I *Post* di AISDUE, IV (2022), *aisdue.eu*
Sezione "Atti convegni AISDUE", n. 16, 28 marzo 2022
Quaderni AISDUE, ISSN 2723-9969

Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione

Cristina Schepisi*

SOMMARIO: 1. Introduzione. – 2. La dimensione europea e il bilanciamento *ex ante* delle esigenze del mercato con la tutela dei diritti. - 3. Il bilanciamento tra i diritti. – 4. La dimensione oggettiva e soggettiva del rischio – 5. La dimensione individuale e collettiva. – 6. La dimensione pubblica in rapporto a quella privata. – 7. Profili conclusivi: la dimensione europea ed internazionale.

1. La regolazione dell'intelligenza artificiale è un tema che occupa il dibattito europeo da alcuni anni. I sistemi che usano tale tecnologia consentono innegabili benefici, sia economici che sociali ma dall'altro possono, come noto, comportare rischi, anche molto elevati, di lesione dei diritti fondamentali, della *rule of law* e dei principi democratici. L'opacità, la complessità, la dipendenza dai dati, il comportamento autonomo sono tutte caratteristiche dei sistemi di IA che possono

* Professore ordinario di Diritto dell'Unione europea, Università di Napoli Parthenope.

incidere negativamente su una serie di diritti protetti dalla Carta europea[1].

Come regolare l'intelligenza artificiale senza imbrigliare l'innovazione e garantendo al contempo un'elevata tutela dei diritti fondamentali? Tale domanda non ha una risposta unitaria a livello globale sia perché la stessa definizione di 'sistema di intelligenza artificiale' non è univoca[2], sia perché dipende dalla tensione tra i diversi valori che ogni ordinamento ha al proprio interno e dunque da un differente bilanciamento tra le esigenze del mercato e dello sviluppo tecnologico, da un lato, e la tutela dei diritti, dall'altro.

A seconda dei contesti e degli ordinamenti le opzioni in campo sono dunque svariate. Esse vanno dalla *self regulation*, giudicata in alcuni ambiti, nazionali ed internazionali, inadeguata nel caso di applicazioni particolarmente rischiose per i diritti fondamentali, alla *soft regulation* – basata su raccomandazioni e indicazione di *best practices* – fino ad arrivare a proposte di *hard regulation*.

[1] V. punto 3.5, della relazione alla proposta di regolazione dell'IA p. 13; la comunicazione della Commissione "Creare fiducia nell'intelligenza artificiale antropocentrica" (COM(2019) 168 final); la risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate 2020/2012(INL). La Commissione ha istituito infatti un Gruppo di esperti ad alto livello sull'intelligenza artificiale, che ha adottato degli Orientamenti etici per un'IA affidabile, 8 aprile 2019 suggerendo il rispetto di sette requisiti fondamentali: intervento e sorveglianza umani, robustezza tecnica e sicurezza, riservatezza e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale, e *accountability*.

[2] Secondo la definizione contenuta nell'art.1 della proposta "sistema di intelligenza artificiale" (sistema di IA): un software sviluppato con una o più delle tecniche e 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".

Quest'ultima è la strada scelta dall'Unione europea[3]. La Commissione ha infatti proposto, il 21 aprile 2021[4], l'adozione di un regolamento sulla base giuridica dell'art. 114 TFUE, con l'obiettivo di introdurre, in capo a coloro i quali producono, mettono in servizio o usano sistemi di intelligenza artificiale, divieti, obblighi ed adempimenti procedurali, calibrati sul diverso livello rischio di lesione che tali sistemi sono suscettibili di produrre per i diritti fondamentali.

Sulla base di tale proposta[5] sono vietati i sistemi che comportano un rischio inaccettabile e dunque i sistemi che usano tecniche subliminali e manipolatorie, che attribuisco un punteggio sociale nella misura in cui siano utilizzati dalle pubbliche autorità, i sistemi di riconoscimento biometrico in *real time*, con eccezioni di taluni casi particolari[6].

I sistemi ad alto rischio sono invece definiti dall'art. 6 (prodotti o componenti di sicurezza di prodotti) e includono tutti i sistemi indicati nell'Allegato III: la gestione e funzionamento delle infrastrutture

[3] Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, 19 febbraio 2020, COM(2020) 65 final. Si veda anche il Report *Getting the future right – Artificial intelligence and Fundamental rights* – FRA- European Union Agency for Fundamental Rights (dicembre 2020), secondo la quale: "A wider range of rights need to be considered when using AI, depending on the technology and area of use. In addition to rights concerning privacy and data protection, equality and non-discrimination, and access to justice, other rights could be considered. These include, for example, human dignity, the right to social security and social assistance, the right to good administration (mostly relevant for the public sector) and consumer protection (particularly important for businesses). Depending on the context of the AI use, any other right protected in the Charter needs consideration" (p. 7); nonché la relazione del PE sull'intelligenza artificiale nell'istruzione, nella cultura e nel settore audiovisivo 2020/2017 (INI) A9-0127/2021; e le Conclusioni della presidenza del Consiglio dell'Unione *The Chartes of Fundamental rights in the context of Artificial Intelligence and Digital Change* – 21 ottobre 2020 1148/20.

[4] Proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021)206 def., 21 aprile 2021.

[5] Art. 5.

[6] Le eccezioni sono le seguenti: i) la ricerca mirata di potenziali vittime specifiche di reato, compresi iminori scomparsi; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; iii) 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.

critiche, l'istruzione e formazione professionale, l'occupazione, gestione dei lavoratori e accesso al lavoro autonomo; l'accesso a prestazioni e servizi pubblici e a servizi privati essenziali; i servizi di emergenza di primo soccorso compresi vigili del fuoco, le applicazioni utilizzate per le attività di contrasto, la gestione della migrazione, dell'asilo e del controllo delle frontiere, l'amministrazione della giustizia e processi democratici[7].

Per tali sistemi, il Capo 2 del regolamento impone una numerosa serie di requisiti (accuratezza, robustezza e cibersicurezza[8]; gestione di rischi; *governance* dei dati; trasparenza e informazioni; conservazione delle registrazioni; ecc.[9]), obblighi in capo ai fornitori distributori e utilizzatori (gestione della qualità, certificazioni, trasparenza)[10] e controllo da parte delle autorità nazionali[11]. L'art. 14 richiede inoltre che sia comunque sempre assicurato il controllo umano e che un sistema ad alto rischio possa essere vietato qualora comporti, all'esito di una verifica, rischi non prevedibili o non controllabili.

Sono invece soggetti solo ad un obbligo di trasparenza e informazione i sistemi di IA destinati a interagire con le persone fisiche come ad esempio i sistemi per il riconoscimento delle emozioni di una persona o categorizzazione biometrica e i sistemi che generano o manipolano immagini o contenuti audio o video e che potrebbero apparire falsamente autentici o veritieri per una persona ("deep fake")[12].

Il presente contributo non intende esaminare nel dettaglio il contenuto della proposta, che è ancora in discussione[13], né ripercorre

[7] Sulla regolazione dell'IA nell'ambito della pubblica amministrazione si rinvia a E. CHITI, B. MARCHETTI, N. RANGONE, *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni: prove generali*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *La rivoluzione dell'intelligenza artificiale: profili giuridici*, Bologna, 2022.
[8] Art. 15.
[9] Artt. da 9 a 16.
[10] Artt. da 16 a 29.
[11] Art. 59 ss. V. la struttura di Governance, art. 56 ss.
[12] Art. 52.
[13] Per alcuni commenti, *ex multis*, A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europea tra mercato unico digitale e tutela dei diritti fondamentali*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, 13 ss.; IDEM, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: brevi considerazioni sulla*

l'iter della sua adozione. L'obiettivo è invece quello di svolgere alcune brevi riflessioni sulle varie 'dimensioni' che caratterizzano la regolazione dell'IA con particolare riferimento alla proposta della Commissione europea. Tali diverse dimensioni spiegano le ragioni dell'opzione regolatoria adottata e delle soluzioni prospettate. Nel rispecchiare le nuove sfide che l'Unione si è posta sia nello sviluppo del mercato che nell'ambito della tutela dei diritti fondamentali, esse evidenziano la complessità dell'approccio adottato e aprono nuovi scenari specie in riferimento al ruolo dei singoli attori (operatori privati, pubbliche autorità, legislatori) e alle modalità della tutela dei diritti fondamentali e del loro reciproco bilanciamento.

2. Una prima dimensione è proprio quella europea. Regolare l'intelligenza artificiale a livello di Unione evita innanzitutto la frammentazione del mercato interno e pertanto giustifica, agli occhi della Commissione, la scelta dell'art. 114 TFUE come base giuridica per l'adozione del futuro atto normativo[14]. Se ciascuno Stato – anche in nome di esigenze più che legittime di tutela dei diritti – ponesse unilateralmente limiti e divieti all'uso di sistemi di intelligenza artificiale, ne deriverebbero evidenti restrizioni alla libera circolazione dei servizi e dei prodotti.

Si tenga inoltre in considerazione – come già accennato – la difficoltà di adottare una nozione unitaria di intelligenza artificiale, concetto questo che racchiude una molteplicità di tipologie e distinte

(difficile) costruzione di un quadro normativo dell'Unione, in A. PAJNO, F. DONATI, A. PERRUCCI, *op. cit.*; G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale e la protezione di dati personali,* in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2022, p. 205 ss.; C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 2021, p. 415 ss.; M. EBERS, S*tandardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in L. A. DI MATTEO, N. CANNARSA, C. PONCIBO (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge, 2021; O. POLLICINO, G. DE GREGORIO, F. PAOLUCCI, *La proposta di Regolamento sull'intelligenza artificiale: Verso una nuova governance europea*, in *Agenda Digitale*, *L'intelligenza artificiale made in Ue è davvero "umano-centrica"? I conflitti della proposta*.

[14] Per alcune riflessioni sulla correttezza della base giuridica prescelta, cfr. A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione*, cit.

applicazioni e che potrebbe dunque essere soggetto ad interpretazioni divergenti. E infatti anche la nozione indicata dalla proposta di regolamento è frutto di un lungo *iter* di modifiche e rimaneggiamenti[15] al fine di essere il più esaustiva possibile[16]: un sistema di IA dovrebbe consistere in un software sviluppato con una o più tecniche specifiche[17], in grado di generare contenuti, previsioni, decisioni e può essere sia un prodotto che una componente di sicurezza di un prodotto[18].

Al fine di evitare che i requisiti e le modalità di applicazione e controllo possano divergere tra i vari Stati membri, la Commissione propone un approccio unitario, diretto a regolare in maniera uniforme le differenti applicazioni di intelligenza artificiale a seconda del rischio, da basso a inaccettabile, che esse producono per i diritti fondamentali.

La scelta di procedere con una regolazione orizzontale ha dunque prevalso su quella di disciplinare verticalmente i diversi settori (o solo alcuni di essi, es. lavoro, sanità, istruzione, giurisdizione) nei quali i sistemi di intelligenza artificiale possono generare maggiore preoccupazione, o direttamente e singolarmente i diversi sistemi (prodotti, *machine learning*, *deep fake*, ecc.), approccio quest'ultimo che sarebbe risultato assai limitativo viste le molteplici applicazioni che un sistema di IA può avere nei vari settori e il diverso impatto che può produrre.

---

[15] V. il punto 7 della relazione illustrativa secondo cui "La nozione di sistema di IA dovrebbe essere definita in maniera chiara al fine di garantire la certezza del diritto, prevedendo nel contempo la flessibilità necessaria per agevolare i futuri sviluppi tecnologici".

[16] La definizione è stata ritenuta da alcuni fin troppo ampia e suscettibile di questioni interpretative. Cfr. *Joint letter on the European Commission's Proposal for an AI Act.*

[17] Secondo l'Allegato I "Tecniche e approcci di intelligenza artificiale di cui all'articolo 3, punto 1), tali tecniche consistono negli: 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".

[18] Secondo la definizione contenuta nell'art. 1 della proposta il "sistema di intelligenza artificiale" è "un software sviluppato con una o più delle tecniche e 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".

La proposta di regolazione dell'IA si struttura infatti in maniera trasversale, coinvolgendo a livello orizzontale qualunque settore, uso, operatore e sue dimensioni. I livelli di rischio, e i connessi divieti e obblighi procedurali, non sono infatti parametrati alle dimensioni del fornitore e/o della piattaforma digitale bensì alla tipologia di applicazione e/o all'uso a cui è destinata o, ancora al settore nell'ambito del quale viene utilizzata. L'opzione di adottare un regolamento, piuttosto che una direttiva, ricalca inoltre quella già effettuata con GDPR[19] nonché con le più recenti proposte del *Digital Markets Act*[20] e del *Digital Servces Act*[21].

La dimensione europea della regolazione dell'IA va tuttavia ben oltre ad una evidente esigenza di non frammentare il mercato, non esaurendosi affatto in essa.

Secondo quanto si legge nella relazione di accompagnamento della proposta l'obiettivo è innanzitutto quanto meno duplice e rimarca quanto già indicato anche nel Libro bianco[22]. L'interesse dell'Unione europea è da un lato quello di "preservare la leadership tecnologica dell'UE e assicurare che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione"[23]. Dall'altro è di basarsi "sui

[19] 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 (GDPR).

[20] Proposta di regolamento del Parlamento europeo e del Consiglio, del 15 dicembre 2020, relativo a mercati equi e contendibili nel settore digitale (DMA), COM(2020) 842 final.

[21] COM(2020) 845 final, 15.12.2020, Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (DSA) e che modifica la direttiva 2000/31/CE; Cfr. Da ultimo, G. CAGGIANO, G. CONTALDI, P. MANZINI, op. cit.

[22] Libro bianco sull'intelligenza artificiale, cit.

[23] La presente proposta risponde altresì alle richieste esplicite del Parlamento europeo e del Consiglio europeo, che hanno ripetutamente chiesto un intervento legislativo che assicuri il buon funzionamento del mercato interno per i sistemi di intelligenza artificiale ("sistemi di IA"), nel contesto del quale tanto i benefici quanto i rischi legati all'intelligenza artificiale siano adeguatamente affrontati a livello dell'Unione. Essa contribuisce all'obiettivo dell'Unione di essere un leader mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica, come dichiarato dal Consiglio europeo, e garantisce la tutela dei principi etici, come richiesto specificamente dal Parlamento europeo.

valori e sui diritti fondamentali dell'UE" e "dare alle persone e agli altri utenti la fiducia per adottare le soluzioni basate sull'IA, incoraggiando al contempo le imprese a svilupparle".

La relazione sembra inoltre precisare ancora meglio tale rapporto poiché l'accento non appare primariamente posto sul primo obiettivo, e cioè quello di regolare in maniera uniforme i requisiti tecnici dei sistemi di IA, tenendo *anche* conto dell'obiettivo di rispettare i diritti fondamentali. Al contrario, appare invece ben enfatizzato l'intento di eliminare o minimizzare i rischi per i diritti fondamentali, evitando l'introduzione di requisiti eccessivamente stringenti per le imprese. Dei due obiettivi previsti nel Libro bianco - "promuovere l'adozione dell'IA e affrontare i rischi associati a determinati utilizzi di tale tecnologia" - la proposta "mira ad attuare il secondo obiettivo al fine di sviluppare un ecosistema di fiducia proponendo un quadro giuridico per un'IA affidabile". Infatti "L'IA dovrebbe rappresentare uno strumento per le persone e un fattore positivo per la società, con il fine ultimo di migliorare il benessere degli esseri umani".

È la tutela dei diritti fondamentali a garantire un ecosistema di fiducia e a favorire pertanto lo sviluppo tecnologico ed affidabile dell'IA[24].

A prescindere dall'effettiva realizzazione di tale auspicio e dalla rispondenza del contenuto della proposta agli obiettivi prefigurati, quel che certamente la proposta fa emergere è che la regolazione (del mercato, e cioè dei prodotti e servizi che hanno sistemi di IA) non avviene 'nel rispetto dei' diritti fondamentali, bensì 'per', o meglio,

[24] Secondo la Commissione "Le regole per l'IA disponibili sul mercato dell'Unione o che comunque interessano le persone nell'Unione dovrebbero pertanto essere incentrate sulle persone, affinché queste ultime possano confidare nel fatto che la tecnologia sia usata in modo sicuro e conforme alla legge, anche in termini di rispetto dei diritti fondamentali". Gli obiettivi espressamente indicati dalla Commissione nella Relazione di accompagnamento alla proposta sono i seguenti: i) assicurare che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione; ii) assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'intelligenza artificiale; iii) migliorare la *governance* e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA; iv) facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato".

"attraverso" il prisma dei diritti fondamentali. È il differente diritto o il diverso livello di tutela dei diritti che guida un *risk based approach* consistente nell'imporre ai vari soggetti (utilizzatori, produttori, ecc.) divieti o obblighi tecnico-procedimentali, con gradazione diversa a seconda dei sistemi, dei settori e quindi dello standard di tutela considerato. Attraverso la "procedimentalizzazione" del rischio la tutela del diritto è incorporato *by design* nel sistema di IA.

Tale approccio presuppone (e chiede) necessariamente che lo standard di tutela dei diritti fondamentali sia, nel rispetto della Carta europea, non solo elevato ma soprattutto *uniforme* nell'ordinamento dell'Unione.

Un ulteriore importante obiettivo della dimensione europea è dunque quello di non frammentare, oltre al mercato, la stessa tutela dei diritti, evitando che siano i singoli Stati membri a decidere un diverso *standard* di tutela dei diritti fondamentali nel contesto dell'IA, con il rischio di fughe in avanti di alcuni Stati (divieti assoluti di alcuni sistemi) e indietro di altri (immissione nel mercato di sistemi nocivi per la salute, la vita la dignità delle persone). E soprattutto con il rischio di coesistenza di distinti meccanismi di regolazione, *ex ante* o *ex post*, per singoli settori o addirittura assente (con un presumibile aumento degli interventi da parte delle Corti costituzionali nel caso di asserito contrasto delle regolazioni nazionali con i diritti fondamentali del proprio ordinamento[25]).

Va inoltre, e infatti, osservato che le questioni che giungerebbero alla Corte di giustizia non potrebbero essere dirette a vagliare la compatibilità di tali normative alla luce della Carta europea (la quale come noto si applica solo nell'ambito del Trattato e non estende le competenze dell'Unione). Sarebbero invece questioni presumibilmente poste per verificare la legittimità di restrizioni nazionali alla luce delle norme sulla libera circolazione dei servizi o delle merci[26], nel consueto

[25] Cfr. A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Biolaw journal*, 2019, p. 63 ss.

[26] Si pensi inoltre al ruolo che le Corti costituzionali (in primis quella italiana) potrebbero svolgere per vagliare la conformità di una normativa nazionale di regolazione sull'IA che al contempo violasse una norma costituzionale e un diritto protetto dalla Carta europea.

rapporto dunque di regola (le libertà di circolazione) ed eccezione (la tutela dei diritti fondamentali).

L'ulteriore effetto di un intervento legislativo europeo sarà dunque quello di lasciare mani libere ai giudici nazionali nell'utilizzo dello strumento dell'art. 267 TFUE e consentire alla Corte di giustizia di vagliare il nuovo strumento regolatorio alla luce della Carta europea dei diritti sulla quale peraltro esso stesso si fonda. Resterà ovviamente da vedere se la Carta europea sia sufficiente ad esprimere i nuovi "diritti digitali" (diritto al controllo umano, diritto alla trasparenza algoritmica, ecc.) o se vi sia necessità di un nuovo catalogo di diritti, come prevede la Commissione[27].

La finalità di tutela (anche) dei diritti fondamentali perseguito dalla proposta di regolazione dell'IA non scalfisce in ogni caso la bontà della scelta della base giuridica dell'art. 114 TFUE, peraltro arricchita dal riferimento anche all'art. 16 TFUE (che consente alle istituzioni di adottare atti a tutela dei dati personali). Resta fermo, infatti, il carattere strumentale dell'intervento rispetto all'obiettivo del mercato interno, né si sarebbero potute percorrere altre vie. L'art. 2 TUE, ad esempio, non legittima l'adozione di atti da parte delle istituzioni, mentre l'art. 19 TFUE oltre ad avere un profilo limitato al principio di non discriminazione non costituirebbe un'idonea base giuridica in ragione della procedura legislativa speciale prevista nella stessa norma[28].

3. Il *risk based approch*, nell'evitare, in una dimensione europea, la frammentazione dei diritti oltre che del mercato, presuppone e valorizza un ulteriore elemento: e cioè che sia definita a monte la centralità di uno specifico diritto fondamentale, la sua irrinunciabilità o comunque la sua minore o maggiore rilevanza per un dato settore o per una data applicazione di IA.

---

[27] Comunicazione della Commissione, relativa alla definizione di una Dichiarazione europea sui diritti e i principi digitali del 26 gennaio 2022 (COM(2022) 27 e COM(2022) 28; per commenti si rinvia a P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea*?, in *Osservatorio europeo DUE*, marzo 2022, p. 1 ss., nonché E. CELESTE, *Towards a European Declaration on Digital Rights and Principles: Guidelines for the Digital Decade*, in *dcubrexitinstitute.eu*, 7 February 2022).

[28] In questo senso cfr. A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione*, cit.

Una delle premesse da cui infatti partire per comprendere le ragioni di un intervento regolatorio *ex ante*, è che in presenza di un diritto fondamentale della persona, il danno che può essere provocato da un uso non calibrato di tali applicazioni (o quanto meno di talune) è in alcuni casi talmente grave da *non* essere in alcun modo riparabile o compensabile *ex post*[29] (considerata peraltro anche l'estrema velocità con la quale si muove lo sviluppo delle nuove tecnologie).

Si pensi infatti ai danni che possono coinvolgere l'integrità fisica (si pensi ad esempio al caso classico delle auto a guida autonoma o alle diagnosi mediche errate o a prodotti difettosi e pericolosi) o psichica di una persona (manipolazioni, valutazioni errate, amministrative o giudiziarie, gravi discriminazioni sulla base dell'appartenenza ad una determinata etnia, mancato beneficio di servizi essenziali, lesione della privacy, *bias* cognitivi).

La prevenzione del danno corrisponde del resto ad un principio generalmente riconosciuto sia a livello nazionale che internazionale, come infatti dimostra il richiamo che ne fa, nel contesto della regolazione dell'IA, il Consiglio d'Europa[30]. Anche la Relazione alla proposta spiega che "Gli obblighi di prova *ex ante*, di gestione dei rischi e di sorveglianza umana faciliteranno altresì il rispetto di altri diritti fondamentali, riducendo al minimo il rischio di decisioni errate o distorte assistite dall'IA in settori critici quali l'istruzione e la formazione, l'occupazione, servizi importanti, le attività di contrasto e il sistema giudiziario. Nel caso in cui si verifichino comunque violazioni dei diritti fondamentali, un ricorso efficace a favore delle

[29] In tal senso anche C. REED, *How should we regulate artificial intelligence?*, in *Phil. Trans. R. Soc A 376*, 2018; P. NIEMITZ *Constitutional Democracy and Technology in the age of Artificial Intelligence, ivi,* 2018. V. anche il report *Need for democratic governance of artificial intelligence* 24 September 2020 (Parliamentary Assembly, Council of Europe); e il report *CAHAI(2020)23 Ad hoc Committee on artificial intelligence*, cit.

[30] Report *CAHAI(2020*)23 *Ad hoc Committee on artificial intelligence*, cit.: "The prevention of harm is a fundamental principle that should be upheld, in both the individual and collective dimension, especially when such harm concerns the negative impact on human rights, democracy and the rule of law. The physical and mental integrity of human beings must be adequately protected, with additional safeguards for persons and groups who are more vulnerable. Particular attention must also be paid to situations where the use of AI systems can cause or exacerbate adverse impacts due to asymmetries of power or information, such as between employers and employees, businesses and consumers or governments and citizens".

persone lese sarà reso possibile assicurando la trasparenza e la tracciabilità dei sistemi di IA unitamente a rigidi controlli *ex post*"[31].

L'identificazione *ex ante* dei diritti che in un dato ordinamento sono considerati inviolabili e non riparabili rispetto ad altri che possono essere considerati 'cedevoli' è un'operazione ovviamente indispensabile con riferimento ai sistemi che sono considerati con un rischio inaccettabile e dunque vietati. Come più volte ripetuto nei Considerando della proposta, la dignità della persona, la vita e la salute sono nel diritto dell'Unione europea, considerati irrinunciabili rispetto ad altre esigenze, siano esse di carattere economico, sociale o anche di protezione di altri diritti.

Dall'esame del contenuto della proposta, il *risk based approach* conduce tuttavia anche un altro tipo di operazione, non limitato ad un bilanciamento tra il diritto fondamentale e lo sviluppo dell'IA. Poiché i sistemi di IA possono invece anche dare un notevole contributo alla stessa tutela e rafforzamento dei diritti[32] (si pensi all'uso di tale tecnologia per le diagnosi sanitarie[33] o per la ricerca di persone scomparse o semplicemente per una maggiore trasparenza nelle

[31] Punto 3.5., p. 13. Il punto segue precisando che "Nel caso in cui si verifichino comunque violazioni dei diritti fondamentali, un ricorso efficace a favore delle persone lese sarà reso possibile assicurando la trasparenza e la tracciabilità dei sistemi di IA unitamente a rigidi controlli *ex post*".

[32] Si veda quanto espresso nella Relazione alla Proposta di regolazione dell'IA: "Definendo una serie di requisiti per un'IA affidabile e di obblighi proporzionati per tutti i partecipanti alla catena del valore, la presente proposta migliorerà e promuoverà la protezione dei diritti tutelati dalla Carta: il diritto alla dignità umana (articolo 1), al rispetto della vita privata e alla protezione dei dati di carattere personale (articoli 7 e 8), alla non discriminazione (articolo 21) e alla parità tra donne e uomini (articolo 23). Essa miraa prevenire un effetto dissuasivo sui diritti alla libertà di espressione (articolo 11) e alla libertà di riunione (articolo 12), nonché ad assicurare la tutela del diritto a un ricorso effettivo e a un giudice imparziale, della presunzione di innocenza e dei diritti della difesa (articoli 47 e 48), così come il principio generale di buona amministrazione. La presente proposta inciderà inoltre positivamente, secondo quanto applicabile in determinati settori, sui diritti di una serie di gruppi speciali, quali i diritti dei lavoratori a condizioni di lavoro giuste ed eque (articolo 31), un livello elevato di protezione dei consumatori (articolo 38), i diritti del minore (articolo 24) e l'inserimento delle persone con disabilità (articolo 26). Rilevante è anche il diritto a un livello elevato di tutela dell'ambiente e al miglioramento della sua qualità (articolo 37), anche in relazione alla salute e alla sicurezza delle persone".

[33] Per alcuni spunti, cfr. in dottrina, C. DE COSTANZO, *Access to intensive care and Artificial Intelligence. A Constitutional Perspective*, in *Italian Journal of Public Law*, n. 2, 2021, p. 494 ss.

selezioni, nell'adozione di decisioni amministrative o giurisdizionali, ecc.), la valutazione che il rischio che tali sistemi possono produrre per altri diritti fondamentali può essere bilanciato con i benefici che è in grado di generare per gli stessi diritti

Ai fini dell'immissione nel mercato o dell'uso di un sistema di IA la valutazione del connesso rischio di violazione di un diritto fondamentale va dunque svolta, in taluni casi, mediante il bilanciamento tra più diritti fondamentali e non tra i diritti, da un lato, e le esigenze del mercato.

Poiché la prevalenza di un diritto sull'altro dipende, anche in tal caso, dal rilievo che un dato ordinamento attribuisce ad un determinato diritto, la proposta rispecchia evidentemente le caratteristiche e specificità dell'ordinamento europeo.

Solo per fare un esempio, il rischio inaccettabile che pone un sistema di riconoscimento biometrico *in real time* da parte delle autorità pubbliche a fini di contrasto (e quindi il suo divieto) e la definizione comunque ad alto rischio di tale sistema se 'a posteriori', esprime la scelta di dare priorità al diritto fondamentale della vita privata e della tutela dei dati personali (di qui la base giuridica anche dell'art. 16 TFUE oltre che dell'art. 114 TFUE) rispetto al diritto alla sicurezza, che potrebbe essere garantito da una generale attività di sorveglianza di massa per fini di contrasto del crimine. La Corte ha già infatti stigmatizzato, come contrarie al diritto dell'Unione e alla Carta dei diritti, le attività di raccolta e la conservazione generalizzata e indifferenziata di dati personali per finalità di sicurezza nazionale[34].

Qualora però il sistema sia finalizzato alla ricerca *mirata* di potenziali vittime di reato, compresi i minori scomparsi, alla prevenzione di minacce di attacchi terroristici o all'azione penale di cui alla Decisione quadro 2002/584/GAI del Consiglio[35], il diritto alla vita privata e alla tutela dei dati personali (ed anche alla dignità) cede invece dinanzi a minacce all'integrità fisica delle persone. Conformemente a

[34] V. ad esempio, sentenza della Corte del 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net French Data Network Fédération des fournisseurs d'accès à Internet associatifs*, e causa C-623/17, *Privacy International*, concernenti il trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche.

[35] Decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri.

consolidati orientamenti, la compressione di tale diritto è dunque giustificata solo quando strettamente indispensabile al perseguimento di un obiettivo legittimo (quale può essere la vita e la sicurezza di altre persone) e limitata nel tempo[36].

Non mancano tuttavia alcune criticità nel testo della proposta. Ci si chiede ad esempio come mai l'uso di sistemi di *deepfake*, che il Parlamento europeo aveva consigliato di limitare al massimo in quanto altamente lesivi (della dignità, del diritto all'informazione)[37], siano invece considerati sistemi a rischio lieve, soggetti dunque ad un obbligo informativo[38]. Per di più tale obbligo cadrebbe non solo qualora l'uso sia autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati, ma anche quando sia *necessario per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e*

[36] Si veda anche la posizione del Parlamento europeo e il comunicato del 22 marzo 2022 secondo cui "The draft text also stresses that AI technologies could pose crucial ethical and legal questions. It highlights the challenge of reaching a consensus within the global community on minimum standards for the responsible use of AI, and concerns about military research and technological developments into lethal autonomous weapon systems. MEPs say that certain AI technologies enable the automation of information processing to an unprecedented scale. This paves the way for mass surveillance and other unlawful interference and poses a threat to fundamental rights, in particular the rights to privacy and data protection. Authoritarian regimes apply AI systems to control, exert mass surveillance and rank their citizens, or restrict freedom of movement. Dominant tech platforms use them to obtain more information on a person. Such profiling poses risks to democratic systems as well as to the safeguarding of fundamental rights, say MEPs".

[37] V. la risoluzione del Parlamento europeo, del 20 gennaio 2021, 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 (2020/2013(INI)). Al punto 76, il Parlamento "esprime profonda preoccupazione per le tecnologie di *deepfake*, che consentono di produrre foto, audio e video falsificati sempre più realistici che potrebbero essere utilizzati per compiere ricatti, creare notizie false o minare la fiducia dei cittadini e influenzare il dibattito pubblico; ritiene che tali pratiche siano in grado di destabilizzare paesi, diffondere la disinformazione e influenzare le consultazioni elettorali; chiede pertanto l'introduzione di un obbligo in base al quale tutti i materiali *deepfake* o altri video artificiali realizzati in modo realistico debbano essere etichettati come "non originali" dal loro creatore, con severi limiti al loro utilizzo a fini elettorali, e che tale obbligo sia applicato rigorosamente; chiede che siano svolte adeguate attività di ricerca in questo campo per garantire che le tecnologie di contrasto dei suddetti fenomeni siano al passo con gli utilizzi dolosi dell'IA".

[38] Ai sensi dell'art. 52 "Per tali sistemi occorre solo rendere noto che il contenuto è stato generato o manipolato artificialmente".

delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, e fatte salve le tutele adeguate per i diritti e le libertà dei terzi. A differenza, pertanto, di altri sistemi indicati sempre dall'art. 52 (i sistemi che interagiscono con le persone - i c.d. *chatbot* - i sistemi di riconoscimento delle emozioni e quelli di categorizzazione biometrica) in riferimento ai quali la deroga all'obbligo informativo è prevista solo (e più correttamente) nei casi autorizzati dalla legge per accertare, prevenire, indagare e perseguire reati, nel caso dei *deepfake* la libertà di espressione (e la libertà delle arti e scienze) prevale dunque, secondo una valutazione *ex ante*, sugli altri diritti considerati dalla norma. Tale previsione, tuttavia, appare stridere con la centralità riservata dall'Unione al diritto alla dignità della persona e alla protezione dei diritti democratici[39], e con l'approccio adottato recentemente in altri contesti paralleli (come, ad esempio, nell'ambito del *Digital Services Act*[40]).

Di criticità ve ne possono essere altre (come il divieto solo per le pubbliche autorità dell'utilizzo dei sistemi di punteggio sociale, o come il divieto dei sistemi che usano tecniche subliminali e manipolatorie

[39] V. anche la bozza di risoluzione del PE del novembre 2021; il PE "Illustrates that AI technologies could also help perpetrators by simplifying the use of very sophisticated cyberattacks, such as through AI-powered malware, identity theft using biometric data or adversarial AI that causes other AI systems to misinterpret input; points, in particular, to the rise in deepfakes, which already lead to doubts about the authenticity of all digital content, including genuinely authentic videos; warns that deepfakes could contribute to a broad climate of public mistrust in AI, as well as a deeper socio-political polarisation within our societies". In linea generale l'approccio dell'Unione appare discostarsi da quello statunitense. Il primo, nel porre al centro la dignità della persona, porta ad esempio a ritenere cedevole la libertà di espressione e informazione se ciò comporta la diffusione di *hate speeches, fake news* attraverso le piattaforme digitali; il secondo, invece, ritiene che la libertà di espressione non possa in alcun modo essere limitata e censurata dal pubblico potere e si affida pertanto all'autoregolazione da parte delle stesse piattaforme.

[40] Il Parlamento europeo aveva ad esempio proposto un emendamento al considerando n. 63 (pubblicità nelle piattaforme), ritenendo fosse necessario l'etichettatura *di "qualsiasi file video, audio o di altro tipo di cui sia nota l'origine deepfake"*, unitamente all'inserimento di un nuovo art. 30 *bis*, secondo cui "Qualora una piattaforma online di dimensioni molto grandi si renda conto di contenuti deepfake, ossia di immagini o contenuti audio o video generati o manipolati che presentano una notevole somiglianza con persone, oggetti, luoghi o altre entità o eventi reali e che sono tali da falsamente apparire autentici o veritieri, il prestatore etichetta tali contenuti in modo da informare in maniera chiaramente visibile per il destinatario dei servizi che si tratta di contenuti non autentici".

solo in riferimento a specifici gruppi di età e solo qualora sia prevedibile che si produca un danno fisico o psicologico)[41].

La proposta è in ogni caso ancora in discussione e potrebbe essere suscettibile di modifiche. Quel che tuttavia preme in tale sede evidenziare è che laddove la norma sia vaga e il margine sia sufficientemente ampio da consentire un bilanciamento *ex post* (eventualmente anche da parte della Corte di giustizia), ne verrebbe meno la certezza del diritto in termini di classificazione di un sistema come vietato o ad alto rischio e dunque l'efficacia dello stesso *risk based approach*. Al contrario, qualora la norma sia eccessivamente dettagliata, il bilanciamento tra i diritti già svolto *ex ante* rischia di non lasciare spazio a correzioni.

4. La complessità di un bilanciamento *ex ante* tra i vari diritti ed esigenze è ancor più tangibile in riferimento ad altro aspetto. Un elemento di riflessione da non tralasciare è infatti quello che attiene alla necessità di una valutazione *ex ante* del rischio di un sistema IA per i diritti fondamentali che sia il più possibile oggettiva.

In alcuni contesti tale elemento è sicuramente apprezzabile. Determinate applicazioni di IA sono vietate o considerate ad alto rischio in quanto *oggettivamente* dannose per i diritti fondamentali: l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto (art. 5, lett. a); l'immissione o utilizzo di un sistema di punteggio sociale (art. 5, lett. c); i sistemi destinati ad essere utilizzati come componenti di sicurezza di un prodotto o che siano essi stesso un prodotto (art. 6). In questi casi la proposta prescinde da una valutazione soggettiva o dalla reazione del potenziale interlocutore e l'operazione di classificazione appare dunque più semplice. Vale tuttavia la pena notare l'esistenza di deroghe ed eccezioni (es. nel caso già riferito delle eccezioni al divieto di sistemi di riconoscimento biometrico), o la limitazione della qualificazione di "alto rischio" a sistemi di IA qualora utilizzati nel settore privato[42]. Va inoltre ricordato che la proposta non include nel campo di applicazione

[41] Art. 5.
[42] V. però, infra, par. 6.

del regolamento i sistemi negli usi militari, nonostante la posizione assunta dal Parlamento europeo[43].

Più delicata è la dimensione soggettiva. I sistemi di IA possono infatti interagire con l'uomo ed elaborare decisioni in maniera autonoma e vanno dai sistemi più semplici (*chatbot*) a quelli più elaborati che possono utilizzare tecniche subliminali e che possono distorcere il comportamento. Per questi tipi di sistemi, la regolazione *ex ante* rischia effettivamente di non valutare attentamente le diverse vulnerabilità o reazioni personali di distinti soggetti[44].

In riferimento ai sistemi vietati, l'art. 5 tenta ad esempio di "oggettivizzare" fenomeni di rischio ancorando il concetto di vulnerabilità a particolari categorie (sistemi che sfruttano la minore età o disabilità fisica o mentale al fine di distorcerne il comportamento e in modo da provocare o poter provocare un danno) o alla tipologia della tecnica (es. la tecnica subliminale, che elimina la consapevolezza della persona ed è finalizzata a distorcere il comportamento)[45]. La norma non sarà di facile applicazione perché richiede, ai fini del divieto del sistema, che siano prospettabili tutti gli elementi indicati (la finalità di distorcere il comportamento, la non consapevolezza di essere soggetto ad una tecnica subliminale, la previsione di un danno, ecc.). Per altro verso, la norma esclude di fatto dal divieto i sistemi di IA, diversi dalle tecniche subliminali, che sfruttano le vulnerabilità soggettive di

[43] Dal regolamento sono espressamente escluse le applicazioni per uso militare. Il parlamento europeo aveva invece suggerito di vietarle a meno che non fosse assicurato un controllo umano. V. la risoluzione, del 20 gennaio 2021, sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale 2020/2013(INI). V. anche la precedente risoluzione del 12 settembre 2018 sui sistemi d'arma autonomi 2018/2752 (RSP).

[44] V. anche la risoluzione del Parlamento europeo del 19 maggio 2021, sull'intelligenza artificiale nell'istruzione, nella cultura e nel settore audiovisivo, A9-0127/2021).

[45] Art. 5, par 1, lett. a): i sistemi di IA che "utilizzano tecniche subliminali senza che una persona ne sia consapevole al fine di distorcere materialmente il comportamento di una persona in modo che provochi o possa provocare a tale persona o ad altre persone un danno fisico o psicologico" e lett. b): i sistemi che "sfruttano la vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona in modo che provochi o possa provocare a tale persona o ad altre persone un danno fisico o psicologico".

individui diversi dai minori o da coloro che sono affetti da disabilità fisica o psichica; così come resterebbero fuori le tecniche subliminali o quelle che sfruttano le vulnerabilità delle indicate categorie, qualora si ritenga *ex ante* che abbiano un'altra finalità o, sempre *ex ante*, non siano suscettibili di provocare un danno[46]. Non introducendo un divieto totale e oggettivo di tali sistemi, il rischio è dunque che la norma non offra una garanzia di certezza e precisione che invece la regolazione *ex ante* si propone di dare nel vietare o autorizzare un determinato sistema di IA.

5. La necessità di evitare *ex ante* la lesione di diritti fondamentali di primaria importanza (dignità, diritto alla privacy, ecc.), non può inoltre essere riguardata in una dimensione unicamente individuale, ma va anche letta in considerazione dell'interdipendenza dei diritti tra loro, del loro valore per la società nel suo complesso, e dunque della loro inscindibilità dalla tutela della *rule of law* e dei principi democratici di un determinato ordinamento[47].

"*Human rights, democracy, and the rule of law are closely linked*", così ricorda il report del Consiglio d'Europa *Artificial Intelligence, Human rights, democracy, and the Rule of Law* riprendendo a sua volta quanto ben sintetizzato nella Dichiarazione di Vienna del 1993 "*All human rights are universal, indivisible and interrelated*"[48].

[46] Una versione precedente della bozza prevedeva un'applicazione più estesa del divieto. La norma non faceva riferimento al danno fisico o psicologico ma semplicemente a uno "svantaggio". Inoltre la "vulnerabilità" richiamata dalla lett. b) non era limitata solo ad alcune categorie di persone ma era intesa in termini generali; cfr. anche G. D'ACQUISTO, *Intelligenza artificiale, obiettivo regole privacy per renderla "umana"*, in *Agendadigitale*, 20 aprile 2021.

[47] V. anche *l'Expalanatory memorandum*, allegato alla proposta di regolamento sull'IA, ove la Commissione che precisa "the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society […] artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law" (considerando 4).

[48] Council of Europe, June 2021 "Human rights, democracy, and the rule of law are closely linked. The capacity of legitimate governments to effectively safeguard human rights is predicated on the interdependence of robust and accountable democratic institutions, inclusive and transparent mechanisms of decision-making, and an independent and impartial judiciary that secures the rule of law. Most generally, human rights are the basic rights and freedoms that are possessed by every person in the world from cradle to grave and that preserve and protect the inviolable

E dunque, solo per fare qualche esempio[49], quando è l'algoritmo a decidere come veicolare dati e notizie, è noto che l'impatto si produca sia sui diritti del singolo (corretta informazione) che sui principi democratici, influenzando i processi elettorali[50] o favorendo la creazione di nuovi modelli sociali e politici anche a causa della concentrazione di potere solo in alcune piattaforme digitali. Lo stesso dicasi per i sistemi di riconoscimento biometrico che possono condurre, oltre alla violazione della privacy o di dati personali, anche ad una sorveglianza di massa, con rischi di autoritarismo o assunzione di decisioni restrittive allo scopo di controllare le proteste o anche di prevederle (e quindi evitare che si svolgano). La mancanza di anonimato può inoltre scoraggiare i cittadini a una libera manifestazione del pensiero, a una partecipazione attiva nella società e ad esprimere opinioni e giudizi. Decisioni che vengano elaborate attraverso sistemi di IA possono minare sia il diritto del singolo a veder tutelati i propri interessi che i principi *rule of law* nella misura in cui incidano sull'indipendenza del giudice[51], così come sulla

dignity of each individual regardless of their race, ethnicity, gender, age, sexual orientation, class, religion, disability status, language, nationality, or any other ascribed characteristic. These fundamental rights and freedoms create obligations that bind governments to respecting, protecting, and fulfilling human rights. In the absence of the fulfilment of these duties, individuals are entitled to legal remedies that allow for the redress of any human rights violations".

[49] Si vedano in particolare e più diffusamente i report e gli studi del Consiglio d'Europa *Artificial Intelligence, Human rights, democracy, and the Rule of Law* (a Primer), June 2021*; Towards Regulation of AI systems* (December 2020); *Ad hoc Committee on artificial intelligence*, Feasibility Study,17 Decemer 2020 (CAHAI (2020) 23); *Study on the impact of Digital transformation on Democracy and good governance*, 26 July 2021.

[50] Sul punto si veda anche l'Opinion No. 974/2019, *European Commission for Democracy through Law (Venice Commission), Principles for a fundamental Rights-compliant Use of Digital Technologies in electoral Processes* – approved by Council of Democratic Elections at its 70th online meeting (10 December 2020) and adopted by the Venice Commission at its 125th online Plenary Session (11-12 December 2020).

[51] Sul punto v. anche la comunicazione della Commissione, del 2 dicembre 2020, Digitalizzazione della giustizia nell'Unione europea. Un pacchetto di opportunità, COM(2020) 710 final. In dottrina cfr. F. DONATI, *Intelligenza artificiale giustizia*, in *Rivista AIC*, n. 1, 2020, p. 415 ss. Si ricorda inoltre *la Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giuridici e negli ambiti connessi*, del 3 dicembre 2018; cfr. al riguardo, tra gli altri, A. PAJNO, *L'uso dell'intelligenza artificiale nel processo tra problemi nuovi e questioni antiche*, in *Astrid Rassegna*, n. 18, 2021; M. LIBERTINI, M. R. MAUGERI, E. VINCENTI, *Giustizia predittiva e*

partecipazione ai processi di *decision making*, o sul buon andamento e trasparenza della pubblica amministrazione. Analisi predittive e le valutazioni da parte di enti creditizi, datori di lavoro o anche pubbliche autorità possono erodere i diritti civili e al contempo creare discriminazioni all'interno della società *targettizzando* gruppi di persone sulla base dell'età, etnia, lingua, ecc.

Si tenga peraltro presente che tali principi potrebbero essere violati anche nel caso in cui non si sia verificata una specifica lesione nel caso singolo. L'erronea attribuzione di un beneficio sociale, a seguito di un funzionamento non corretto di un sistema di IA, a favore di un cittadino che non avrebbe i requisiti per ottenerlo, non viola nel caso specifico alcun diritto individuale ma lede certamente il principio del buon andamento dell'amministrazione[52]. Può inoltre accadere che non vi sia a livello individuale un'esatta percezione della lesione (o che la percezione sia addirittura assente) che invece ha rilievo se riguardata a livello collettivo. Si pensi alla sorveglianza di massa o alla disinformazione sulle piattaforme digitali.

Poiché la lesione che sistemi di intelligenza artificiale possono cagionare ai diritti fondamentali può essere particolarmente elevata e soprattutto in grado di minare direttamente i principi democratici e la *rule of law*, emerge dunque in maniera del tutto chiara la valutazione di rischio inaccettabile che presentano alcuni sistemi di IA in ragione dell'interesse pubblico sotteso[53].

---

giurisdizione civile. Primi appunti, in *Astrid Rassegna*, n. 16, 2021; U. RUFFOLO (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, Torino, 2021.

[52] V. anche *Getting the Future – Artificial Intelligence and Fundamental right*s, cit., p. 28, il quale ad esempio precisa che "A public agency combatting hate crime uses an AI-based tool to detect online hate speech by analysing patterns of speech online. On the basis of the processing, the system determines which social groups are targeted. This helps law enforcement adopt measures to protect them before threats are realised. Although the tool aims to identify potential victims, rather than perpetrators, law enforcement can use the information generated by the system to ask social media providers for information on users to pursue criminal investigations" (p. 36).

[53] Il regolamento persegue una serie di motivi imperativi di interesse pubblico "quali un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali (considerando 1). L'intelligenza artificiale può nel contempo, a seconda delle circostanze relative alla sua applicazione e al suo utilizzo specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti tutelati dalla legislazione dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale". Sull'interesse pubblico nella regolazione dell'IA, sulla sua definizione, sui differenti approcci e soluzioni,

6. Come noto, ai diritti e libertà fondamentali della persona, nella sua individualità o collettività corrispondono generalmente una serie di obblighi di rispetto e protezione che gravano sia su altri soggetti privati che sullo Stato[54]. Quanto appena esposto ci conduce pertanto ad un'ulteriore dimensione: quella pubblica in rapporto a quella privata.

Diversi appaiono i piani di coinvolgimento dello Stato e/o delle pubbliche autorità nell'ambito della regolazione dell'IA e sotto il profilo del diritto dell'Unione europea.

In primo luogo, anche gli Stati e le loro pubbliche autorità (ad esclusione di quelle di Stati terzi[55]) risultano essere soggetti destinatari del futuro regolamento.

Lo Stato è tuttavia un destinatario 'qualificato'. Si osservi infatti che talune applicazioni di IA comportano infatti un rischio inaccettabile – e dunque sono vietate – proprio nella misura in cui siano utilizzate nel settore pubblico[56]. L'art. 5, par. 1, lett. c) vieta ad esempio l'immissione

---

anche nei doversi contesti in cui operano i sistemi di IA, cfr. in dottrina G. GANTZIAS, *Dynamics of Public Interest in Artificial Intelligence: 'Business Intelligence Culture' and Global Regulation in the Digital Era*, in S.H. PARK ET AL (eds.), *The Palgrave Handbook of Coroporate Sustainabilty in the Digital Era*, Hellenic Open University, Patras Greece, 2021, p. 259 ss.; A. DIGNAM, *Artificial intelligence, tech corporate governance and the public interest regulatory response*, in *Cambridge Journal of Regions, Economy and Society*, 2020, p. 37 ss., secondo cui "The biggest challenge lies not in identifyeng the problems with AI and its controllers but the public governance response"; N. ELKIN-KOREN, *Contesting algorithms: Restoring the public interest in content filetring by artificial intelligence*, in *Big Data and Society*, 2020, p. 1 ss.

[54] Per alcuni spunti, *ex multis* A. PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, F. PAOLO PATTI, O. POLLICINO, S. QUATTROCOLO, D. SIMEOLI E P. SIRENA, *AI: profili giuridici Intelligenza artificiale: criticità emergenti e sfide per il giurista*, in *Biodiritto.*

[55] Secondo l'art. 1 "il presente regolamento non dovrebbe applicarsi alle autorità pubbliche di un paese terzo e alle organizzazioni internazionali che agiscono nel quadro di accordi internazionali conclusi a livello nazionale o europeo per la cooperazione delle autorità giudiziarie e di contrasto con l'Unione o con i suoi Stati membri. Tali accordi sono stati conclusi bilateralmente tra Stati membri e paesi terzi o tra l'Unione europea, Europol e altre agenzie dell'UE e paesi terzi e organizzazioni internazionali".

[56] V. anche il report FRA secondo cui "The White Paper on AI indicates the Commission's preference for the possible new regulatory framework to follow a risk-based approach, in which mandatory requirements would, in principle, only apply to high-risk applications. These would be determined on the basis of two cumulative

sul mercato, la messa in servizio o l'uso di sistemi di IA *da parte alle autorità pubbliche* (o per loro conto) finalizzate a valutare il comportamento sociale delle persone fisiche, o la classificazione della loro affidabilità, sulla base della loro personalità o di caratteristiche personali, e dunque all'attribuzione di un punteggio sociale[57].

Un ruolo molto marcato del settore pubblico emerge inoltre nell'ulteriore classificazione delle applicazioni ad alto rischio contenute nell'Allegato III, richiamato dall'art. 6, par. 2. La lista dei settori è lunghissima[58], ma quel che è utile rilevare è che, anche in tal caso, la maggior parte dei sistemi considerati ad alto rischio sono quelli messi in servizio o utilizzati da pubbliche autorità (incluse autorità di contrasto e autorità giudiziarie) o per la prestazione di servizi pubblici[59].

Tale approccio rimarca dunque la consapevolezza, da parte dei redattori della norma, di una particolare responsabilità della Stato e delle pubbliche autorità, in ragione degli interessi generali sottesi, e di una conseguente inaccettabilità del rischio che sistemi di IA, proprio in

---

criteria: if it is employed in a sector, such as healthcare, transport or parts of the public sector, where significant risks can be expected to occur; and if it is used in a manner where significant risks are likely to arise" (p. 22). Lo stesso report sottolinea come alcuni settori sono particolarmente sensibili riguardo ai diirtti fondamentali (social benefits, predictive policing, health services, and targeted advertising): "These areas are particularly sensitive as regards fundamental rights. Two cover mainly the public administration's use of AI (social benefits allocation and predictive policing). The other two concern private companies (health services and targeted advertising)" (p. 26).

[57] E "il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari: i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità".

[58] La gestione e funzionamento delle infrastrutture critiche, l'istruzione e formazione professionale, l'occupazione, gestione dei lavoratori e accesso al lavoro autonomo; l'accesso a prestazioni e servizi pubblici e a servizi privati essenziali; i servizi di emergenza di primo soccorso compresi vigili del fuoco, le applicazioni utilizzate per le attività di contrasto, la gestione della migrazione, dell'asilo e del controllo delle frontiere, l'amministrazione della giustizia e processi democratici.

[59] Sulla regolazione dell'IA nell'ambito della pubblica amministrazione si rinvia a E. CHITI, B. MARCHETTI, N. RANGONE, *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni: prove generali.*

quanto utilizzati nell'ambito dei pubblici poteri, appaiono essere ancor più lesivi dei diritti fondamentali.

Ciò sia in ragione dell'obbligo generale che lo Stato ha di proteggere i singoli diritti fondamentali sia in considerazione del fatto che il rischio di danno che un sistema di IA può produrre coinvolge non solo i diritti individuali ma si ripercuote anche sui principi generali che la pubblica autorità e lo Stato in genere sono tenuti ad osservare e dunque investe interessi di natura collettiva. Si pensi ad esempio al buon andamento dell'amministrazione[60], o all'obbligo di garantire una tutela giurisdizionale effettiva (art. 19 TUE e art. 47 della Carta).

In secondo luogo, lo Stato è anche il garante della corretta applicazione e del rispetto della nuova disciplina. Sotto tale profilo il suo primo obbligo è quello di adottare prontamente eventuali misure che si ritengano indispensabili affinché il regolamento possa concretamente avere efficacia. La complessità che a volte tali atti presentano (pensiamo anche al regolamento *privacy*) può rendere necessaria l'adozione di misure di integrazione, esecuzione, accompagnamento al fine di rendere concretamente operativo il suo funzionamento[61]. E questo è certamente anche il caso del Regolamento sull'IA. Il riferimento maggiore è ovviamente alla predisposizione di una struttura di *governance* a livello nazionale, e all'effettività della funzione di controllo e di sanzione.

In terzo luogo, lo Stato ha un ruolo che trascende la proposta di regolazione dell'IA proprio in ragione della dimensione 'collettiva' della tutela dei diritti fondamentali nella regolazione dell'IA, e in particolare della *rule of law* e dei principi democratici.

Particolare attenzione deve ad esempio rivolgersi all'obbligo di generale rispetto dei principi democratici, connessi all'uso di sistemi di IA, che discende dall'appartenenza al Consiglio d'Europa e all'Unione europea.

Riguardo al primo va innanzitutto segnalata l'intenzione di adottare una convenzione, proprio sotto lo specifico profilo della tutela dei

[60] V. anche *Getting the Future – Artificial Intelligence and Fundamental right*s, FRA report 2020, p. 81.
[61] Sentenza della Corte del 26 febbraio 2008, causa C-132/05, *Commissione c. Germania*; dell'11 febbraio 2001, causa C-403/98, *Monte Arcosu.*

principi democratici nel contesto dell'IA[62].· Ulteriori responsabilità possono poi in particolare discendere dalla CEDU. Benché la Corte europea di Strasburgo non si sia ancora pronunciata espressamente su questioni riguardanti nello specifico l'uso delle applicazioni di IA[63], in alcune pronunce essa ha già stigmatizzato la violazione di diritti fondamentali (in particolare degli artt. 8, 10 e 14 CEDU) e dei principi democratici per profili connessi ad un utilizzo non ritenuto conforme (o all'abuso) degli algoritmi[64], sia da parte delle stesse pubbliche autorità che da parte degli operatori privati.

Sempre sulla base della CEDU, la responsabilità dello Stato va tuttavia oltre gli obblighi di sorveglianza, controllo, o attuazione della normativa. La Corte di Strasburgo ha, infatti, da lungo tempo precisato che gli obblighi che discendono per lo Stato dalla non si limitano a obbligazioni 'in negativo' ma si estendono ad azioni 'in positivo' [65].

Poiché, ai fini della tutela dei principi democratici, il bilanciamento dei vari diritti in gioco non può essere delegato ad operatori privati – i quali infatti non hanno neppure un obbligo generale di sorveglianza[66] - è evidente che la regolazione privata, anche la più stringente, incontra

[62] V. ad esempio risoluzione n. 2341 (2020), *Need for democratic governance of AI*, del 22 ottobre 2020;

[63] V. anche *Feasibility Study, "Ad Hoc Committee on Artificial Intelligence"*- 17 Decembre 2020, Council of Europe.

[64] I casi hanno riguardato la sorveglianza di massa (ECtHR, 13 September 2018, *Big Brother Watch and others v. the United Kingdom*, case referred to the Grand Chamber in February 2019; ECtHR, 19 June 2018, *Centrum För Rättvisa v. Sweden*, No. 35252/08 referred back to the Grand Chamber in February 2019 - hearing held on 10 July 2019); l'interferenza nei processi elettorali (*ECtHR* 23 January 2018, *Magyar Kétfarkú Kutya Párt v. Hungary*, case referred to the Grand Chamber in May 2018); la responsabilità editoriale delle piattaforme (ECtHR, 16 June 2015, *Delfi AS v. Estonia*; l'elaborazione da parte di pubbliche autorità di dati e informazioni attraverso sistemi statistici e tecniche per ottenere valutazioni in campo finanziario ed economico (ECtHR, 4 June 2019, *Sigurður Einarsson and Others v. Iceland*); l'abuso da parte di autorità pubbliche di sistemi di sorveglianza al fine di prevedere e prevenire la commissione di illeciti (ECtHR, 29 June 2006, *Weber and Saravia v. Germany*, No. 54934/00).

[65] *Artificial Intelligence in the Audiovisual sector* – European Audiovisual Observatory (Council of Europe) 2020, p. 65 ss.

[66] Si veda la relazione introduttiva al *Digital Services Act* (p. 13), e il contenuto della proposta. V. anche sentenza dela Corte del 3 ottobre 2019, causa C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland* (a proposito della ricerca attraverso sistemi algoritmici di contenuti lesivi o illeciti).

un limite proprio nello stesso interesse pubblico sotteso alla sua introduzione[67].

L'art. 10 della CEDU, che impone agli Stati di tutelare la libertà di espressione "senza interferenza da parte della pubblica autorità" implica che lo Stato non solo debba astenersi da interventi che limitino il pluralismo di informazione ma debba anche agire attivamente al fine di rimuovere gli ostacoli all'interno del proprio ordinamento[68]. Obblighi in positivo discendono inoltre ed evidentemente anche dall'art. 11 della Carta europea sui diritti, il quale, al par. 2 stabilisce che "il pluralismo dell'informazione è rispettato"[69]. Anche tale norma è formulata in negativo ma da lungo tempo la Corte di giustizia ne ha tratto un contenuto molto più esteso[70], che include tutte le azioni che lo Stato è tenuto a svolgere, anche in adempimento di regole rivolte in contesti diversi, al fine di garantire e promuovere la diversificazione dei media, e dunque il pluralismo dell'informazione.

Ed è quanto si propone effettivamente l'Unione nel chiedere agli Stati membri interventi su più fronti a garanzia del pluralismo dell'informazione e, in particolare per controbilanciare i rischi che la digitalizzazione e l'uso di sistemi algoritmici può comportare[71].

---

[67] Per alcune proposte, cfr. N. ELKIN-KOREN, *Contesting algorithms: Restoring the public interest in content filetring by artificial intelligence*, cit.

[68] La Corte EDU pur non giungendo ad occuparsi direttamente dell'uso algoritmico nell'informazione, da parte ad esempio dei *new media*, ha, in talune pronunce, ritenuto l'esistenza di un obbligo di garantire l'accesso imparziale ai *new media* (ECtHR, *Manole e.a. c. Moldova*, par. 100) o di adottare una solida legislazione amministrativa al fine di garantire il pluralismo nel settore audiovisivo (ECtHR, *Center Europa 7 Di Stefano c. Italy* (2021), No. 38433/09, para 134). Utili spunti derivano inoltre dalla raccomandazione del 2018 *sul pluralismo dei media del Consiglio d'Europa* (CM/Rec (2018)1).

[69] *Ex multis* B. NASCIMBENE, F. ROSSI DAL POZZO, *L'evoluzione dei diritti e delle libertà fondamentali nel settore dei media. Diritto dell'Unione europea e orientamenti giurisprudenziali*, in *rivista.eurojus.it*, 2019, p. 132 ss.

[70] Sentenza della Corte del 30 aprile 1974, causa C-155/73, *Sacchi*; conclusioni dell'avvocato generale Poiares Maduro, del 12 settembre 2007, causa C-350/05, *Centro Europa 7*.

[71] Comunicazione della Commissione sul piano per la Democrazia europea, 3 dicembre 2020, COM(2020) 790 final. Come ben illustrato dal *Democracy Action Plan*, tali strumenti sono di vario tipo ad includono anche interventi sia nei confronti degli Stati che delle imprese. Accanto a strumenti mirati che gli Stati dovrebbero adottare per ridurre il *digital devide* (e dunque ampliare l'accesso alle informazioni) la Commissione focalizza espressamente l'attenzione anche sul tema degli aiuti di Stato per la digitalizzazione dei *new media* ai fini di una maggiore offerta

7. Un'ultima considerazione: poiché l'intelligenza artificiale si avvale di dati, di algoritmi e della rete, essa non può neppure essere regolata con successo a livello solo locale (nazionale, europeo, statunitense, cinese). L'esistenza di *big-tech* di dimensioni mondiali e la circolazione dei dati, personali e non personali, a livello globale è allo stesso tempo causa ed effetto dell'evidente interconnessione dei mercati e servizi digitali. E questo è un dato chiaramente noto.

Non è infatti un caso che proposte, programmi o semplicemente ipotesi di regolazione dell'intelligenza artificiale siano elaborate in numero crescente anche nell'ambito di organizzazioni internazionali (UNESCO, ONU, Consiglio d'Europa, UE). A seconda dei contesti queste ovviamente variano sia nei contenuti che negli strumenti proposti.

In ambito europeo i punti in comune tra Consiglio d'Europa e Unione europea sono ovviamente numerosi ponendosi entrambe le organizzazioni l'obiettivo di uno *standard* particolarmente elevato nella tutela dei diritti fondamentali, dei principi democratici e della *rule of law*[72]. Le finalità e le modalità di intervento sono però evidentemente differenti. Mentre gli interlocutori del Consiglio d'Europa sono come noto solo gli Stati, l'Unione europea è in grado di rivolgersi direttamente a tutte le categorie di soggetti e/o operatori pubblici e privati (incluse dunque anche le piattaforme digitali).

La proposta presentata dalla Commissione, ancora migliorabile in alcune sue parti, rappresenta un progetto di ampia portata poiché

---

dell'informazione (v. anche la comunicazione della Commissione I media europei nel decennio digitale: un piano d'azione per sostenere la ripresa e la trasformazione, del 3 dicembre 2021 COM(2020) 784 final e la risoluzione del Parlamento europeo, del 19 maggio 2021, sull'intelligenza artificiale nell'istruzione, nella cultura e nel settore audiovisivo, A9-0127/2021); nonché per alcuni profili il report *Artificial Intelligence in the audiovisual sector*, cit. *Guiding template: Digitalisation of news media*.

[72] Report del Consiglio d'Europa *Artificial Intelligence, Human rights, democracy, and the Rule of Law*, June 2021*; Towards Regulation of AI systems* (December 2020); *Ad hoc Committee on artificial intelligence*, Feasibility Study, 17 December 2020 (CAHAI (2020) 23); *Study on the impact of Digital transformation on Democracy and good governance*, 26 July 2021; *Artificial Intelligence in the audiovisual sector,* European Audiovisual Observatory, 2020.

investe in maniera trasversale tutti i settori e si fonda su un difficile e complesso bilanciamento tra le esigenze del mercato e la tutela dei diritti fondamentali, nonché tra gli stessi diritti. La sfida che l'Unione si pone non è solo quella di diventare leader mondiale nello sviluppo di un'intelligenza artificiale, ma anche quella di garantire un elevato *standard* di diritti fondamentali.

L'occasione è dunque quella di generare un nuovo "effetto Bruxelles"[73], come già avvenuto per il regolamento *privacy* e che rivestirà particolare importanza proprio per la tutela o esportazione di principi democratici e della *rule of law*. Il fatto che via sia una condivisione tra i valori della proposta europea e quelli del Consiglio d'Europa faciliterà senz'altro tale compito. Ricordiamo infatti che quest'ultimo ha già preannunciato l'adozione di una convenzione, obbligatoria per gli Stati membri, per dare seguito alla risoluzione del 2020 il cui titolo ben sintetizza il suo auspicio: *Need for democratic governance of AI*[74].

[73] F. DONATI, *Verso una nuova regolazione delle piattaforme digitali*, in *Rivista della Regolazione dei Mercati*, n. 2, 2021, p. 238 ss.

[74] Risoluzione n. 2341 (2020), *Need for democratic governance of AI*, del 22 ottobre 2020. Tra le altre risoluzioni adottate v. risoluzione n. 2343 (2020), *Preventing discrimination caused by the use of artificial intelligence*, del 22 ottobre 2020; risoluzione n. 2345 (2020), *Artificial intelligence and labour markets; friends or foe?* del 22 ottobre 2020.