure in questione debbono essere idonee al raggiungimento dello scopo perseguito con il sistema, senza travalicare le necessità per il raggiungimento dello stesso.

La verifica dei sistemi di IA ad alto rischio deve essere in ogni caso eseguita prima dell'immissione sul mercato o della messa in servizio. I test devono essere effettuati in base a metriche definite in via preliminare e soglie appropriate allo scopo previsto per quel sistema ad alto rischio.

L'art. 10 prescrive particolari procedure di verifica per quei sistemi di IA ad alto rischio che fanno uso di particolari tecniche che implicano l'addestramento di modelli di dati.

L'articolo successivo prescrive, invece, la redazione e l'aggiornamento di una documentazione tecnica prima che il sistema di IA ad alto rischio sia immesso sul mercato o messo in servizio. Tale documentazione deve essere redatta in modo da poter dimostrare che il sistema ad alto rischio sia conforme ai requisiti prescritti nel capo II, titolo III, del Regolamento, fornendo dunque alle autorità nazionali competenti, e agli altri organismi, tutte le informazioni necessarie per valutare la conformità del sistema[36].

L'articolo 12 prevede che i sistemi di IA ad alto rischio devono essere progettati e sviluppati con capacità tali da consentire la registrazione automatica degli eventi ("*log*") che si verificano mentre sono in funzione.

L'art. 13 prescrive gli obblighi di trasparenza per i sistemi ad alto rischio. Essi debbono essere progettati e sviluppati in modo che possano garantire un funzionamento sufficientemente trasparente, permettendo agli utenti di interpretare correttamente i

[36] Il contenuto deve essere almeno quello di cui agli elementi presenti nell'allegato IV del Regolamento.

risultati del sistema e utilizzarli in modo appropriato. Non solo. Debbono essere accompagnati da apposite istruzioni per il loro utilizzo che specifichino alcuni elementi tra cui le caratteristiche, le capacità e i limiti di *performance* del sistema, incluso lo scopo perseguito, il livello di accuratezza e robustezza; ogni circostanza conosciuta o conoscibile relativa al loro uso e parametrato allo scopo perseguito, nonché al loro eventuale abuso e ai rischi che ne potrebbero derivare alla salute e ai diritti umani in generale; il ciclo di vita atteso per quel sistema e ogni misura necessaria per il mantenimento e per assicurare un appropriato funzionamento.

In tema di sorveglianza umana, l'art. 14 prevede che i sistemi ad alto rischio devono essere progettati e sviluppati in modo che - anche con opportuni strumenti di interfaccia uomo-macchina - possano essere efficacemente sorvegliati da persone fisiche durante il periodo in cui il sistema AI è in uso. L'art. 15 prescrive che il sistema ad alto rischio deve essere progettato e sviluppato in un modo tale che raggiunga un "appropriato" livello di accuratezza, robustezza e sicurezza.

Il capo III è dedicato agli obblighi per gli operatori. In particolare, agli obblighi previsti in capo ai fornitori, agli utenti ed altri soggetti legati ai sistemi ad alto rischio. All'art. 16 è previsto che i fornitori dei sistemi ad alto rischio sono tenuti a: (a) garantire che i loro sistemi siano conformi ai requisiti stabiliti nel capo II; (b) disporre di un sistema di gestione della qualità come stabilito nell'articolo 17[37]; (c) redigere la documentazione tecnica del sistema di IA ad alto rischio; (d) quando sono sotto il loro controllo, conservare i registri generati automaticamente dai loro sistemi di IA ad alto rischio; (e) garantire che il sistema di IA ad alto rischio sia sottoposto alla pertinente procedura di valutazione della conformità prima della sua immissione sul mercato; (f) ottemperare agli obblighi di registrazione previsti all'articolo 51; (g) realizzare le azioni correttive necessarie nel caso in cui il sistema ad alto rischio non fosse conforme ai requisiti di cui al suddetto capo II; (h) informare le autorità nazionali competenti degli Stati membri in cui hanno messo a disposizione il sistema di IA e, se del caso, l'organismo competente in ordine alla difformità ed alle eventuali azioni correttive intraprese; (i) apporre il marchio CE sui propri sistemi ad alto rischio per la conformità a norma dell'articolo 49 del regolamento; (j) su richiesta di un'autorità nazionale competente, dimostrare la conformità del sistema di IA ad alto rischio in ordine ai requisiti di cui al suddetto capo II.

L'art. 19 prevede che i fornitori sono tenuti a sottoporre i loro sistemi ad alto rischio alla procedura di valutazione della conformità di cui al successivo articolo 43, prima della loro immissione sul mercato o della loro messa in servizio. Se la conformità dei sistemi di IA ai requisiti di cui al capo 2 del presente titolo è stata dimostrata in seguito a tale

[37] L'art. 17 prescrive che i fornitori dei sistemi di IA ad alto rischio debbono istituire un sistema di gestione della qualità che garantisca la conformità a quanto prescritto nel regolamento. Tale sistema è documentato in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte e comprende una serie di elementi elencati nel medesimo articolo.

valutazione della conformità, i fornitori redigono una dichiarazione di conformità UE a norma dell'articolo 48 e appongono il marchio CE in virtù dell'articolo 49[38].

L'art. 20 stabilisce invece che i fornitori di sistemi ad alto rischio sono tenuti a conservare i registri generati automaticamente dagli stessi qualora questi siano sotto il loro controllo in base ad un accordo contrattuale con l'utente o perché previsto per legge. I registri sono conservati per un periodo appropriato alla luce dello scopo del sistema e degli obblighi *ex lege* applicabili.

Qualora i fornitori di sistemi di IA ritenessero che un sistema ad alto rischio da essi immesso sul mercato sia difforme a quanto prescritto nel regolamento, sarebbero tenuti – come previsto dall'art. 21 – all'adozione delle più appropriate azioni correttive volte a rendere il sistema conforme, oppure a ritirarlo o richiamarlo, a seconda del caso.

Analogamente a quanto previsto nel GDPR in caso di *Data Breach*, l'art. 22 della proposta di regolamento prevede che, nell'ipotesi in cui il sistema presenti un rischio particolarmente rilevante, ossia si verifichi una delle ipotesi disciplinata dall'articolo 65, par. 1, del regolamento, e tale rischio sia noto al fornitore del sistema, quest'ultimo sia tenuto ad informare immediatamente le autorità nazionali competenti della difformità e delle eventuali azioni correttive intraprese. Tale obbligo grava, come previsto dall'art. 27, par. 4, anche sul distributore.

I fornitori di sistemi ad alto rischio, come previsto dal successivo articolo, su richiesta dell'autorità nazionale competente, sono tenuti a fornire tutte le informazioni e la documentazione necessaria per dimostrare la conformità del sistema ai requisiti di cui al predetto capo II. Tale obbligo grava anche sui distributori. Su richiesta motivata dell'autorità, i fornitori sarebbero inoltre tenuti a concedere l'accesso ai registri generati automaticamente dal sistema di IA ad alto rischio, qualora tali registri fossero sotto il loro controllo.

L'art. 27 - dedicato agli obblighi per i distributori - prevede che, prima di rendere disponibile sul mercato un sistema di IA ad alto rischio, questi verifichino che il sistema rechi il marchio CE di conformità, che sia accompagnato dalla documentazione e dalle istruzioni per l'uso richieste e che il fornitore e l'importatore abbiano ottemperato agli obblighi previsti dal regolamento.

Qualora il distributore ritenga o abbia motivo di ritenere che il sistema non sia conforme ai requisiti del regolamento, non sarà legittimato alla sua immissione sul mercato. Nel caso in cui tale difformità sopravvenga all'immissione sul mercato, il distributore sarà tenuto a realizzare le opportune azioni correttive volte ad ovviare a tale circostanza,

[38] L'art. 49 prevede che il marchio CE deve essere apposto in modo visibile, leggibile e indelebile per i sistemi di IA ad alto rischio. Se ciò non fosse possibile o non è assicurato per la natura del sistema di IA ad alto rischio, verrebbe apposto sull'imballaggio o sulla documentazione di accompagnamento.

oppure ad assicurare che siffatte azioni vengano intraprese dal fornitore, importatore o altro operatore.

Secondo quanto previsto dall'art. 28, qualsiasi distributore, importatore, utente o altra terza parte, al cospetto di specifiche circostanze, viene considerato un fornitore con tutti gli obblighi connessi e sanciti nell'articolo 16. Le circostanze che comportano tale estensione possono riguardare l'ipotesi in cui il soggetto immetta sul mercato un sistema di IA ad alto rischio con il proprio nome o marchio; modifichi lo scopo previsto per un sistema di IA ad alto rischio già immesso sul mercato; oppure apporti una modifica sostanziale al sistema. Nelle ultime due ipotesi, il fornitore originario non viene più considerato tale per le finalità e per l'applicazione del regolamento.

Per quanto riguarda gli obblighi gravanti sugli utenti, l'art. 29 prevede che questi siano tenuti ad utilizzare tali sistemi nel rispetto delle istruzioni d'uso che li accompagnano monitorandone il funzionamento. Questa disposizione, tuttavia, non pregiudica l'applicazione di ulteriori e alternativi obblighi previsti per questi soggetti in forza della normativa vigente e non pregiudicano la discrezionalità dell'utente nell'organizzazione della propria attività in funzione dell'adozione di quelle misure di sorveglianza indicate dal fornitore. L'utente che ha il controllo sui cd. dati di *input* è tenuto a garantire la loro pertinenza rispetto allo scopo previsto per il sistema di cui dispone. Sebbene l'utente sia tenuto ad osservare le istruzioni d'uso del sistema, nel caso in cui accerti che ciò possa comportare un rischio di cui all'art. 65 del regolamento, è tenuto ad informare il fornitore o il distributore, sospendendo allo stesso tempo l'uso del sistema. L'informativa al fornitore o distributore spetta altresì in caso di incidenti gravi o malfunzionamenti. Il paragrafo 5 dell'art. 29 prevede peraltro – nel caso in cui le registrazioni automatiche generate dal sistema fossero nella disponibilità dell'utente – un obbligo di conservazione per un congruo periodo di tempo commisurato allo scopo del sistema.

Il capo IV è dedicato agli organismi predisposti per le verifiche e le convalide dei sistemi IA ad alto rischio. È previsto che ciascuno Stato membro designi o istituisca un'autorità responsabile per le procedure necessarie per la valutazione, designazione e notifica di quegli organismi di valutazione della conformità e monitoraggio.

Spetta a quegli organismi che rispettano i requisiti di cui all'art. 33 verificare la conformità del sistema di IA ad alto rischio secondo le procedure di valutazione della conformità stabilite all'articolo 43. Il capo successivo - dall'art. 40 all'art. 51 - è infatti dedicato alla disciplina degli standard, della valutazione di conformità, della certificazione e della registrazione dei sistemi ad alto rischio.

L'art. 47 stabilisce una eccezione prevedendo che, in deroga all'articolo 43, qualsiasi autorità di vigilanza del mercato possa autorizzare l'immissione sul mercato o la messa in servizio di specifici sistemi di IA ad alto rischio nel territorio dello Stato membro interessato, per motivi eccezionali di pubblica sicurezza o di protezione della vita e salute delle persone, tutela ambientale e tutela dei principali asset industriali e infrastrutturali. Nel frattempo, debbono essere attivate le procedure di verifica e convalida. Quindi,

l'autorizzazione *de qua* ha una efficacia temporale limitata, cessando una volta che le procedure in questione vengano completate. L'art. 48 prevede che il fornitore è tenuto a stilare una dichiarazione di conformità UE per ciascun sistema di IA conservandola per 10 anni dopo che il sistema di IA è stato immesso sul mercato o messo in servizio. Tale dichiarazione – che deve contenere le informazioni previste nell'allegato 5 del regolamento - è volta ad identificare il sistema per cui è stata redatta e ad attestare che il sistema possieda i requisiti di cui al capo II del titolo III del regolamento.

3.2.3 Il rischio limitato

Il titolo IV del regolamento, composto dal solo art. 52, prevede obblighi di trasparenza per alcuni sistemi IA non ad alto rischio, dunque con un livello di rischio limitato.

I fornitori, in questo caso, sono tenuti a garantire che i sistemi di intelligenza artificiale destinati a interagire con persone fisiche vengano progettati e sviluppati in modo tale da informarle del fatto che stanno interagendo con un sistema di intelligenza artificiale, ad eccezione dell'ipotesi ove ciò risulti palese dalle circostanze e dal contesto d'uso. L'obbligo in questione non trova applicazione ai sistemi di IA autorizzati per legge a rilevare, prevenire, indagare e perseguire reati.

Gli utenti di un sistema di intelligenza artificiale di c.d. *deep fake* sono tenuti ad informare che il contenuto è stato generato o manipolato artificialmente. Ciò, tuttavia, non trova applicazione 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.

3.2.4 Disposizioni finali

Il titolo VIII della proposta è riservato al tema del monitoraggio dei sistemi nel periodo successivo alla sua immissione sul mercato, alla condivisione delle informazioni e alla vigilanza di mercato. All'art. 61 è previsto che i fornitori debbono istituire un sistema di monitoraggio del sistema in modo proporzionato alla natura della tecnologia IA ed ai rischi specifici di un sistema IA ad alto rischio. Il capo II è dedicato alla disciplina della condivisione di informazioni su incidenti e malfunzionamenti dei sistemi. In particolare, all'art. 64 è previsto il potere di accesso ai dati del sistema da parte delle Autorità preposte in alcune circostanze particolari.

L'art. 67 prevede il potere, in capo alle autorità nazionali di vigilanza, di disporre l'adozione delle misure più opportune nel caso in cui un sistema di IA che, ancorché conforme ai requisiti previsti dal regolamento, manifesti comunque un rischio per la salute o la sicurezza delle persone. Tra le misure rientrano anche quelle riguardanti il ritiro del prodotto dal mercato o il suo richiamo entro un termine ragionevole e commisurato alla natura del rischio.

Il titolo successivo è dedicato ai codici di condotta. L'art. 69, in particolare, incentiva l'elaborazione di codici di condotta tesi a favorire l'applicazione volontaria, per i sistemi di IA non ad alto rischio, dei requisiti di cui al titolo III, capo II, sulla base di misure appropriate per lo scopo previsto per i sistemi in questione. Il titolo X, infine, è dedicato alla riservatezza ed alle sanzioni applicabili in caso di violazioni del regolamento.

4. Riflessioni conclusive

Il settore dell'innovazione racchiude numerose sfide da affrontare. La sfida più complessa risiede nell'abilità di adattare le differenti soluzioni di diritto alle differenti realtà tecnologiche. Un approccio con un orizzonte esteso ad una seria cooperazione internazionale e ad una prospettiva interdisciplinare costituisce un intangibile auspicio[39].

L'intervento legislativo, o meglio la sua necessità, è stato sottoposto a sollecitazioni non solo da fonti istituzionali, bensì anche dalla letteratura[40].

Uno degli obiettivi riguardanti il tema in commento consiste nella necessità di prevedere ed accompagnare il progresso scientifico e tecnologico nella sua evoluzione, o meglio, rivoluzione. Tra gli equilibri da rintracciare non si può trascurare quello inerente al bilanciamento tra la previsione di strumenti legislativi di *hard law* e strumenti di *soft law*. Una capillare normativa in tema di nuove tecnologie, da un lato potrebbe ostacolare un regolare processo di perfezionamento tecnologico se eccessivamente complessa, dall'altro potrebbe guidarlo verso orizzonti più chiari, rapidi ed efficienti[41]. La soluzione proposta dalla Commissione europea, meritoria nell'intento di regolamentare orizzontalmente un settore dalle più variegate declinazioni, presenta in parte caratteri di rigore potenzialmente capaci di dissuadere lo sviluppo e l'investimento di alcuni sistemi IA nel continente europeo a favore di altri Stati, dall'altro presenta un articolato sistema a protezione dei diritti dei singoli e di gruppi sociali.

Nell'impianto normativo generale, sebbene vi siano elementi da far supporre un approccio analogo a quello della *accountability*, tipico della disciplina europea sul trattamento dei dati personali, l'impostazione utilizzata non fornisce una identica flessibilità al soggetto responsabile. A titolo esemplificativo, l'art. 11 del regolamento

[39] M. GONZÁLEZ-FIERRO, *10 ethical issues of artificial intelligence and Robotics*, april 1, 2018, reperibile su:
https://miguelgfierro.com/blog/2018/10-ethical-issues-of-artificial-intelligence-and-robotics/
L'A rileva che il compito gravante su politici, professionisti e ricercatori consiste nel lavorare insieme per far sì che intelligenza artificiale e la robotica forniscano un beneficio all'umanità.

[40] Si veda NEMITZ, P. Friedrich, *Constitutional Democracy and Technology in the age of Artificial Intelligence* (August 18, 2018). DOI 10.1098/RSTA.2018.0089 - Royal Society Philosophical Transactions A, Available at SSRN: https://ssrn.com/abstract=3234336 or http://dx.doi.org/10.2139/ssrn.3234336; Sul tema si veda anche G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in Politica del diritto, 2/2019, Il mulino, p. 199.

[41] Sul tema si veda anche quanto già esposto dallo scrivente in *La responsabilità nell'intelligenza artificiale e nella robotica. Attuali e futuri scenari nella politica del diritto e nella responsabilità contrattuale*, Milano, 2020, p. 220 ss.

prevede la redazione della documentazione tecnica che precede l'immissione del sistema sul mercato al fine di provare che il sistema ad alto rischio sia conforme ai requisiti prescritti dal Regolamento. Nel fornire tutte le informazioni necessarie per valutare la conformità del sistema, vi dev'essere un contenuto che contempli tutti i numerosi e rigidi elementi stabiliti nell'allegato IV del regolamento. Inoltre, come si è visto, nell'art. 13 vengono imposti altri rigidi requisiti facenti capo al c.d. *provider*, tra cui quello di specificare, tra gli obblighi di informativa, le circostanze relative ad un eventuale abuso del sistema IA, nonché ai rischi derivabili alla salute e ai diritti umani. L'opacità e l'autonomia che in alcuni casi caratterizza tali sistemi, sfociando finanche nell'imprevedibilità, potrebbe tuttavia rendere addirittura impossibile l'assolvimento di tali incombenze.

Invece, in un'ottica comparatistica, l'impostazione della proposta di regolamento ricalca in buona parte quella delineata nel Libro bianco sull'IA del febbraio 2020, benché quest'ultimo - accompagnato dalla relazione dedicata alle implicazioni dell'intelligenza artificiale, dell'IoT e della robotica in tema di sicurezza e responsabilità[42] - affrontava anche ulteriori profili che esulano dalla proposta in commento.

Il Libro bianco condivide un approccio fondato sul rischio suddividendo le applicazioni IA in due categorie, ad alto rischio e non ad alto rischio. Le prime, classificabili sulla base di due presupposti, ovvero il settore o contesto in cui verrebbero applicate le tecnologie – il quale presenterebbe peculiarità e rischi significativi – ed il loro uso previsto e prevedibile. L'approccio che veniva invece avanzato dal Parlamento europeo con la risoluzione del 2017 sembrava invece fondato su un discernimento piuttosto tecnico tra uno strumento e l'altro, ovvero a seconda delle caratteristiche del sistema, anziché sulla base del contesto in cui è chiamato ad operare[43]. Una terza strada, astrattamente percorribile, potrebbe essere quella che consideri sia le caratteristiche tecniche, sia l'ambito settoriale di applicazione del sistema.

Riguardo la previsione di obblighi in capo ai vari operatori della catena, il Libro bianco suggerisce una loro ripartizione tra i vari attori economici che si trovano nella migliore posizione per affrontare meglio il rischio derivante dal sistema. Anche questo approccio sembra ripreso nella proposta legislativa.

Nel Libro bianco vengono poi sintetizzate le principali sfide derivanti dalla diffusione delle nuove tecnologie quali l'opacità (da cui deriverebbe il fenomeno della *black box*[44]),

[42] Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità, reperibile su:
https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en

[43] Nella risoluzione del 2017 si proponeva l'istituzione di un registro contenente l'elenco aggiornato dei robot più avanzati.

[44] PASQUALE, *The Black Box Society. The secret Algorithms That Control Money and Information*, Cambridge-London, 2015; CERQUITELLI, QUERCIA, PASQUALE, *Trasparent Data Mining for Big and Small*

l'autonomia e la connettività tra sistemi. Alcuni di tali rischi vengono succintamente ripresi nella proposta per motivare le misure previste. L'opacità, ad esempio, è ripresa nel considerando n. 47 per giustificare la necessità di un certo grado di trasparenza per i sistemi ad alto rischio in modo da consentire agli utenti di interpretare i risultati del sistema utilizzandolo quindi in modo appropriato; nonché per motivare la previsione della documentazione e delle istruzioni che debbono accompagnare il sistema.

Un altro controverso obiettivo rintracciabile nella proposta di regolamento riguarda l'ambito definitorio; in particolare, il tentativo di fornire una nozione di intelligenza artificiale. Ebbene, la delicatezza e la difficoltà di giungere ad un tale risultato è nota, per questo il legislatore europeo non fornisce una definizione *tout court* e astratta come si è tentato in precedenza, ma effettua sostanzialmente un rinvio ad un allegato del regolamento, il quale a sua volta contiene un elenco di differenti approcci e tecniche in cui si può caratterizzare l'IA.

In precedenza, il tentativo di fornire una ampia definizione è stato effettuato dal gruppo di esperti ad alto livello nel documento "una definizione di IA: principali capacità e discipline"[45].

Un altro tentativo di definizione è stato effettuato anche nella Comunicazione della Commissione del 2018 "L'intelligenza artificiale per l'Europa" laddove si legge che il termine IA «*indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose) (…)*»[46].

Data, New York, 2017; Y. BATHAEE, *The Artificial Intelligence Black Box and The Failure of Intent and Causation*, vol. 31, n. 2/2018, Harvard Journal of Law & Technology, p. 890 s.

[45] Il gruppo di lavoro in questo documento, p. 6, propone la seguente definizione:
«*I sistemi di intelligenza artificiale (IA) sono sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulle conoscenze, o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti. Come disciplina scientifica, l'IA include diversi approcci e diverse tecniche, come l'apprendimento automatico (di cui l'apprendimento profondo e l'apprendimento per rinforzo sono esempi specifici), il ragionamento meccanico (che include la pianificazione, la programmazione, la rappresentazione delle conoscenze e il ragionamento, la ricerca e l'ottimizzazione), e la robotica (che include il controllo, la percezione, i sensori e gli attuatori e l'integrazione di tutte le altre tecniche nei sistemi ciberfisici)*».

[46] La definizione viene ripresa anche dalla citata Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza

La difficoltà di elaborare una definizione di intelligenza artificiale, come rilevato in dottrina, risiede anche in una inevitabile antropomorfizzazione del tema per l'utilizzo del termine "intelligenza" o "intelligente"[47]. I tentativi di includere una definizione di questa multiforme tecnologia sono stati numerosi[48] e saranno indubbiamente oggetto di evoluzioni e dibattiti.

La trasversalità degli ambiti in cui i sistemi IA troverebbero applicazione, l'incertezza tecnica sul loro sviluppo e sulla loro incidenza farebbero salutare con favore quei principi europei che consentono la protezione dei diritti senza vincolare eccessivamente il mercato. Il principio di precauzione[49] costituirebbe uno di questi e l'art. 67 della proposta

artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)) laddove alla lett. a) dell'art. 4 viene proposta una definizione di intelligenza artificiale come «*un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento intelligente, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi*.». La stessa definizione viene proposta nella citata risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale alla lett. a) dell'art. 3, in cui viene fornita una definizione di "sistema di intelligenza artificiale (IA)". In quest'ultima risoluzione, al punto n. 23 viene evidenziata la necessità di «*adeguare e semplificare le definizioni di sistema di IA, operatore di front-end e di back-end, produttore, difetto, prodotto e servizio in tutti gli atti legislativi, e tale adeguamento dovrebbe avvenire in parallelo*.»

[47] G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, in Contratto e impresa, 2/2020, p. 724-726. L'A. sottolinea come utilizzando il termine di intelligenza artificiale si sottintende l'esistenza di una entità che è espressione di intelligenza. Tuttavia, l'intelligenza «*si attribuisce all'essere umano o agli animali. Dunque già utilizzare questo termine induce sviluppare la narrazione in termini antropomorfici*.» Sarebbe invece differente confrontare i risultati di un processo. «*se il processo è qualificato intelligente quando è svolto da un essere umano, allora lo si può qualificare intelligente se è svolto da una macchina. Quindi l'intelligenza artificiale può essere definita la scienza di far fare ai computer cose che richiedono intelligenza quando vengono fatte dagli esseri umani*.»; Sul tema si veda anche M. MONTAGNANI, *Intelligenza artificiale e governance della "nuova" grande impresa azionaria: potenzialità e questioni endoconsiliari*, Rivista delle Società, 4/2020, p.7; A. SANTUOSSO, in *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano, 2020, p. XI, rileva come «(…) *quello che viene appellato IA non è altro che lo sviluppo ampio, potente, talora sofisticato di capacità computazionali settoriali. Niente che abbia a che fare con le entità alle quali normalmente connettiamo l'attributo di intelligenza nella nostra vita di tutti i giorni* (…).» Lo stesso autore, p. 6, rileva che il campo dell'intelligenza artificiale presenta molte definizioni, ma manca un significato universalmente accettato.

[48] S.J. RUSSELL, P. NORVIG, *Artificial Intelligence: A Modern Approach*, Pearson, 2010, p. 4; V. RAJARAMAN, *John McCarthy – Father of Artificial Intelligence*, Resonance (Mar. 2014), p. 200. https://www.ias.ac.in/article/fulltext/reso/019/03/0198-0207; R. CALO, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C.D. L. REV. 399, 405 (2017); si veda altresì G. SARTOR e F. LAGIOIA, *Le decisioni algoritmiche tra etica e diritto*, in *Intelligenza artificiale - il diritto, i diritti, l'etica*, U. RUFFOLO (a cura di), Milano, 2020, pp. 63 ss.

[49] Secondo il Consiglio di Stato, Sez. IV, 27 marzo 2017, n. 1392, tale principio «*impone che quando sussistono incertezze riguardo all'esistenza o alla portata di rischi per la salute delle persone, possono essere adottate misure di protezione senza dover attendere che siano pienamente dimostrate l'effettiva esistenza e la gravità di tali rischi*». *Secondo lo stesso Organo giurisdizionale, Cons. Stato, Sez. III, 03 ottobre 2019, n. 6655, l'attuazione di tale principio «comporta che, ogni qual volta non siano conosciuti con certezza i rischi indotti da un'attività potenzialmente pericolosa, l'azione dei pubblici poteri debba tradursi in una prevenzione anticipata rispetto al consolidamento delle conoscenze scientifiche*».

di regolamento enuncia un principio strutturalmente analogo, ancorché mancante di un riferimento esplicito ad una situazione di incertezza scientifica[50]. Infatti, la disposizione conferisce alle autorità nazionali di vigilanza il potere di adottare le opportune misure qualora un sistema IA, benché conforme ai requisiti prescritti dal regolamento - e a seguito di una valutazione di rischio prevista nell'art. 65 - presenti un pericolo per la salute o la sicurezza delle persone; quindi, la situazione prospettata sembrerebbe relativa ad un pericolo esistente piuttosto che una incertezza. A tal proposito può essere operato un raffronto con il principio di precauzione stabilito in materia alimentare laddove all'art. 7 del Reg. (CE) n. 178/2002 del Parlamento Europeo e del Consiglio- rubricato espressamente "principio di precauzione" - è previsto che qualora "*in circostanze specifiche a seguito di una valutazione delle informazioni disponibili, venga individuata la possibilità di effetti dannosi per la salute ma permanga una situazione d'incertezza sul piano scientifico, possono essere adottate le misure provvisorie di gestione del rischio necessarie per garantire il livello elevato di tutela della salute che la Comunità persegue, in attesa di ulteriori informazioni scientifiche per una valutazione più esauriente del rischio.*"[51]

Il principio di derivazione europea, inizialmente circoscritto ad ambiti particolari come l'ambiente ed il settore alimentare, è stato esteso nella sua portata - dalla comunicazione del 2 febbraio del 2000 della Commissione europea - ad una generalità di campi sociali in cui emergono esigenze protezionistiche dovute ad incertezze di carattere scientifico che possano produrre rischi di varia natura[52].

Un principio di questo genere, qualora articolato e distribuito a sufficienza tra i vari poteri pubblici e qualora attuato in modo appropriato - ovvero sulla base di decisioni fondate su un'analisi dei potenziali vantaggi e oneri dell'azione o dell'inazione, tra cui l'analisi costi/benefici - sarebbe in grado di contribuire a rintracciare un maggiore ed efficace

[50] Sul principio di precauzione si veda FISHER, *Precaution, Precaution Everywhere: Developing a 'Common Understanding' of the Precautionary Principle in the European Community*, Maastricht Journal of European and Comparative Law, 2002, 9(1), 7-28; SADELEER (de), N., *The Precautionary Principle in EU Law*, AV&S, 5(October), 2010, 173-184, 184; LÖFSTEDT, R., *The Swing of the Regulatory Pendulum in Europe: From Precautionary Principle to (Regulatory) Impact Analysis*, The Journal of Risk and Uncertainty, 2004, 28(3), 237-260.

[51] Il par. 2 prosegue prevedendo che «*Le misure adottate sulla base del paragrafo 1 sono proporzionate e prevedono le sole restrizioni al commercio che siano necessarie per raggiungere il livello elevato di tutela della salute perseguito nella Comunità, tenendo conto della realizzabilità tecnica ed economica e di altri aspetti, se pertinenti. Tali misure sono riesaminate entro un periodo di tempo ragionevole a seconda della natura del rischio per la vita o per la salute individuato e del tipo di informazioni scientifiche necessarie per risolvere la situazione di incertezza scientifica e per realizzare una valutazione del rischio più esauriente.*»

[52] Nella Comunicazione della Commissione sul principio di precauzione si legge che «*il ricorso al principio di precauzione presuppone l'identificazione di effetti potenzialmente negativi derivanti da un fenomeno, da un prodotto o da un procedimento; una valutazione scientifica del rischio che, per l'insufficienza dei dati, il loro carattere non concludente o la loro imprecisione, non consente di determinare con sufficiente certezza il rischio in questione*.» Comunicazione reperibile su:
https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A52000DC0001

equilibrio tra i diritti dell'individuo (e di gruppi di individui) e gli interessi di mercato, consentendo finanche una maggiore flessibilità tra gli articolati requisiti richiesti per l'immissione sul mercato di sistemi IA[53].

Per quanto riguarda ulteriori profili, come si è visto, la proposta legislativa non mira ad una regolamentazione specifica e diretta del regime di responsabilità per i sistemi IA, rinviandolo ad un successivo intervento. Tuttavia, il paradigma elaborato dalla Commissione europea, composto da un capo del titolo III dedicato agli obblighi in capo ai vari operatori, fornirebbe indirettamente un quadro indicativo anche per il profilo della responsabilità. Quantunque il regime della responsabilità e le regole sulla imputabilità siano quelli della normativa ordinaria vigente, va da sé che la violazione degli obblighi imposti dal regolamento comporterebbero una fattispecie di responsabilità. Nel considerando n. 58 della proposta viene specificato che in virtù della natura dei sistemi IA e dei rischi per la sicurezza e i diritti fondamentali associati al loro utilizzo, è opportuno stabilire specifiche responsabilità per gli utenti, chiamati ad utilizzare sistemi ad alto rischio conformemente alle istruzioni d'uso e dovrebbero essere previsti altri obblighi per quanto riguarda il monitoraggio del funzionamento dei sistemi di IA nonché per ciò che riguarda la tenuta dei registri, a seconda delle ipotesi.

In relazione agli obblighi imposti nella proposta di regolamento, viene segnalato a più riprese come questi siano previsti – al pari dell'intera architettura normativa - a protezione di alcuni interessi fondamentali, specificando che vengono stabiliti «*obblighi prevedibili, proporzionati e chiari ai fornitori e agli utenti di tali sistemi per garantire la sicurezza e il rispetto della legislazione esistente che protegge i diritti fondamentali durante l'intero ciclo di vita dei sistemi di IA*.»[54].

Il paradigma normativo proposto, dunque, per le sue peculiarità, pone indirettamente una questione riguardante il tema dell'imputabilità di una responsabilità per la violazione di uno degli obblighi che si traducono in una regola di condotta, ovvero la possibilità o meno di generare una fattispecie di responsabilità da contatto sociale qualificato. Siffatta fattispecie di responsabilità si configurerebbe allorché l'ordinamento imponga ad un soggetto un'obbligazione, in ragione dell'attività o funzione esercitata, affinché osservi specifici comportamenti in determinate situazioni, generando quindi obblighi di protezione «*nei confronti di tutti coloro che siano titolari degli interessi la cui tutela costituisce la ragione della prescrizione di quelle specifiche condotte*.»[55].

---

[53] La stessa Commissione europea, tra l'altro, nella citata comunicazione del 2000, sostiene che il principio di precauzione viene spesso utilizzato per «*equilibrare le libertà e i diritti degli individui, delle industrie e delle organizzazioni con l'esigenza di ridurre o eliminare il rischio di effetti negativi per l'ambiente o per la salute*».

[54] Proposta di regolamento, p. 3.

[55] In questo senso, Cass. civ., Sez. I, Sent., 11/07/2012, n. 11642. La Cassazione prosegue che: «*Dire che, in tali situazioni, la responsabilità deriva dal mero "contatto" serve ad evidenziare la peculiarità della fattispecie distinguendola dai casi nei quali la responsabilità contrattuale deriva propriamente da contratto (cioè dall'assunzione volontaria di obblighi di prestazione nei confronti di determinati soggetti), ma non*

Una imputabilità di questo tipo costituirebbe ovviamente un elemento di favore aggiuntivo per il soggetto che subisce un danno ed un onere ulteriore a carico dell'operatore su cui graverebbe l'obbligo di protezione, inserendosi così nel perimetro costruito dal regolamento proposto dalla Commissione europea, fondato essenzialmente su un approccio prudente e antropocentrico.

deve far dimenticare che essenziale per la configurabilità della responsabilità in esame è la violazione di obblighi preesistenti di comportamento posti a carico di un soggetto dalla legge per la tutela di specifici interessi di coloro che entrano in contatto con l'attività di quel soggetto, che la legge stessa regola, tanto più ove il fondamento normativo della responsabilità in esame si individui - come da taluni si ritiene - nel riferimento, contenuto nell'art. 1173 cod. civ., agli altri atti o fatti idonei a produrre obbligazioni in conformità dell'ordinamento giuridico.»; nello stesso senso, Cass. civ. Sez. II Ord., 29/12/2020, n. 29711, secondo cui: «*La cosiddetta responsabilità "da contatto sociale", soggetta alle regole della responsabilità contrattuale, pur in assenza d'un vincolo negoziale tra danneggiante e danneggiato, è configurabile non in ogni ipotesi in cui taluno, nell'eseguire un incarico conferitogli da altri, nuoccia a terzi, come conseguenza riflessa dell'attività così espletata, ma soltanto quando il danno sia derivato dalla violazione di una precisa regola di condotta, imposta dalla legge allo specifico fine di tutelare i terzi potenzialmente esposti ai rischi dell'attività svolta dal danneggiante, tanto più ove il fondamento normativo della responsabilità si individui nel riferimento dell'art. 1173 c.c. agli altri atti o fatti idonei a produrre obbligazioni in conformità dell'ordinamento giuridico.*»; conf. la giurisprudenza di merito, Trib. Roma, sez. II, Sent. 12/08/2019.