

RIVISTA ELETTRONICA DI DIRITTO, ECONOMIA, MANAGEMENT



Inquadra il QR-CODE
per il download
degli altri numeri
della Rivista

Numero 3 - 2022 - Supplemento 1
**Intelligenza artificiale
e Nuove Forme di Discriminazione**
**atti del Convegno a cura di Maria Novella Campagnoli
e Massimo Farina**

FONDATA E DIRETTA DA
DONATO A. LIMONE

La “Rivista elettronica di Diritto, Economia, Management” è un periodico totalmente digitale, accessibile e fruibile gratuitamente, che ha lo scopo di trattare le diverse tematiche giuridiche, economiche e manageriali con un approccio integrato e trasversale, di tipo comparato, in un contesto locale, nazionale, comunitario ed internazionale caratterizzato dalla società dell'informazione, dalla trasformazione digitale, dalla globalizzazione dei mercati, da processi innovativi di tipo manageriale ed organizzativo nei settori pubblico e privato.

La rivista ha anche la finalità di ospitare contributi di giovani studiosi per valorizzarne le attitudini alla ricerca e il loro contributo allo sviluppo delle scienze giuridiche, sociali, economiche e manageriali.

Direttore responsabile: Donato A. Limone

Comitato scientifico: Estanislao Arana García, Catedrático de Derecho administrativo de la Universidad de Granada (Spagna); Piero Bergamini (Comitato Direttivo del Club degli Investitori di Torino); Francesco Capriglione (professore di diritto degli intermediari e dei mercati finanziari, Luiss, Roma); Mario Carta (Professore di diritto dell'Unione europea dell'Università degli Studi di Roma Unitelma Sapienza); Enzo Chillelli (esperto di sanità e di informatica pubblica); Claudio Clemente (Banca d'Italia); Fabrizio D'Ascenzo (professore ordinario, preside della Facoltà di Economia, Università “La Sapienza”); Angelo Del Favero (“Health and Welfare School”, Università degli Studi di Roma “Unitelma Sapienza”); Luigi Di Viggiano (Università del Salento; esperto di scienza dell'amministrazione digitale); Jorge Eduardo Douglas Price, ordinario di Teoria generale del diritto; Direttore del Centro di Studi Istituzionali Patagónico (CEIP), Facoltà di Giurisprudenza e Scienze Sociali dell'Università Nazionale di Comahue (Argentina); Maria Rita Fiasco (consulente, Vice Presidente Assinform); Donato A. Limone (professore di informatica giuridica, fondatore e direttore della “Rivista elettronica di diritto, economia, management”); Andrea Lisi (Avvocato, docente ed esperto di Diritto dell'Informatica; Presidente di Anorc Professioni); Valerio Maio (ordinario di diritto del lavoro, Università degli Studi di Roma, Unitelma Sapienza); Vincenzo Mongillo (ordinario di diritto penale, Università degli studi di Roma, Unitelma Sapienza); Mario Nobile (dirigente generale, responsabile della transizione digitale, Ministero delle infrastrutture e dei trasporti); Roberto Pasca di Magliano (Professore di Economia e gestione dell'Innovazione; Direttore School of Financial Cooperation and Development, Unitelma Sapienza); Gianni Penzo Doria (dirigente universitario di ruolo, direttore dell'Archivio di Stato di Venezia e dell'annessa Scuola di archivistica, paleografia e diplomatica); Pier Luigi Petrillo (ordinario di diritto pubblico comparato, Università degli studi di Roma, Unitelma Sapienza); Nadezhda Nicolaevna Pokrovskaja, docente universitario presso Herzen State Pedagogical University of Russia e Peter the Great Saint-Petersburg Polytechnic University; Francesco Riccobono (ordinario di teoria generale del diritto, Università Federico II, Napoli); Sergio Sciarelli (professore di economia aziendale, Università Federico II, Napoli); Marco Sepe (ordinario di diritto dell'economia, Università degli studi di Roma, Unitelma Sapienza).

Comitato di redazione: Alberto Bruni, Angelo Cappelli, Luca Caputo, Claudia Ciampi, Ersilia Crobe, Tiziana Croce, Wanda D'Avanzo, Sandro Di Minco, Paola Di Salvatore, Massimo Farina, Santo Gaetano, Paolo Galdieri, Salvatore Gallo, Fabio Garzia, Edoardo Limone, Emanuele Limone, Lucio Lussi, Marco Mancarella, Antonio Marrone, Alessio Mauro, Alberto Naticchioni, Cristina Evangelina Papadimitriou, Giulio Pascali, Gianpasquale Preite, Azzurra Rinaldi, Fabio Saponaro, Pasquale Sarnacchiaro, Sara Sergio, Franco Sciarretta.

Direzione e redazione: Via Riccardo Grazioli Lante, 15 – 00195 Roma - donato.limone@gmail.com

Gli articoli pubblicati nella rivista sono sottoposti ad una procedura di valutazione anonima. Gli articoli sottoposti alla rivista vanno spediti alla sede della redazione e saranno dati in lettura ai referees dei relativi settori scientifico disciplinari.

Anno XII, n. 3/2022 - Supplemento 1

ISSN 2039-4926

Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010

Editor ClioEdu

Roma - Lecce

Tutti i diritti riservati.

È consentita la riproduzione a fini didattici e non commerciali, a condizione che venga citata la fonte. La rivista è fruibile dal sito www.clioedu.it gratuitamente.

Codice etico: www.clioedu.it/rivistaelettronica#codice-etico

Procedure di referaggio: www.clioedu.it/rivistaelettronica#referaggio

Elenco dei numeri pubblicati: www.clioedu.it/rivistaelettronica

INDICE

Editoriale	
<i>Donato A. Limone</i>	2
Presentazione	
<i>Maria Novella Campagnoli - Massimo Farina</i>	3
Sulla ragione artificiale	
<i>Agata C. Amato Mangiameli</i>	8
Principi e tutela in tema di privacy	
<i>Gianluigi Ciacci</i>	13
Discriminazioni algoritmiche?	
<i>Gianmarco Gometz</i>	25
Big data, Little Certainties. La Società digitale tra opportunità di sviluppo e rischi di algocrazia	
<i>Guido Saraceni</i>	31
Ars distinguendi, discriminazione e macchine intelligenti	
<i>Angelo Costanzo</i>	41
Persona e rete: la garanzia dei diritti fondamentali nello spazio cibernetico	
<i>Claudia Cipolloni</i>	50
IA e privacy: l'approccio con il modello DAPPREMO e le prossime sfide	
<i>Nicola Fabiano</i>	73
La tutela del programma per elaboratore nell'amministrazione algoritmica	
<i>Alessia Palladino</i>	85
Dati personali e discriminazione da IA: l'esperienza del Garante.	
<i>Guido Scorza</i>	96

EDITORIALE

In questo numero pubblichiamo gli atti del convegno “*IA e nuove forme di discriminazione*”, 24 marzo 2022. L’iniziativa è stata organizzata da Maria Novella Campagnoli della Università di Roma “Tor Vergata” e da Massimo Farina dell’Università di Cagliari che hanno curato questa pubblicazione. Ringrazio i colleghi per il convegno e per la curatela di questo numero.

I temi trattati riguardano il rapporto tra ragione umana ed intelligenza artificiale, privacy e IA, discriminazione algoritmica, big data e democrazia, discriminazione e macchine intelligenti, spazio cibernetico e diritti fondamentali, rete e persona, amministrazione algoritmica, l’esperienza del Garante relativamente al tema del convegno. Rinvio alla presentazione del convegno a cura di Campagnoli e Farina. La lettura degli articoli è stimolante anche in considerazione della recente evoluzione della tecnologia e della regolamentazione in materia di IA. La parola chiave del convegno è “discriminazione” (nuove forme di discriminazione) e che attraversa tutti gli atti che pubblichiamo. Ringrazio tutti i relatori per il loro prezioso contributo scientifico.

Il Direttore della Rivista
Donato A. Limone

PRESENTAZIONE

Maria Novella Campagnoli¹

Massimo Farina²

Il 24 marzo 2022 si è svolto il convegno dedicato a “IA e nuove forme di discriminazione”. L’iniziativa – realizzata grazie al patrocinio dell’associazione ANDIG, del Laboratorio ICT4 Law&Forensics dell’Università di Cagliari e della Collana DirICTo – ha visto fra i relatori professori delle Università di Roma “Tor Vergata”, di Cagliari e di Teramo, giudici delle più alte magistrature e componenti dell’Autorità Garante per la Privacy.

La spinta propulsiva all’organizzazione di questo evento è scaturita dalla convinzione che – pur senza tacere il prodigioso e irrinunciabile aiuto fornito dalle ITC – sia oramai necessario iniziare a misurarsi con le possibili discriminazioni che (direttamente o indirettamente) vengono occasionate proprio dall’impiego delle nuove tecnologie e dal procedere, spesso tutt’altro che neutrale, degli algoritmi. Situazioni, che, non di rado, interessano soggetti particolarmente vulnerabili, talvolta, semplicemente riproponendo vecchi stilemi e inveterati *cliché*, talaltra, giungendo persino a perpetuare – anche all’interno di quel vasto oceano che è la rete – condotte denigratorie e comportamenti prevaricatori e violenti. La varietà dei temi trattati e la ricchezza degli approcci proposti dai diversi relatori hanno favorito il confronto su questioni di interesse emergente e su problematiche di frontiera.

I lavori, articolati in due distinte sessioni, hanno avuto avvio con l’ampia e raffinata prolusione di Agata C. Amato Mangiameli dedicata al rapporto fra ragione umana e Intelligenza Artificiale, nella quale – muovendo dal fondamentale distinguo fra intelligenza artificiale debole ed intelligenza artificiale forte – sono stati messi in luce accenti e risvolti dell’interazione, sempre più intensa e penetrante, fra l’uomo e la macchina.

La prima sessione è stata contraddistinta dall’avvicinarsi delle stimolanti relazioni di Gianluigi Ciacci, che ha prospettato un’interessante riflessione su *Principi e tutele in tema di privacy*; di Gianmarco Gometz, che ha prospettato una decisiva e provocatoria analisi della possibile *Discriminazione algoritmica*; e di Guido Saraceni, che, con il suo intervento dedicato a *Molti bit, poche garanzie. Appunti su Big Data e democrazia* ha offerto un acuto e lucido quadro dei possibili rischi sottesi all’attuale implementazione digitale.

¹ Ricercatrice presso il Dipartimento di Giurisprudenza dell’Università degli Studi di Roma “Tor Vergata”.

² Ricercatore presso il Dipartimento di Ingegneria elettrica ed elettronica dell’Università degli Studi di Roma “Tor Vergata”.

La seconda sessione è stata arricchita dagli interventi di Angelo Costanzo, che, con il suo importante contributo dedicato a *Ars distinguendi, discriminazione e macchine intelligenti*, ha messo in evidenza le implicazioni che l'IA può avere in fase di giudizio; di Claudia Cipolloni, che ha riflettuto su *Persona e Rete: la garanzia dei diritti fondamentali nello spazio cibernetico*, aprendo alla visione costituzionale; di Nicola Fabiano, che, con la relazione dal titolo IA e privacy: l'approccio con il modello DAP-PREMO e le prossime sfide, ha presentato un inedito e innovativo modello idoneo a trovare applicazione su larga scala; di Alessia Palladino, che si è incentrata su *La tutela del programma per elaboratore nell'amministrazione algoritmica*, presentando a una stimolante lettura; e di Guido Scorza, che, con la suggestiva relazione dal titolo *Dati personali e discriminazione da I.A.: l'esperienza del Garante* ha concluso il convegno, ha presentato dall'interno la fondamentale posizione dell'Autorità Garante.

Questo numero monografico della rivista *Rivista elettronica di Diritto, Economia, Management*, edito a curatela congiunta, raccoglie gli atti del convegno di cui ripropone l'ordine dei temi.

Autori di questo numero

Agata C. Amato Mangiameli

Professore Ordinario di «Filosofia del Diritto», «Informatica giuridica» e «Biogiuridica», presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma «Tor Vergata», dove insegna anche «Semiotica giuridica» e «Strategie digitali». Presso il medesimo Ateneo è membro della Giunta di Dipartimento, del Collegio dei docenti del Dottorato in Diritto Pubblico e del Consiglio scientifico del Centro di Studi Giuridici «Di-con-per Donne». Presiede la Commissione di valutazione per il conferimento dell'Abilitazione Scientifica Nazionale a professore di prima e di seconda fascia (IUS/20). Dirige le collane «Ius et Fas» e «Stelle Inquiete. Interventi e confronti» (edite da Giappichelli, Torino), ed è membro del Comitato di direzione e del Consiglio scientifico di numerose riviste italiane e straniere.

Maria Novella Campagnoli

Ricercatrice presso il Dipartimento di Giurisprudenza dell'Università di Roma «Tor Vergata», dove è membro della Giunta di Dipartimento e del Consiglio Scientifico del Centro di Studi Giuridici «Di-con-per Donne». Abilitata al ruolo di professore di seconda fascia. Insegna «Teoria e pratica dei diritti Umani» (Corso di Laurea SARI – Università di «Tor Vergata»), «Informatica giuridica» e «Elementi di Informatica giuridica» (SSPL – Università di Perugia). Condirettrice (con Massimo Farina) della Collana «Diritto Dell'Informatica e Delle Nuove Tecnologie».

Gianluigi Ciacci

Avvocato specializzato nel diritto delle nuove tecnologie, dottore di ricerca in «Informatica giuridica e Diritto dell'informatica» presso l'Università degli studi di Roma «La Sapienza», docente titolare degli insegnamenti di «Diritto digitale e tutela dei dati personali», «Macchine intelligenti e diritto» e «Diritto Civile della Società Digitale», presidente di ANDIG (Associazione Nazionale Docenti di Informatica Giuridica).

Claudia Cipolloni

Dottore di Ricerca in Diritto costituzionale presso L'Università degli Studi di Teramo (titolo della tesi: «L'evoluzione del moderno costituzionalismo alla prova della globalizzazione tecnologica. Stato e persona nella Rete del fenomeno digitale»). È stata assegnista di ricerca dell'Issirfa-CNR.

Angelo Costanzo

Consigliere della Corte di Cassazione. Ha svolto diversi ruoli nella magistratura giudicante anche con funzioni semi-direttive e direttive. Tiene corsi universitari di filosofia e teoria generale del diritto, insegna «Diritto penale e argomentazione giuridica» in Scuole di specializzazione nelle professioni legali partecipando ai loro consigli

direttivi. Opera nella formazione dei magistrati, come relatore dei corsi della Scuola Superiore della Magistratura, referente per la formazione decentrata e coordinatore dei tirocini presso gli Uffici giudiziari. È autore di diversi articoli e monografie sulla logica e l'argomentazione giuridica oltre che varie materie del diritto positivo. Abilitato al ruolo di professore di prima fascia. Tiene un corso su «Macchine intelligenti e diritto» presso la LUISS.

Nicola Fabiano

Avvocato cassazionista. Già Presidente dell'Autorità per la Protezione dei Dati Personali della Repubblica di San Marino ed esperto del Comitato Consultivo del Consiglio d'Europa della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale e del Comitato *ad hoc* sull'intelligenza artificiale. È presidente del «Centro per l'Informatica e l'Innovazione Forense» dell'Ordine degli Avvocati di Foggia. Componente del «IEEE SA P7007 Ontological Standard for Ethically Driven Robotics and Automation Systems Working Group» e chair del sottogruppo «Data Privacy and Protection»; Componente del Program Committee della conferenza internazionale «The 13th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC 2022©» (Florida, USA).

Massimo Farina

Ricercatore presso il DIEE dell'Università degli Studi di Cagliari, dove è membro della Commissione Spin-off di Dipartimento, Responsabile del Laboratorio Universitario «ICT4Law&Forensics» e Data Protection Officer dell'Ateneo. Abilitato al ruolo di professore di seconda fascia. Insegna «Informatca giuridica», «Informatca forense» e «Computer Law» (Corsi di Laurea Magistrale in «Ingegneria delle Tecnologie per Internet» e in «Computer Engineering, Cybersecurity and Artificial intelligence» - Università di Cagliari) e «teoria e tecnica dell'argomentazione e informatica giuridica» (SSPL – Università di Cagliari). Condirettore (con Maria Novella Campagnoli) della Collana «Diritto Dell'Informatca e Delle Nuove Tecnologie» e fondatore del Network «DirICTo».

Gianmarco Gometz

Professore ordinario di «Filosofia del diritto» e «Informatica giuridica» presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Cagliari. Presso il medesimo ateneo è membro del Collegio dei docenti del Dottorato in Scienze Giuridiche e membro del Collegio dei docenti del Master di II livello «La Governance Multi-livello. La gestione integrata delle politiche pubbliche». Partecipa al Comitato di direzione e al Consiglio scientifico di numerose riviste italiane e straniere. Ha diretto svariati corsi di formazione e perfezionamento su temi di informatica giuridica e amministrazione digitale.

Alessia Palladino

Dottore di ricerca in «Humanities and technologies: an integrated research path» presso l'Università degli Studi Suor Orsola Benincasa. Master of studies e ELGS Young Researcher presso l'European Public Law Organization (EPLO) di Atene

Guido Saraceni

Professore Associato di «Filosofia del diritto» e di «Informatica giuridica» presso la Facoltà di Giurisprudenza dell'Università degli Studi di Teramo. Abilitato al ruolo di professore di prima fascia. Nel medesimo Ateneo, è stato: Presidente del Corso di Laurea Magistrale in Giurisprudenza; delegato del Rettore per il «Diritto allo Studio, l'Assistenza e l'Integrazione degli Studenti Diversamente Abili»; Vicedirettore della Scuola di Specializzazione in «Diritto Amministrativo e Scienza dell'Amministrazione»; Coordinatore del Master in «Sicurezza Informatica» e del Corso di Specializzazione su «Valore Giuridico e Tutela del Documento Informatico». Attualmente, è membro del Collegio del Dottorato in «Processi di Armonizzazione del Diritto tra Storia e Sistema». Fa parte del Comitato Consultivo del Centro Studi Giuridici «Di-con-per Donne» dell'Università di Roma «Tor Vergata». È membro del Comitato di direzione e del Consiglio scientifico di numerose riviste italiane e straniere.

Guido Scorza

Avvocato, giornalista pubblicista, professore a contratto di diritto delle nuove tecnologie. Già responsabile degli affari regolamentari del team per la trasformazione digitale della Presidenza del Consiglio dei Ministri e, poi, Consigliere giuridico del Ministro per l'innovazione. Insegna «Diritto delle nuove tecnologie» presso l'Università europea, «Diritto dei contratti ad oggetto informatico» presso il Master in «Informatica giuridica e diritto dell'informatica» dell'Università degli Studi di Bologna e «Privacy nelle comunicazioni elettroniche» presso il Master in protezione dei dati personali dell'Università Roma Tre.

Ha fondato lo Studio «Elex». È rappresentante vicario del Governo italiano presso il «Government advisory Board» dell'ICANN.

INTELLIGENZA ARTIFICIALE

ARTIFICIAL INTELLIGENCE

Agata C. Amato Mangiameli¹

Abstract [IT]: Muovendo dalla differenza fra intelligenza artificiale debole e forte, il saggio ricostruisce e ripercorre l'evoluzione degli studi di settore, sino a interrogarsi criticamente sull'influenza che l'intelligenza artificiale ha via via acquisito in quasi tutti gli ambiti dell'esistenza, giungendo anche a condizionare molte scelte umane.

Abstract [EN]: Starting from the difference between weak and strong artificial intelligence, the essay traces the evolution of sector studies, up to critically questioning the influence that artificial intelligence has gradually acquired in almost all areas of existence, even reaching to condition many human choices.

Keywords [IT]: IA – dati – algoritmi – comportamenti e scelte umane.

Keywords [EN]: AI – data – algorithms – human behavior and choices.

Sommario: 1. Scena prima: la stanza cinese. – 2. Scena seconda: la stanza di Google. – 3. Epilogo: la stanza (valle) del perturbante.

1. Scena prima: la stanza cinese

In una stanza è rinchiusa una persona di madrelingua inglese, che non conosce affatto il cinese e che ha a disposizione due fogli: nel primo di essi sono rappresentati degli ideogrammi cinesi, nel secondo, invece, c'è un elenco di domande sempre in cinese. Nella stessa stanza si ritrova anche un libro, scritto questa volta in inglese, che spiega le regole da seguire per abbinare i simboli del primo foglio con quelli del secondo. Ora, seppure non comprenda il cinese, seguendo alla lettera le istruzioni, il protagonista dell'esperimento potrà riuscire a produrre risposte formalmente corrette, tanto da indurre un eventuale osservatore esterno di madrelingua cinese ad avere una falsa rappresentazione della realtà e a ritenere che il soggetto in questione abbia una buona padronanza della sua lingua.

Com'è noto, si tratta dell'esperimento che John Searle propose in *Minds, brains and programs*², per spiegare la differenza che passa tra le due concezioni dell'Intelli-

¹ Ordinario di Filosofia del diritto, Biogiuridica e Informatica giuridica presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma "Tor Vergata".

² Searle J.R., *Menti, cervelli e programmi*, trad. it. in, D. Hofstadter, D. Dennett (a cura di), *L'io della mente*, trad. it., Adelphi, Milano, 1985, pp. 341-360.

genza artificiale: quella debole, prospettata da coloro che nell'IA vedono un mero strumento (potente, ma nulla di più) in grado di verificare e di formulare le ipotesi in modo esatto e coerente; quella forte, avanzata dai fautori dell'IA quale calcolatore che, se programmato opportunamente, sarebbe in grado di simulare in tutto e per tutto il funzionamento della mente umana e perciò assai diversa da un semplice strumento. Come è chiaro, l'immagine dell'uomo che meccanicamente produce output di risposte, in base alle istruzioni rinvenute in un libro e senza comprendere il cinese, a suo modo, rappresenta una metafora del calcolatore che, nell'eseguire il programma secondo il linguaggio di programmazione (la sua madrelingua), non fa altro che manipolare simboli dei quali in realtà ignora completamente il significato, ragion per cui il suo operare è meramente sintattico. Non a caso, secondo Searle, l'IA – fondamentalmente diversa da quegli aspetti che sono propri solo della mente e che sono legati alla comprensione di ciò che abbiamo intorno (livello semantico) – ha a che fare con i simboli, anziché con i significati, che restano di appannaggio esclusivo dell'uomo, e il suo scopo è quello di manipolare correttamente le forme ignorandone (e nonostante) i (loro) contenuti.

Al di là delle differenze tra le due possibili concezioni (quella debole o quella forte), l'espressione IA – usata per la prima volta dal matematico John McCarthy³ in occasione di un convegno volto a definire i termini di una nuova disciplina con oggetto la simulazione e la riproduzione di alcuni processi del cervello umano – risponde all'esigenza tipicamente umana di superare le tante difficoltà che si presentano nel quotidiano e le molteplici mancanze della nostra condizione, realizzando sistemi in grado di espletare con successo e con notevole rapidità alcune funzioni complesse umane. Si pensi, ad esempio, alla traduzione automatica dei testi: l'azione del software non può certo essere equiparata all'atto propriamente umano del comprendere, che, in quanto tale, richiederebbe coscienza e intenzionalità, oltre a un autentico approfondimento della realtà esterna e un'intensa capacità di discernimento tra le varie e possibili circostanze concrete. Ed è entro questa cornice che, tra le principali applicazioni dell'IA, possono segnalarsi: 1) la rappresentazione della conoscenza (con le sue due più importanti metodologie: linguaggi formali e alberi di decisione); 2) l'apprendimento automatico, grazie a sistemi che si basano su osservazioni o su esempi come dati per la sintesi di una nuova conoscenza e che sono da distinguere in apprendimento non supervisionato (algoritmi: clustering, regole di associazione), supervisionato (algoritmi: albero di decisione, regole di decisione, apprendimento bayesiano, sistemi esperti), per rinforzo (algoritmi: reti neurali, algoritmi genetici, sistemi a classificatori); 3) la programmazione logica induttiva, ossia l'apprendimento automatico con l'uso della programmazione logica come linguaggio di rappresentazione di esempi e concetti; 4) l'elaborazione del linguaggio naturale, suddivisa in analisi lessicale, grammaticale, sintattica, semantica; 5) il c.d. visual retrieval, sistemi (con differenti modalità: semantica, formale, strutturale, coloristica, parametrica) per

³ McCarthy J., Minsky M.L., Rochester N., Shannon C.E., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, August 31, 1955, in *AI Magazine*, 26, 4/2006.

indicizzare, archiviare, ricercare, documenti visivi digitali; 6) la visione artificiale, l'insieme dei processi che permettono di acquisire, registrare ed elaborare immagini, per varie finalità (classificazione, controllo, selezione, ecc.); 7) la tecnica di risoluzione di problemi di pianificazione, allocazione delle risorse, e così via.

2. Scena seconda: la stanza di Google

Qui si avvicinano figure professionali specializzate nella progettazione di software, il cui impegno è quello di superare via via i limiti dell'IA. Deep Blue (1997) calcola statisticamente la mossa migliore e vince a scacchi, ma resta pur sempre un calcolatore. Watson (2011) comprende il linguaggio umano e dà risposte esatte, ma resta pur sempre un elaboratore. Rispetto al primo, c'è tuttavia qualcosa in più: il programma utilizza le c.d. reti neurali che, analogamente a quelle biologiche che sono in grado di comprendere l'ambiente e i suoi mutamenti, si prestano ad essere usate in tutti quei settori in cui sono richiesti data mining, elaborazione di modelli predittivi e simulativi, oppure classificazioni. Ed è proprio sulle reti neurali che AlphaGo (2015) si sviluppa e sconfigge il maestro di un gioco, qual è il go, sino a quel momento fuori dalla portata delle tecniche di apprendimento automatico, e che richiede al contempo le doti umane della disciplina, della concentrazione e dell'equilibrio. E tra le tante versioni di AlphaGo, nella stanza di Google, lì dove tutto è accelerato e il tempo per adattarsi è decisamente esiguo, si processano senza sosta e senza particolare dispendio di tempo e di energie grandi moli di dati. Nel frattempo, l'IA inizia ad imparare 'da sola', apprende dai suoi stessi errori e opera in modo corretto nonostante input imprecisi o incompleti, si auto-aggiorna in presenza di modifiche ambientali e sembra possedere persino una sorta di intuito non molto diverso da quello degli uomini.

Che si tratti di una vera e propria IA o meno, resta il fatto che ogniqualvolta qualcuno di noi utilizza un'app, visita un sito, fa una ricerca, scambia messaggi, vede un video, tutto viene caricato sui server e i dati raccolti vanno ad allenare l'IA, la quale via via conosce sempre di più ed è in grado di proporre e indirizzare a delle scelte migliori e più efficienti grazie alla gestione delle interrogazioni (query) espresse dall'utente tutte le volte che questi digita il suo quesito, ad esempio, sulla barra di ricerca di Google. Com'è intuitivo, l'IA diventa così del tutto imperscrutabile. Se fino a non molto tempo fa, sarebbe stato possibile ripensare all'algoritmo a fondamento di una certa gerarchia, ben difficilmente adesso è ipotizzabile risalire ai miliardi di interrogazioni sempre più personalizzate che di fatto determinano delle vere gerarchie e consentono la crescita esponenziale dell'IA.

Non è l'IA (delle concezioni: debole o forte), l'IA specializzata (Artificial Narrow Intelligence) o l'IA ampliata (Artificial General Intelligence) e anche super (Artificial

Super Intelligence), a destare delle serie perplessità. Del resto, già Turing⁴ nel saggio *Computing machinery and intelligence* ha risposto agli interrogativi del tipo: cosa vuol dire pensare e cosa avviene quando si pensa? Cosa distingue un'attività consapevole, cosciente, da una stessa operazione compiuta in modo automatico? Cosa distingue il gioco tra umani e il gioco anche con umani dei diversi programmi? La macchina universale, equivalente logico di una macchina a stati finiti, è equiparabile al cervello e può dunque essere programmata in modo da imitare il funzionamento cerebrale? A sollevare invece alcuni significativi dubbi sono piuttosto le ricadute di una IA di così vasta e profonda portata che abbia la capacità di estrapolare da una enorme quantità di dati (big data) ogni singola informazione per analizzare, elaborare, suggerire e orientare modelli di interpretazione e di azione, in ogni settore (privato e/o pubblico). In particolare, sono le ricadute di una IA che abbia il potere di dire con precisione e in tempo reale lo stato teoricamente esatto delle cose e di qui il potere di esercitare il controllo e di orientare l'azione umana.

3. Epilogo: la stanza (valle) del perturbante

Nello scambio continuo tra umani e sistemi, l'IA è diventata una formidabile compagna di gioco, uno sterminato scaffale della conoscenza e della competenza, un magnifico supporto organizzativo delle situazioni umane. È presentata come il doppiogiochista artificiale dell'uomo. Non importa quale sia la sua forma, poiché le macchine possono essere di vario tipo e di diversa struttura, qualche volta si tratta di robot estranei e opposti all'uomo, nelle loro forme irte, metalliche, sferraglianti, talaltra invece si tratta di robot vicini e somiglianti all'uomo, nelle loro forme morbide, sinuose, espressive (Sophia), qualche altra volta ancora di macchine del corpo-mente, ovvero di macchine mentali che vivono e si sviluppano nell'interazione con l'ambiente e che rispondono in modo adattivo ed evolutivo alle sollecitazioni esterne tramite l'interfaccia omeostatica del corpo. Quel che invece importa è, per un verso, il nostro atteggiamento rispetto all'IA: non di rado si conversa con i programmi come se si trattasse di persone, cui confidare – come notava già Weizenbaum⁵ – i segreti più intimi. Per un altro verso, l'affermarsi di una tecno-ideologia della perfezione che determina un affidarsi pressoché totale alle intelligenze artificiali, visto che i sistemi hanno la capacità di auto-apprendere: nel caso ad esempio dell'apprendimento non supervisionato, è a partire da un insieme di variabili di input che la rete crea dei cluster rappresentativi per categorizzarle, e nell'ipotesi dell'apprendimento per rinforzo, è dall'interazione con l'ambiente che i circuiti neurali imparano ed eseguono

⁴ Turing A., *Computing machinery and intelligence*, in *Mind*, 59, 1950, pp. 433-460. Turing A., *Intelligenza meccanica*, trad. it., Bollati Boringhieri, Torino, 1994.

⁵ Weizenbaum J., *Il potere del computer e la ragione umana. I limiti dell'intelligenza artificiale*, trad. it., Edizioni Gruppo Abele, Torino, 1987.

una serie di azioni, delle quali quelle che si avvicinano al risultato sono considerate di rinforzo, mentre le altre sono eliminate perché foriere di errore.

L'IA ha ormai il potere di dire e il punto è che oggi il suo dire rappresenta la verità. Si pensi all'uso sempre più diffuso di software che simulano ed elaborano le conversazioni umane, così che l'utente interagisce con un dispositivo come se stesse comunicando con una persona reale. Sono detti chatbot, e possono essere anche particolarmente sofisticati, come appunto gli 'agenti conversazionali', progettati per fornire livelli crescenti di personalizzazione, informandoci e guidandoci. Sono in ogni caso ovunque e sono sempre più preziosi, nei nostri ambienti abituali e con i nostri consueti dispositivi (computer, smartphone, ecc.). Altrimenti detto, gli assistenti digitali diventano i nostri più premurosi interlocutori, si rivolgono a noi con competenza e dispensano buoni consigli, e le loro parole via via conquistano un'aura e un'autorità tali da essere percepite come naturali e da essere prese – riprendendo l'espressione di Sadin⁶ – per 'oro colato'.

Com'è intuitivo, se il dialogo dovesse avvenire (e avviene) con una macchina le cui fattezze ci sono familiari – l'automa antropomorfo è somigliante all'essere umano, in particolare l'IA Sophia si comporta in modo realistico e riproduce molte espressioni facciali umane –, allora quelle stesse parole possono generare molteplici e contrastanti sensazioni. Qualche volta è l'empatia, la percezione di familiarità e con essa la risposta emotiva positiva, talaltra è invece il senso di repulsione e di inquietudine che può contraddistinguere il rapporto fra l'umano e l'umanoide. Dalla simpatia all'avversione, dal momento che – secondo il modello matematico di Mori⁷ – la ricerca del realismo a tutti i costi si rivela controproducente e con l'eccessiva somiglianza degli artefatti robotici si apre una condizione di familiarità negativa e si rischia una caduta in una sorta di valle del perturbante (uncanny valley).

⁶ E. Sadin, *Critica della ragione artificiale. Una difesa dell'umanità*, trad. it., Luiss University Press, Roma, 2019.

⁷ Mori M., *Bukimi no tani – The uncanny valley* (K. F. MacDorman & T. Minato, Trans.), in *Energy*, 7(4)/1970, pp. 33-35.

I.A. PRINCIPI E TUTELE IN MATERIA DI PRIVACY

Gianluigi Ciacci¹

Abstract [IT]: Lo sviluppo repentino ed esponenziale dei sistemi di Intelligenza Artificiale, e della correlata attenzione “diffusa” per la stessa, conseguenza anche del moltiplicarsi delle sue applicazioni nella quotidianità degli utenti (si pensi ad esempio agli assistenti virtuali nei cellulari o in *device* casalinghi), ha fatto nascere un dibattito sulla necessità di trovare un equilibrio fra due opposte esigenze: non rallentare, o addirittura bloccare, il progresso del settore, e quindi le conseguenze positive dello stesso; impedire che tale progresso avvenga in danno dei suoi utenti. Dicotomia che raggiunge una forte criticità, da una parte, nel momento in cui dal suo sviluppo dipendono enormi interessi economici e, dall'altra, quando il danno agli utenti riguarda i loro dati personali: in questo secondo caso soprattutto a causa della presenza di una normativa forte, rappresentata dal Regolamento UE 2016/679, finalizzata proprio a prevenire, o comunque limitare, tale danno. La pregnante disciplina in materia di protezione dei dati personali, infatti, prevede una serie di principi e disposizioni di difficile, se non impossibile, applicazione ai sistemi di Intelligenza Artificiale: si pensi, ad esempio, alla necessità di rispettare la minimizzazione e trasparenza nel trattamento dei dati personali (art. 5, par. 1, del Regolamento), rispetto ad una realtà tecnologica che in generale ha la necessità di essere alimentata da ingenti quantità di informazioni (i c.d. *big data*) per ottenere migliori risultati, e le cui modalità di funzionamento, nonché gli stessi risultati dei processi elaborativi basati sull'I.A., sono, e spesso devono essere, “oscuri”. Per risolvere l'indicata dicotomia la scelta non riguarda solo il tema contingente, ma quello più ampio relativo al rispetto o meno della legalità anche nel mondo digitale.

Abstract [EN]: The sudden and exponential development of Artificial Intelligence systems, and the related “widespread” attention for the same, also a consequence of the multiplication of its applications in the everyday life of users (think, for example, of virtual assistants in cell phones or in home devices), has given rise to a debate on the need to strike a balance between two opposing needs: not to slow down, or even block, the progress of the sector, and thus the positive consequences of the same; to prevent that this progress occurs to the detriment of its users. A dichotomy that reaches a strong criticality, on the one hand, when enormous economic interests depend on its development and, on the other hand, when the harm to users concerns their personal data: in the latter case mainly due to the presence of strong

¹ Docente presso l'Università LUISS Guido Carli.

legislation, represented by EU Regulation 2016/679, aimed precisely at preventing, or at least limiting, such harm. The pregnant data protection regulations, in fact, provide for a series of principles and provisions that are difficult, if not impossible, to apply to Artificial Intelligence systems: one thinks, for example, of the need to respect minimization and transparency in the processing of personal data (Art. 5(1) of the Regulation), with respect to a technological reality that in general needs to be fed by huge amounts of information (so-called big data) in order to achieve better results, and whose modes of operation, as well as the very results of the processing processes based on A.I, are, and often must be, “obscure.” In order to resolve the indicated dichotomy, the choice is not only about the contingent issue, but the broader one related to whether or not legality is also respected in the digital world.

Keywords [IT]: privacy – big data – intelligenza artificiale – legalità – cultura.

Keywords [EN]: privacy - big data - artificial intelligence - legality - culture.

Sommario: 1. Introduzione. – 2. I c.d. Big Data e l’Intelligenza Artificiale. – 3. Big Data, Intelligenza Artificiale e protezione dei dati personali. – 4. Gli aspetti della disciplina in materia di protezione dei dati personali di rilievo per le attività di trattamento collegate all’I.A. – 5. Big Data, Intelligenza Artificiale e protezione dei dati personali: problemi e possibili soluzioni

1. Introduzione

Nell’evoluzione degli studi sull’Informatica Giuridica di frequente l’attenzione degli esperti della materia è stata catalizzata dall’avvento di fenomeni tecnologici che hanno sollevato rilevanti, e interessanti, problemi giuridici: dalla nascita dei contratti informatici negli anni ottanta, alla tutela dei programmi per elaboratore ed al valore giuridico del documento elettronico/firma digitale degli anni Novanta; successivamente l’avvento della rete Internet, dei social network, e poi la tecnologia blockchain, la moneta elettronica, gli smart contracts, ed infine proprio l’Intelligenza Artificiale.

Quest’ultima, non potendomi dilungare nel riportare le varie definizioni, e nel dettagliare i suoi contenuti (che verranno sicuramente trattati dagli altri relatori), certamente è un fenomeno di rilevante, e crescente, interesse, in repentino sviluppo e con importanti, e complesse, implicazioni giuridiche: che quindi, nell’attirare l’attenzione degli studiosi di informatica giuridica, e non solo (l’attualità del tema infatti coinvolge sempre più anche la dottrina “tradizionale”: aspetto molto utile nell’ottica della ormai improrogabile necessità di aumentare la diffusione della cultura sulle nuove tecnologie anche nel mondo del diritto), la sta portando ad essere anche di grande ... “moda”.

A parte però gli elementi positivi del “successo” dell’Intelligenza Artificiale, si deve rilevare un rischio in tale situazione? Probabilmente sì, quello rappresentato dalla concreta possibilità di distrarsi con aspetti secondari del fenomeno (si pensi ad

esempio al tema della guida autonoma, e della connessa responsabilità: sicuramente molto interessante e importante, ma per lungo tempo è sembrato rappresentare il solo, o comunque principale, problema giuridico da approfondire e risolvere). Un “successo” che spesso “condiziona” anche chi se ne occupa professionalmente e/o a livello istituzionale: si possono fare a tale proposito due esempi.

Con riferimento al primo, riporto un passaggio di una interessante monografia pubblicata un paio di anni fa, che abbiamo presentato in LUISS il 27 ottobre 2020 (A. Longo – G. Scorza, *L’impatto sulle nostre vite, diritti e libertà*, Mondadori Università, 2021, pp. XII-244). Gli autori, nel descrivere ed introdurre il tema dell’intelligenza artificiale, riportano l’evoluzione storica del suo sviluppo, con l’indicazione delle principali date che hanno caratterizzato i passaggi più rilevanti di tale evoluzione; l’aspetto curioso è rappresentato dall’idea di associare agli episodi “reali” quelli collegati a produzioni letterarie o cinematografiche realizzate più o meno negli stessi periodi: quasi a dimostrare la stretta correlazione, in questo settore, tra realtà tecnologica e divulgazione. Nella tabella che segue riporto alcuni esempi tratti dal volume (pp. 9-31):

1939 Atanasoff-Berry Computer (ABC)	1942 Asimov, le 3 leggi della robotica
1950 test di Turing	
1959 machine learning	
1966 Shakey the Robot	1968 “2001 Odissea nello spazio”
1970 WABOT 1	1977 “Star Wars”
1995 chatbot Alice	1984 “Electric Dreams”
1997 Deep Blue	2001 “AI - Artificial Intelligence”
2000 ASIMO	2004 “Io, robot”
2011 Watson	2013 “Her (Lei)”

Ma la commissione che sto cercando di evidenziare, non ultimo allo scopo di sottolineare la necessità di non farsi distrarre dagli aspetti “di moda” dell’importante tema, più divulgativi che scientifici, non si limita ad interventi non istituzionali o della dottrina (non solo accademica, ma anche nella stampa d’opinione). Il secondo esempio riguarda infatti una fonte ufficiale, la *“Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica”*, che nel punto A dell’introduzione riporta

“A. considerando che, dal mostro di Frankenstein ideato da Mary Shelley al mito classico di Pigmalione, passando per la storia del Golem di Praga e il robot di Karel C apek, che ha coniato la parola, gli esseri umani hanno fantasticato sulla possibilità di costruire macchine intelligenti, spesso androidi con caratteristiche umane”.

Testo che permette di capire come il rischio della prevalenza dell’Intelligenza Artificiale “divulgativa” (mostri, Golem, robot, ...) possa portare a trascurare la necessità

di un serio approfondimento giuridico delle varie ed ulteriori (rispetto alla responsabilità da guida autonoma) problematiche.

Volendo però vedere il “bicchiere mezzo pieno”, non si deve ignorare, a causa del rischio evidenziato, l’opportunità creata dal forte interesse per questa realtà, rappresentata dalla nuova domanda di conoscenza legata alla necessità di comprendere l’I.A.: che porta al moltiplicarsi di eventi, di pubblicazioni non solo divulgative, ma anche tecniche, e con riferimento anche ai diversi campi applicativi (prospettiva degli ultimi mesi, che sempre più hanno portato ad un approfondimento più “maturo” dei problemi giuridici dell’intelligenza artificiale). Domanda di conoscenza che assume una grande importanza, soprattutto nel nostro Paese, dove la carenza di competenze nelle nuove tecnologie ha sempre rappresentato uno dei suoi grandi problemi, ancor di più se si pensa alla mancata percezione della necessità di un approccio culturale alle stesse. Carenza oggi sempre più grave.

Così, lo sviluppo di un’attenzione “diffusa” per l’I.A., conseguenza anche del moltiplicarsi delle sue applicazioni nella quotidianità degli utenti (si pensi ad esempio agli assistenti virtuali nei cellulari o in *device* casalinghi), oltre a portarla al di fuori della discussione tra esperti, ha fatto nascere un dibattito sulla necessità di trovare un equilibrio fra due opposte esigenze:

- non rallentare, o addirittura bloccare, il progresso del settore, e quindi le conseguenze positive dello stesso (e poi sì, anche l’enorme business da essa resa possibile direttamente, per il valore in sé dell’I.A., e indirettamente, per la ricchezza prodotta dalle sue applicazioni);
- impedire che tale progresso avvenga in danno dei suoi utenti.

Dicotomia che raggiunge una forte criticità, da una parte, nel momento in cui dal suo sviluppo dipendono enormi interessi economici (“alzando la posta in gioco”), e, dall’altra, quando il danno agli utenti riguarda i loro dati personali: in questo secondo caso soprattutto a causa della presenza di una normativa forte, rappresentata dal Regolamento UE 2016/679, finalizzata proprio a prevenire, o comunque limitare, tale danno.

Prima di affrontare il fondamento dell’indicata dicotomia, e di provare a cercare le possibili soluzioni, occorre in premessa analizzare una realtà strettamente legata a quella dell’intelligenza artificiale, il fenomeno dei c.d. “*big data*”.

2. I c.d. Big Data e l’Intelligenza Artificiale

Quando ci si occupa delle nuove tecnologie, e non solo, è oramai costante il richiamo alla c.d. “società dell’informazione”, e all’importanza fondamentale acquisita dai dati (“il nuovo petrolio”).

L’informazione è infatti diventata il motore dell’economia, e l’evoluzione negli anni delle tecnologie dell’informazione e della comunicazione ha portato ad una sua trasformazione in “informazione automatica”, e quindi “informatica”.

L'ulteriore evoluzione degli ultimi anni ha portato un cambiamento nelle modalità di creazione, acquisizione, gestione, comunicazione, ..., delle informazioni. La tecnologia ha infatti modificato il Volume, la Velocità, la Varietà, (la Veridicità), il Valore economico dei dati (le famose "V") e la possibilità di loro utilizzo, analisi e sviluppo, in una realtà di autoalimentazione che genera quotidianamente miliardi di informazioni. Realizzando la realtà dei c.d. "Big Data" che vengono definiti (punto A dei considerando della *"Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto"*) come le *"ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento dei dati, che usano sia informazioni memorizzate sia in streaming, al fine di individuare"*.

Non potendo approfondire in queste poche pagine la realtà dei Big Data, ci basti richiamare il fatto che essi si pongono in stretta correlazione con l'Intelligenza Artificiale: da un lato, ne "alimentano" l'apprendimento (ad esempio nei sistemi di *machine learning*), mentre dall'altro rappresentano il risultato dell'applicazione dei relativi algoritmi.

Se questo è il contesto, se i dati hanno assunto questa importanza, allora è diventato fondamentale proteggere il loro valore, insieme alla necessità sempre più sentita di sviluppare l'Intelligenza Artificiale. Ma se poi i dati di cui si parla sono ... "personali", cioè sono riferiti (o riferibili, anche indirettamente) ad individui, non basta più proteggere il loro *valore*, e allo stesso tempo non si può pensare solo a diffondere l'utilizzo dell'I.A., sostenendo il relativo settore economico; diventa invece prioritariamente necessario tutelare *i soggetti* a cui si riferiscono i dati oggetto di questa nuova tecnologia, la loro dignità e libertà individuale. Necessità di tutela per raggiungere la quale è nata la normativa europea a protezione dei dati personali, rappresentata da ultimo (dopo la Direttiva 95/45/CEE degli anni Novanta) proprio dal Regolamento UE 2016/679.

3. Big Data, Intelligenza Artificiale e protezione dei dati personali

Nell'affrontare il tema della "privacy", più correttamente della protezione dei dati personali, soprattutto con riferimento al nostro Paese, si entra in contatto con un'anomalia "paradigmatica": principalmente creata dall'idea generalizzata che vede la relativa disciplina come assolutamente inutile, burocratica, anzi, addirittura dannosa per chi vuole oggi fare impresa ("se c'è la privacy non si può fare niente"), qualcosa da cui difendersi. Conseguenza di tale anomalia è stata la forte carenza negli anni di una generalizzata "cultura" della protezione dei dati personali, la disattenzione

politica al problema, lo scarso livello di adeguamento alla legge delle strutture dei vari titolari, privati ed anche pubblici.

Come detto, la situazione è migliorata con l'avvento nel maggio del 2018 del Regolamento 2016/679, il c.d. G.D.P.R.: di cui tutti parlano, molti si attivano per poterlo rispettare, ma alla fine non così tanti riescono ad approfondirne i diversi aspetti per arrivare a conoscerlo.

Ad ogni modo, l'ingente importo delle sanzioni, l'introduzione di un sistema basato sulla responsabilizzazione del titolare (c.d. *accountability*), una serie di scelte... "strategiche" nella costruzione della disciplina normativa (ad esempio, l'introduzione della figura e del ruolo del Responsabile per la Protezione dei Dati Personali, comunemente DPO, dell'obbligo di tenuta di un Registro dei trattamenti come momento di "autoconsapevolezza" del titolare, l'obbligo di denuncia dei c.d. *data breach*, l'introduzione del principio di *accountability* alla base del nuovo approccio sistematico della disciplina,...), hanno trasformato il fallimento del sistema di tutela degli anni '90, avente fonte nella Direttiva 95/45/CEE, in un successo. Questo principalmente per la natura "sostanzialista" Regolamento UE 2016/679, il cui sistema di tutela non si risolve solo nel rispetto formale degli obblighi, come in quello precedente, ma nella costruzione di un'effettiva, ed efficace, protezione delle informazioni personali degli individui: si è passati cioè da una logica "di adempimento" (il mero rispetto di obblighi precostituiti ed uguali per tutti, semplicemente rispettati dai titolari del trattamento, senza curarsi del risultato dell'adeguamento al loro disposto) a quella di sistema (dove prevale l'efficacia del sistema, basato come detto sulla responsabilizzazione, sull'*accountability* dei titolari).

Ancora, il cambiamento ha riguardato proprio l'oggetto della disciplina, la sua finalità: in particolare

- prima (Direttiva 95/46/CE) si voleva assicurare la protezione dei dati personali e la loro libera circolazione;
- ora il Regolamento 2016/679 inquadra invece la protezione dei dati personali quale diritto fondamentale e inviolabile della persona, ritiene prioritario rafforzare la fiducia degli interessati sulla tutela forte delle informazioni, stabilendo un quadro normativo adeguato allo sviluppo dell'economia digitale.

Cambiamento di impostazione che riporta centrale proprio l'importanza della tutela delle informazioni relative agli individui, come già previsto in due fonti di primaria importanza per l'Europa: fonti costantemente richiamate nell'affrontare il tema della protezione dei dati personali, ma che poi devono effettivamente essere tenute presenti nell'analizzare, valutare e disciplinare le attività sulle informazioni relative agli individui, e quindi anche i nuovi fenomeni tecnologici.

La prima è la Carta dei diritti fondamentali della UE, il cui art. 7 (intitolato "*Rispetto della vita privata e della vita familiare*"), testualmente dispone

- "*ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*"

mentre l'art. 8 (intitolato proprio "*Protezione dei dati di carattere personale*"), sancisce

-
- “1. ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano; 2. tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica; 3. il rispetto di tali regole è soggetto al controllo di un'autorità indipendente”

La seconda fonte è il Trattato sul funzionamento della UE, il cui art. 16 prevede al par. 1 che

- “Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano”,

e al par. 2

- “Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti”.

4. Gli aspetti della disciplina in materia di protezione dei dati personali di rilievo per le attività di trattamento collegate all'I.A.

Ma tornando al Regolamento 2016/679, ricordiamo velocemente il suo oggetto (“... protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali”, art. 1, par. 2), e procediamo a schematizzare alcuni suoi aspetti che hanno un diretto rilievo per la tutela dei dati personali coinvolti in processi di Intelligenza Artificiale. In particolare, occorre ricordare:

- l'ambito di applicazione territoriale del Regolamento, che aggiunge alla regola generale dello stabilimento (art. 3, par. 1: la normativa sulla protezione dei dati si applica a chi è stabilito nello Spazio Economico Europeo), quella innovativa del c.d. “target” (art. 3, par. 2: ovunque sia stabilito il titolare del trattamento, se utilizza dati di interessati che si trovano nell'Unione, in presenza di due condizioni previste dalla norma, dovrà applicare il Regolamento), che estende la sua applicabilità anche a sistemi di I.A. non utilizzati in Europa, o comunque riconducibili a titolari extra europei;
- i principi generali del trattamento, e nella specie quelli di liceità/correttezza/trasparenza (art. 5 par. 1, lett. *a*), limitazione della finalità (par. 1, lett. *b*), minimizzazione (par. 1, lett. *c*), limitazione conservazione (par. 1, lett. *e*); e poi, in generale, quello di *accountability* (art. 5, par. 2) e quelli dell'art. 25 (*protection data by*

-
- design e by default*);
- l'individuazione delle c.d. basi giuridiche del trattamento, necessaria per "giustificare" l'utilizzo dei dati personali, in applicazione degli artt. 6 (per i dati personali "comuni") e 9 (per i dati personali "particolari");
 - infine, tra gli obblighi che il titolare del trattamento deve osservare quando utilizza sistemi di Intelligenza Artificiale, a maggior ragione se operanti con "*big data*", ricordiamo, oltre a quello del punto precedente, quello di informativa (artt. 13 e 14 del Regolamento) e quello di rendere possibile, effettivo ed agevole, l'esercizio dei diritti riconosciuti all'interessato, cioè del soggetto a cui i dati trattati si riferiscono.

A parte gli indicati elementi della disciplina del Regolamento UE 2016/679 da tenere presenti nell'analisi delle criticità sollevate dall'applicazione della stessa all'Intelligenza Artificiale, occorre poi riportare quanto viene disposto dall'art. 22 di tale fonte, intitolato "*Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*": l'unica norma del Regolamento che si riferisce direttamente ad una possibile applicazione dell'intelligenza artificiale, ma, più in generale, al momento una delle prime disposizioni sul tema *tout court*.

Il suo titolo individua il settore dell'I.A. di interesse, quello cioè che riguarda le decisioni prese da sistemi algoritmici con riferimento ad un individuo: ad esempio, per la selezione dei *curricula* al fine dell'individuazione di risorse lavorative da assumere in un'azienda, o in applicazioni più specifiche, come per la decisione sulla libertà vigilata dei detenuti raggiunta attraverso l'intervento del sistema di intelligenza artificiale *Compas* utilizzato dalla Corte di La Crosse in Wisconsin USA. In particolare il disposto del suo primo paragrafo prevede:

"L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona".

Quindi, proprio a tutela dei diritti e delle libertà fondamentali, della dignità delle persone fisiche, si prevede la possibilità per l'interessato di rifiutare l'applicazione esclusiva di un sistema automatizzato nelle determinazioni che lo riguardano. Disposizione che ha poi alcune eccezioni nel paragrafo 2 della norma, nella specie quando la decisione

- sia necessaria per la conclusione o l'esecuzione di un contratto
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento,
- si basi sul consenso esplicito dell'interessato.

Eccezioni che, per la loro estensione (si pensi al problema dell'effettiva efficacia del consenso, in generale e nel caso concreto), sembrano svuotare di qualsiasi utilità l'art. 22 del Regolamento, ma che comunque sono equilibrate dall'applicazione di un'ulteriore regola generale a garanzia della persona coinvolta (il suo par. 3):

"il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano

da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione”,

e che comunque hanno a loro volta un’eccezione, stabilita dall’ultimo paragrafo dell’art. 22 (che le esclude in ogni caso in cui si tratti di “categorie particolari di dati personali”). Ma, a parte la disciplina dei processi decisionali automatizzati appena indicata, le disposizioni con cui il Regolamento 2016/679 ha strutturato la protezione dei dati personali sono applicabili alle attività di trattamento di tali dati svolte attraverso sistemi di I.A.?

5. Big Data, Intelligenza Artificiale e protezione dei dati personali: problemi e possibili soluzioni

La risposta al quesito è sicuramente affermativa, anche se poi altrettanto sicuramente si deve rilevare che le caratteristiche del “sistema GDPR” sollevano, come detto, diversi problemi per la sua effettiva operabilità rispetto alla realtà dell’I.A. e dei *big data*.

Premesso che il Regolamento UE 2016/679 deve essere osservato da qualunque titolare che utilizzi le informazioni personali di interessati che si trovano nell’Unione, “*con o senza l’ausilio di sistemi automatizzati*” (e quindi anche nella realtà tecnologica in esame), vediamo quali difficoltà si incontrano nell’applicare gli aspetti della disciplina normativa richiamati nel precedente paragrafo. Schematicamente,

- per quanto riguarda il rispetto dei principali generali del trattamento, le criticità maggiori si realizzano per quello di “*trasparenza*” (il trattamento deve avvenire in maniera chiara per l’interessato, principio da cui deriva l’obbligo di informativa, su cui si veda oltre), a causa della necessità di segretezza per consentire una prima tutela degli algoritmi di intelligenza artificiale, a fronte delle difficoltà per realizzare una loro effettiva protezione giuridica quale proprietà intellettuale; ma anche per quelli di “*minimizzazione*” e di “*finalità*” (secondo i quali si devono utilizzare solo i dati personali strettamente necessari per il raggiungimento dello scopo del trattamento, che non possono poi essere impiegati per scopi diversi), di impossibile applicazione se il sistema di I.A., in particolare di quelli basati sul *machine learning*, necessita del maggior numero di dati possibile per poter funzionare, con sviluppi spesso imprevedibili; ed infine per quello di “*limitazione della conservazione*”, anche in questo caso diametralmente opposto all’esigenza dei *big data*, come detto numerosissimi e comunque “per sempre”.
- con riferimento all’individuazione della corretta base giuridica del trattamento, in linea di massima consensuale, la difficoltà deriverebbe dalla possibilità concreta di rispettare il disposto normativo, non ultimo a livello di organizzazione pratica dell’adempimento: quella necessaria per raccogliere il consenso degli interessati coinvolti nel processo di intelligenza artificiale, di cui non si ha alcuna conoscen-

za, e poi per gestirlo nel tempo (si pensi alle eventuali richieste di revoca, da rendere effettive andando a cancellare i relativi dati personali nell'insieme complessivo delle diverse banche dati).

- strettamente connessi a quanto appena detto sarebbero infine il tema dell'adempimento dell'obbligo di informativa e quello di organizzazione dell'effettiva possibilità di esercizio dei diritti da parte dell'interessato: temi che non posso affrontare in questa breve relazione, ma le cui difficoltà sono intuibili.

Come evidenziato da diversa dottrina, ulteriori problematiche sono legate alla tipologia di trattamento dati posti in essere in tali realtà. Quella ad esempio causata dal fatto che in genere le informazioni risalgono a una lunga catena di acquisizioni, e solo alla fine vengono aggregate ed esaminate/utilizzate da titolari che possono non coincidere con coloro che li hanno raccolti; ancora, il fatto che spesso l'intervento di sistemi di I.A. sulla massa di dati portano a creare nuove informazioni impreviste, e imprevedibili, all'inizio della raccolta: realizzando ad un'indeterminatezza soggettiva che non si concilia con la stessa impostazione del Regolamento UE 2016/679. E, tra l'altro, i titolari di questi sistemi sono in genere le aziende "over the top" di difficile "gestione" per portarle al rispetto della normativa europea.

Come risolvere questi problemi? Rinunciare alla possibilità di proteggere i dati personali coinvolti in sistemi di intelligenza artificiale? Abdicazione che però porterebbe, alla luce dell'evoluzione tecnologica, ad eliminare del tutto la tutela di un diritto fondamentale dell'individuo, quello alla protezione dei suoi dati personali?

Prima di tentare di ipotizzare alcune soluzioni al problema, occorrerebbe procedere ad un'attenta analisi sul se e sul come viene oggi richiamata la disciplina sulla protezione dei dati personali nelle diverse fonti in materia di intelligenza artificiale. Si scoprirebbe infatti che quasi tutte prevedono indicazioni ben precise sul tema: ribadendo e sottolineando l'importanza del rispetto dei diritti fondamentali dell'individuo, in particolare quello alla protezione dei suoi dati personali.

Non potendo approfondire in queste brevi note l'esame delle varie fonti, mi limiterò a prendere come esempio la *"Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale"*: numerose sono in essa le norme sul punto, ad iniziare dal paragrafo 4.2 intitolato "Dati personali e riservatezza", ed in particolare il suo art. 126 in cui si *"ribadisce che il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali, quali sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali e dall'articolo 16 del trattato sul funzionamento dell'Unione europea si applicano a tutti i settori della robotica e dell'intelligenza artificiale e che il quadro giuridico dell'Unione per la protezione dei dati deve essere pienamente rispettato"*, e si *"evidenzia che i progettisti di sistemi robotici e intelligenza artificiale sono responsabili di sviluppare prodotti che siano sicuri e adeguati agli scopi previsti e di applicare le procedure per il trattamento dei dati rispettando la legislazione esistente e garantendo la riservatezza"*.

Ma si può fare riferimento anche all'art. 140, norma che introduce un altro tema, quello della cooperazione tra Commissione, Stati membri e mondo accademico, allo

scopo di

“rafforzare la condivisione delle conoscenze e promuovere l’istruzione e la formazione

- *per i progettisti, relativamente alle implicazioni etiche, alla sicurezza e al rispetto dei diritti fondamentali, e*
- *per i consumatori, per quanto riguarda l’utilizzo della robotica e dell’intelligenza artificiale, con una particolare enfasi sulla sicurezza e la riservatezza dei dati”.*

Cooperazione di cui il presente convegno rappresenta a pieno titolo un primo esempio applicativo.

La lettura della fonte appena riportata può far raggiungere un primo punto fermo: a fronte di un apparato normativo che si sta costruendo per regolamentare usi e sviluppi dell’I.A., che prende in grande considerazione la protezione dei dati personali, il contrasto sembrerebbe porsi non tanto e non solo nella dicotomia “applico/non applico”, ma anche nella più ampia scelta “rispetto/non rispetto” la legge. E allora, anche da questo punto di vista, non si può certo ritenere ammissibile la rinuncia a tale protezione, la rinuncia alla legalità.

Proviamo allora ad immaginare le possibili soluzioni, che indichiamo in tre differenti ambiti:

- dal punto di vista dei “player” del settore, cioè da un lato i fornitori di sistemi di Intelligenza Artificiale, dall’altro gli utilizzatori di tali sistemi (comunque tutti “titolari del trattamento” se vengono applicati ad informazioni relative agli individui, direttamente o indirettamente identificabili), ad adeguarsi correttamente al sistema della protezione dei dati personali introdotto dal Regolamento UE 2016/679;
- sviluppare il più possibile una tutela “dal basso”, cioè posta in essere dagli stessi interessati, che a loro volta sono utenti delle nuove tecnologie, e in maniera più o meno consapevole cedono i loro dati ai player citati: tutela che deve partire da una corretta formazione e informazione degli interessati (non quindi non possono più essere solo “tecno-entusiasti”, ma anche “tecno-consapevoli”), in generale sulla realtà digitale in cui vivono, ma in particolare sulla realtà del trattamento dei dati personali e sulla loro tutela;
- potenziare il più possibile la tutela “dall’alto”, quindi a livello normativo (non solo affermazioni generali di principio, ma regole più dettagliate e certe) ma in particolare potenziando l’Autorità Garante (che deve portare all’adeguamento al Regolamento anche i più importanti player, punto 1, e consapevoli il maggior numero possibile di interessati, punto 2), nella possibilità concreta di operare.

Utopia?

Sicuramente le soluzioni proposte sono ambiziose, e allo stesso tempo, riguardando la ... “privacy” (e tutte le difficoltà correlate di cui si è detto), di difficile realizzazione, e comunque non in tempi brevi.

Ma occorre capire che non si può non decidere, soprattutto a fronte della repentina evoluzione di sistemi I.A. sempre più potenti ed invasivi della nostra sfera privata, accorciando il più possibile i tempi per giungere alla soluzione del contrasto tra

sviluppo dell'intelligenza artificiale e protezione dei dati: avendo ben chiaro che la scelta in realtà si pone su un livello più ampio, in particolare tra la limitazione, o addirittura la rinuncia a un diritto fondamentale, per l'importanza (economica) del settore, ed invece un salto "culturale" che deve portare al successo al 100% del sistema di protezione dei dati personali, anche rispetto alle innovative (e di moda) applicazioni di intelligenza artificiale.

DISCRIMINAZIONI ALGORITMICHE?

Gianmarco Gometz¹

Abstract [IT]: Il funzionamento delle odierne IA basate sul modello del machine learning rende alquanto disagiata determinare se un certo responso algoritmico posto alla base di scelte, decisioni e policies produttive di effetti giuridici rilevanti per le persone, sia o no censurabile in quanto direttamente o statisticamente discriminatorio, ossia fondato sulla considerazione di una qualche caratteristica protetta dal diritto antidiscriminatorio come ragione, motivo o causa di un certo trattamento svantaggioso. Se tuttavia i dati di addestramento e gli algoritmi delle IA sono disponibili, v'è talora la possibilità di rieseguire questi ultimi per verificare se avrebbero prodotto gli stessi output qualora i soggetti considerati fossero stati di razza, sesso, religione, orientamento sessuale ecc. diversi, invalidando le decisioni fondate sulla considerazione di elementi che la legge vieta di porre alla base di disparità di trattamento produttive di svantaggi per gli interessati. I costi di questo approccio diventano però estremamente onerosi, e forse insostenibili, quando gli elementi utilizzati dal sistema per elaborare le proprie previsioni non sono ricavati da dataset "statici", bensì da ingenti flussi di dati continuamente aggiornati.

Abstract [EN]: The operation of today's AIs based on the machine learning model makes it somewhat uncomfortable to determine whether or not a certain algorithmic response placed at the basis of choices, decisions and policies productive of legal effects relevant to individuals is censurable as directly or statistically discriminatory, that is, based on the consideration of some characteristic protected by anti-discrimination law as the reason, motive or cause of a certain disadvantageous treatment. If, however, the training data and AI algorithms are available, there is sometimes the possibility of re-running them to see whether they would have produced the same outputs had the subjects considered been of a different race, sex, religion, sexual orientation, etc., invalidating decisions based on the consideration of elements that the law prohibits from being the basis for unequal treatment that is productive of disadvantages for those affected. The costs of this approach, however, become extremely onerous, and perhaps unsustainable, when the elements used by the system to make its predictions are derived not from "static" datasets, but from massive streams of continuously updated data.

Keywords [IT]: discriminazione – algoritmi – profilazione – intelligenza artificiale – discriminazione statistica – discriminazione algoritmica.

¹ Ordinario di Filosofia del diritto presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Cagliari.

Keywords [EN]: discrimination - algorithms - profiling - artificial intelligence - statistical discrimination - algorithmic discrimination.

Alla categoria concettuale delle “discriminazioni algoritmiche” vengono ascritte cose molto diverse: situazioni che risultano da errori degli (o negli) algoritmi, le cui prestazioni scadono “selettivamente” con riguardo ai soggetti appartenenti a certe minoranze; disparità di trattamento derivanti da vari bias nei dati utilizzati dagli algoritmi per elaborare le proprie stime, che perciò risultano inattendibili; decisioni o policies adottate col supporto di sistemi algoritmici che, pure accurati e attendibili nelle loro previsioni, svantaggiano sistematicamente gli individui appartenenti a taluni gruppi e così perpetuano condizioni di subalternità e svantaggio che sono frutto di inveterate situazioni sociali, eventualmente determinate o favorite da un passato di discriminazioni, ecc. Sorge perfino il sospetto che non tutte le eterogenee istanze di discriminazione algoritmica denunciate in letteratura possano essere ricondotte a un unico concetto giuridico, per quanto generico, e ci si può porre addirittura il dubbio che alcune di esse non possano essere propriamente qualificate come “discriminazione”. Occorre dunque elucidare un concetto di discriminazione algoritmica sufficientemente determinato da consentirci almeno di individuare gli abusi semantici più lampanti, ciò che tenterò di fare subito.

Se, come mi pare opportuno, ci si accosta alla nozione di discriminazione algoritmica muovendo dal concetto giuridico generale di discriminazione, se ne può evidenziare il connotato eminentemente tecnico-strumentale: è discriminazione algoritmica la prescrizione generale o singolare, il criterio o la pratica che comporta svantaggi relativi per taluni soggetti in quanto portatori delle caratteristiche protette dal diritto di cui parlavo prima, se adottata o attuata (anche) mediante l’impiego di algoritmi, compresi quelli dell’IA. Uso la formula “adottata o attuata mediante l’impiego di algoritmi” in un senso sufficientemente ampio da ricomprendere sia i “processi decisionali automatizzati relativi alle persone fisiche” ex art. 22 del GDPR sia ogni altra decisione adottata col supporto di algoritmi che forniscono ai decisori umani stime, descrizioni e previsioni probabilistiche su una certa situazione o caratteristica a cui il diritto ricollega effetti giuridici, direttamente o a seguito della decisione stessa.

Discriminazioni del genere, nella maggior parte dei diritti occidentali, possono venire proscriette a titolo di discriminazione diretta oppure indiretta. La distinzione in oggetto, dibattuta sia sul piano analitico-concettuale che su quello etico-fondazionale, oppone a) i trattamenti sfavorevoli di gruppi o persone a causa, in ragione o a motivo di certe loro caratteristiche protette a b) le prescrizioni, i criteri e le pratiche che svantaggiano in modo proporzionalmente maggiore gli appartenenti a un gruppo portatore di una caratteristica protetta, pur non essendo specificamente ad essi e a ciò indirizzate.

Ebbene, considerate nella loro modalità specificamente algoritmica, le discriminazioni indirette non presentano peculiarità degne di nota, giacché esse occorrono indipendentemente dal mezzo impiegato per provarle, dalla presenza di un intento discriminatorio esplicito o implicito e da qualsivoglia considerazione di un fattore di

protezione a fini discriminatori.

Molto più rilevante in una sede come questa, invece, è il tema dell'accertamento della ricorrenza di una discriminazione algoritmica diretta. Qui occorre infatti elucidare e provare le ragioni del trattamento asseritamente discriminatorio, ossia appurare se una certa decisione o pratica algoritmicamente assistita abbiano svantaggiato dei soggetti a cagione della loro appartenenza a una categoria protetta. Ciò può essere alquanto complicato nel caso di processi decisionali automatizzati mediante l'impiego di reti neurali basate su tecnologie di machine learning.

Come sappiamo, questi sistemi sono particolarmente “abili” nello scoprire automaticamente delle correlazioni tra dati per poi estrapolarne di nuovi, ciò che consente di utilizzarle come formidabili strumenti di profilazione, ossia a fini di analisi e previsione di comportamenti, qualità e disposizioni delle persone fisiche. Tale profilazione, oggi perlopiù applicata nel marketing, potrebbe senz'altro essere impiegata in un prossimo futuro in settori assai più pregnanti sotto il profilo pubblicitario: welfare, sicurezza, sanità, contrasto al crimine ecc.: ove vi sia sufficiente disponibilità dei dati personali degli individui, si potrebbero ad esempio usare le IA per scoprire se un certo soggetto sia più (o meno) bisognoso di particolari prestazioni sociali, o idoneo a ricoprire certi ruoli, oppure presenti maggiori probabilità di recidiva dopo esser stato condannato o di fuga dopo esser stato indagato, o se si stia radicalizzando come terrorista di matrice religiosa, o ancora se sia particolarmente propenso a commettere certi crimini e via dicendo.

Uno dei problemi che dovremo affrontare, nel momento in cui decideremo se impiegare questi strumenti di profilazione in settori caratterizzati da rilevanti interessi pubblici, proviene per l'appunto dal rischio di discriminazioni algoritmiche dirette. Allo stato attuale dei progressi tecnologici, infatti, le IA non possono chiarire esplicitamente, se, come e quanto dei fattori di protezione (ad es. la razza, il sesso, l'orientamento sessuale, l'età, la religione, le opinioni personali ecc.) abbiano influito nelle stime di volta in volta presentate, né quale sia il loro peso relativamente ad altre caratteristiche non protette dal diritto antidiscriminatorio ma parimenti rappresentate nei dati personali accessibili al sistema (residenza, preferenze d'acquisto, dati di geolocalizzazione, “likes”, siti visitati, contatti ecc.).

Tale opacità discende non da limitazioni superabili con idonei accorgimenti adottati in sede di progettazione degli algoritmi, ma da motivi strutturali legati al loro funzionamento come previsori statistico-quantitativi, piuttosto che come operatori razionali capaci di compiere inferenze logico-causali. Le reti neurali attuali non sono in grado di presentare alcun log circa le ragioni, i motivi, le cause, i fattori o anche solo i singoli passaggi computazionali che le hanno determinate a operare in un certo modo o a produrre un certo risultato, e il log manca perché non c'è alcun log, almeno ricostruibile al livello di astrazione richiesto in un contesto di controllo e giustificazione. L'attuale intelligenza artificiale è in questo senso un'intelligenza non intelligibile.

Per contrastare le discriminazioni algoritmiche discendenti dall'impiego di reti neurali basate sul paradigma dell'apprendimento automatico abbiamo dunque due stra-

de: 1) proscrivere a titolo di discriminazioni indirette; 2) approntare un quadro normativo rivolto alla verifica a posteriori di eventuali discriminazioni dirette nei responsi delle IA.

La prima strada non presenta criticità peculiari alle discriminazioni algoritmiche: Per accertare l'occorrenza di una discriminazione indiretta non è infatti necessario ispezionare gli algoritmi o i dataset di training alla ricerca di una qualche prova circa la funzionalizzazione dei dati relativi a caratteristiche protette alla produzione degli output del sistema. Sarà invero sufficiente accertare se la decisione o policy algoritmicamente assistita sia produttiva di effetti che nel complesso mettono gli appartenenti a qualche gruppo protetto in una condizione di particolare svantaggio, e valutare se ricorra o meno una delle cause di esclusione della discriminazione indiretta previste nel dato diritto positivo; per esempio, sia in ambito europeo che americano non ricorre alcuna discriminazione indiretta tutte le volte in cui una certa pratica o policy, pur produttiva di effetti svantaggiosi che colpiscono in modo proporzionalmente maggiore gli appartenenti a una categoria protetta, sia oggettivamente giustificata da una "finalità legittima" perseguita attraverso "mezzi appropriati e necessari". Queste formule rimandano ovviamente a qualificazioni altamente discrezionali da parte degli interpreti, ma non si tratta di problemi specifici delle discriminazioni algoritmiche, dunque possiamo tralasciarli in questa sede.

Una seconda direttrice normativa da percorrere per il contrasto alle discriminazioni algoritmiche passa per l'istituzione di controlli ex post sul funzionamento dei sistemi algoritmici di supporto alle decisioni produttive di effetti giuridici che riguardano le persone. Infatti, se pure è vero che i responsi delle odierne IA sono opachi in quanto non corredati né corredebili da un razionale intelligibile, la stessa cosa non vale necessariamente per i dati che sono stati usati per addestrare l'algoritmo a svolgere una certa funzione, né del resto per la funzione stessa: già dall'esame di questi elementi, se disponibili, accessibili e aperti a ulteriori sperimentazioni, può evincersi una spiegazione a posteriori e dunque una prova convincente del perché una certa IA ha deciso come ha deciso, in particolare quando si osservino delle disparità nei risultati che facciano sorgere il sospetto di una discriminazione algoritmica in corso. Gli algoritmi delle IA, contrariamente a quanto talora si afferma, non sono invero "liberi" di produrre qualsivoglia risultato, ma sono meccanicamente determinati dai processi di training attraverso i quali sono stati prodotti, ossia dai dati utilizzati per l'addestramento stesso, dagli outcomes da prevedere e dai fattori utilizzati per tale previsione; tutti elementi in buona misura dipendenti da contingenti scelte umane. Se dunque gli algoritmi e i dati di addestramento sono disponibili, v'è la possibilità di rieseguirli per verificare se avrebbero prodotto gli stessi output qualora i soggetti considerati fossero stati di razza, sesso, religione, orientamento sessuale ecc. diversi. In tal modo, è possibile rilevare ex post una discriminazione algoritmica diretta, e così invalidare la relativa decisione in quanto fondata sulla considerazione di elementi che la legge vieta di porre alla base di disparità di trattamento produttive di svantaggi per gli interessati. Sulla base di tutti questi rilievi, v'è anzi chi ritiene che le decisioni algoritmiche siano essere in generale più trasparenti di quelle umane,

soprattutto sotto il profilo dell'accertamento di eventuali discriminazioni, a patto di adottare i già menzionati accorgimenti relativi alla conservazione dei dati di addestramento, all'accessibilità agli algoritmi e alla loro rieseguitività in condizioni sperimentali di controllo.

Il limite di questo approccio è che prevede costi che divengono estremamente onerosi, e forse insostenibili, quando gli elementi utilizzati dal sistema per elaborare le proprie previsioni non siano ricavati da dataset "statici", bensì da ingenti flussi di dati continuamente aggiornati, come avviene nel caso delle ricerche sul web o nell'online ad delivery.

Questo è uno dei problemi che dovremo affrontare nel momento in cui dovremo decidere se impiegare questi strumenti di profilazione in settori caratterizzati da una notevole rilevanza degli interessi pubblici in gioco e dalle conseguenti frizioni tra interessi pubblici e diritti individuali, comprese le libertà fondamentali.

Un altro problema discende dalla domanda se le discriminazioni algoritmiche operate dalle odierne reti neurali basate sul paradigma del machine learning possono essere giuridicamente vietate in quanto discriminazioni statistiche, proscritte in buona parte dei diritti occidentali. Una discriminazione statistica, com'è noto, occorre quando un fattore di protezione (razza, sesso, ecc.) viene utilizzato come indicatore statistico di altre caratteristiche o disposizioni ordinariamente non visibili ma ricollegate a trattamenti svantaggiosi (quali controlli mirati, misure di sicurezza, esclusione da certe prestazioni sociali ecc.). Se ad esempio in una certa società gli appartenenti a un particolare gruppo etnico versano, in media, in condizioni economiche particolarmente disagiate, magari a causa delle discriminazioni di cui quel gruppo è stato vittima in passato, potrà facilmente spiegarsi il più elevato tasso di criminalità che si registra tra costoro. Se tuttavia questo dato è confermato da successive osservazioni empiriche, allora può razionalmente operarsi quella che Frederick Schauer chiama una generalizzazione non universale pura, ossia fondata su una buona base statistica: l'appartenenza di un certo soggetto a un gruppo etnico nel quale si registra un alto tasso di criminalità è un elemento che, singolarmente considerato, determinerà la stima di una maggiore probabilità di quel soggetto di commettere crimini, con possibili conseguenze sfavorevoli che potranno andare da un'intensificazione dei controlli di polizia a giudizi negativi operati nelle sedi in cui si valutino il pericolo di fuga, di recidiva ecc. Ecco allora la discriminazione statistica, consistente nell'aver impiegato la razza come indicatore statistico da cui inferire una maggiore probabilità di commettere crimini e, dunque, come ragione per disporre un trattamento sfavorevole.

Le discriminazioni statistiche si fondano su argomenti schematizzabili nella forma «molti X sono Y; Tizio è X; dunque v'è una particolare probabilità che Tizio sia Y», dove Y è una caratteristica o disposizione a cui vengono giuridicamente ricollegati degli svantaggi di qualche tipo. Si noti tuttavia che le stime e previsioni presentate dalle odierne IA non sono compiute sulla base di inferenze causali del genere di quelle coinvolte nel ragionamento appena schematizzato, ma sono il prodotto un'elaborazione in cui dati personali di qualsiasi sorta vengono convertiti in schemi di

attivazione di neuroni artificiali, “dissolvendosi” in impulsi binari trattati alla rinfusa e ricombinati in processi che rendono impossibile determinare direttamente se e quanto un singolo elemento discreto ricavato da un particolare dato personale abbia influito sul responso del sistema. La statistica, qui, non rileva al livello logico-inferenziale della conferma di una delle premesse dell’argomentazione che si conclude col responso discriminatorio, ma a un livello più profondo, elettronico-quantitativo, imperscrutabile agli esseri umani e per così dire oracolare: possiamo verificare ex post l’esattezza, accuratezza, attendibilità e lungimiranza delle stime e previsioni delle IA, quantomeno nel loro complesso, ma non possiamo ricostruire direttamente, specialmente al livello di astrazione richiesto in un contesto di giustificazione/controllo, il processo inferenziale che ha condotto alla loro elaborazione e i fattori e gli elementi in esso considerati. Ciò per la semplice ragione che il sistema non compie alcuna inferenza in senso logico-proposizionale, intesa come processo per cui si arriva ad affermare una proposizione dotata di significato sulla base di qualche altra proposizione dotata di significato.

Le discriminazioni algoritmiche operate mediante l’impiego delle odierne IA, pertanto, possono essere giuridicamente proscritte in quanto discriminazioni statistiche solo a condizione che sia chiaramente accertabile l’impiego d’una caratteristica protetta come fattore rilevante per la produzione del responso a cui vengono ricollegate conseguenze svantaggiose. Una condizione, questa, di ben difficile soddisfazione, alla luce dell’attuale paradigma di funzionamento delle reti neurali utilizzate a fini di profilazione.

MOLTI BIT, POCHE GARANZIE. APPUNTI SU BIG DATA E DEMOCRAZIA

Guido Saraceni¹

Abstract [IT]: L'avvento dei Big Data ha consegnato nelle mani delle principali piattaforme informatiche un formidabile potere politico. Non intendo richiamare l'attenzione *solo* sulla grande capacità esse hanno di archiviare “a futura memoria” qualsiasi foto, filmato o opinione espressa dagli internauti; non mi riferisco esclusivamente al fatto che siano in grado di seguire in tempo reale la navigazione degli utenti, mettendone sotto una lente di ingrandimento gli interessi, le preferenze e le abitudini; intendo soprattutto alludere al fatto che, analizzando i data assets, possono giungere a previsioni statisticamente consistenti sul comportamento futuro dei cittadini. Ancor di più, le società informatiche possono oggi significativamente orientarne gli atteggiamenti ed i pensieri, organizzando campagne di marketing il cui livello di targhettizzazione non era neanche lontanamente immaginabile solo dieci anni fa. Per questo motivo, molti autori parlano di algocrazia, la dittatura dell'algoritmo, dalla quale il web potrebbe liberarsi solo attraversando un ulteriore e radicale step evolutivo.

Abstract [EN]: The advent of Big Data has delivered formidable political power into the hands of major computing platforms. I do not mean to draw attention only to the great capacity they have to store “for future memory” any photo, film or opinion expressed by Internet users; I am not referring exclusively to the fact that they are able to track users' browsing in real time, putting their interests, preferences and habits under a magnifying glass; I mean above all to allude to the fact that, by analyzing data assets, they can arrive at statistically consistent predictions about the future behavior of citizens. Even more so, IT companies can now significantly direct their attitudes and thoughts, organizing marketing campaigns whose level of targeting was not even remotely imaginable just ten years ago. For this reason, many authors speak of algocracy, the dictatorship of the algorithm, from which the Web could free itself only by going through one more radical evolutionary step.

Keywords [IT]: Big Data – Algocrazia – Sovranità – Privacy – Web 3.0.

Keywords [EN]: Big Data - Algocracy - Sovereignty - Privacy - Web 3.0.

Sommario: 1. Il Web e le sue principali rivoluzioni. 2. Big Data. 3. Chi controlla le informazioni controlla il mondo. 4. Una gabbia di cristallo. 5. Il Metaverso: la rivoluzione prossima ventura.

¹ Associato di Filosofia del diritto e Informatica giuridica presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Teramo.

1. Il Web e le sue principali rivoluzioni

Il primissimo prototipo di intranet fu realizzato dal dipartimento della difesa nordamericano (ARPA) in maniera per dir così “casuale” e “laterale”, mentre i ricercatori erano impegnati in tutt’altra sperimentazione che nulla aveva a che fare con i protocolli di comunicazione informatica.

A differenza del programma all’interno del quale essa vide la luce, questa innovativa invenzione non fu classificata *top secret*; tutt’altro, venne consegnata nelle mani delle università e dei centri di ricerca, di modo che potesse essere approfonditamente studiata ed eventualmente implementata. Per un lungo periodo, fu un terreno esclusivo di sperimentazione riservato a docenti universitari, ricercatori, ingegneri informatici e hacker.

Dopo molti anni e duro lavoro, al quale collaborarono un numero imprecisato di appassionati sparsi in tutto il mondo, il seme inizialmente gettato dagli americani diede frutto al CERN di Ginevra, dove Tim Berners Lee inaugurò il *world wide web* - una versione di internet arricchita da innovazioni a dir poco essenziali affinché la rete potesse essere utilizzata da chiunque, a prescindere dal possesso di specifiche competenze informatiche².

La terza, successiva ed eclatante, rivoluzione fu dovuta all’avvento di due *killer applications*, ovvero, alla creazione di due piattaforme informatiche che stravolsero il *world wide web* trasformandolo in qualcosa di parecchio diverso, più performante e valoroso, rispetto alla sua prima versione: i motori di ricerca e i social network. O forse sarebbe più corretto dire, semplicemente, *Google* e *Facebook*³.

L’invenzione di un motore di ricerca il cui algoritmo prendeva in considerazione i link creati dagli utenti (ovvero sceglieva di seguire gli utenti, piuttosto che indirizzarli) ha rivoluzionato la rete almeno quanto la mondiale diffusione di una costellazione di blog interconnessi da una interfaccia accattivante e semplice da usare. In questo modo nacque il web 2.0, o new web, una struttura informazionale i cui contenuti di maggior successo sono opera degli stessi utenti che, in maniera più o meno spontanea e consapevole, lasciano tracce, condividono idee, fotografie, filmati. Mentre l’umanità passava dall’utilizzare internet, al world wide web, al web 2.0, un fiume carsico di dati iniziava a scorrere silenzioso nei server delle società informatiche.

² Mi riferisco, nello specifico, all’ipertesto, alla url ed al browser.

³ Per quanto riguarda la nascita ed il successivo sviluppo del *world wide web* la bibliografia risulta davvero sconfinata, risulta tuttavia imprescindibile il riferimento a ALBERT L. BARABÁSI, *Link. La scienza delle reti*, Torino, Einaudi, 2004; M. CASTELS, *La nascita della società in rete*; Milano, Boccioni, 2002; Id., *Galassia Internet*, Milano, Feltrinelli, 2013; J. FEDERER, *The hidden psychology of social networks*, New York, McGraw-Hill, 2020; S. JOHNSON, *La nuova scienza dei sistemi emergenti. Dalle colonie di insetti al cervello umano. Dalle città ai videogame e all’economia. Dai movimenti di protesta ai network*, Milano, Garzanti, 2001; L. LESSIG, *Il futuro delle idee*, Feltrinelli, Milano 2006; P. LÉVY, *L’intelligenza collettiva. Per un’antropologia del cyberspazio*, Milano, Feltrinelli, 1999; Id., *Cyberdemocrazia*, Mimesis, Milano, 2007; H. RHEINGOLD, *Smart mobs. Tecnologie senza fili, la rivoluzione sociale prossima ventura*, Milano, Raffaello Cortina, 2003.

I più acuti tra i ricercatori intuirono che si stava preparando l'avvento di una ulteriore rivoluzione ed i più avveduti tra gli imprenditori investirono fortemente su di essa. Con il passare del tempo, questo travolgente flusso di dati venne alla luce, imponendo all'attenzione di ricercatori informatici, politici e giuristi, il tema dei Big Data. Non siamo qui di fronte ad un vero e proprio *hot topic*. Per il dibattito pubblico, i big data non hanno il fascino o la popolarità dei motori di ricerca o dei social network. Di essi si parla meno, perché gli utenti sono coinvolti, in maniera spesso inconsapevole, solo sul versante della *produzione grezza*, mentre alle piattaforme informatiche è riservata l'analisi (il cosiddetto *data mining*), l'utilizzo e lo sfruttamento economico. Fatto sta che i Big Data rappresentano la quarta e forse la più importante rivoluzione informazionale cui abbiamo assistito sino ad oggi; sono il prodotto spontaneo, inarrestabile ed in una certa misura inevitabile, delle precedenti innovazioni; costituiscono una preziosa opportunità⁴ e, al tempo stesso, un grande pericolo.

2. Big Data

Non risulta affatto facile stabilire una definizione compiuta e condivisa di Big Data. Proviamo, in linea di prima approssimazione, ad elaborarne una tassonomia. Per quanto concerne la genesi, i Big Data possono essere prodotti dall'utente di un servizio digitale che, in maniera più o meno consapevole, lascia traccia delle proprie idee, abitudini e preferenze, mentre naviga sulla rete e utilizza gli strumenti messi a disposizione dal web; possono essere altresì creati in maniera del tutto autonoma dalle apparecchiature elettroniche di uso comune, che, collegandosi ad un sito o ad una specifica banca dati, comunicano con i server della società che le ha prodotte⁵. Per quanto riguarda il contenuto, non esiste nulla di ciò che siamo o facciamo che non possa essere digitalizzato, trasmesso e conservato, all'interno di una banca da-

⁴ Come ricorda B. KAISER, già venti anni fa, le Nazioni Unite e le ONG di tutto il mondo stavano provando ad utilizzare in tempo reale i dati a propria disposizione con finalità umanitarie, come, ad esempio, prevedere rivolte di piazza, carestie o genocidi – come quello accaduto in Ruanda nel 1994. Grazie all'analisi dei dati preventivi – come il costo del pane o la diffusione di insulti razzisti di Twitter –, i ricercatori speravano di poter fornire alle forze di pace le informazioni necessarie per garantire la sicurezza delle società ad alto rischio, consentendo loro di intervenire addirittura *prima* che determinati fenomeni superassero la soglia di attenzione (*La dittatura dei dati. La talpa di Cambridge Analytica svela come i big data e i social vengono usati per manipolare e minacciare la democrazia*, HaperCollins, Milano 2019).

⁵ Mettendoci in guardia circa i rischi impliciti nell'uso di apparecchiature connesse al web, B.-C. HAN scrive “Lo *smart bed* con fior di sensori perpetua la sorveglianza anche durante il sonno. La sorveglianza s'insinua sempre più nel quotidiano, sotto forma di *convenience*. Nell'atto di svolgere tante incombenze per noi, gli *infomi* si rivelano efficientissimi informatori che ci sorvegliano e ci influenzano” (*Le non cose. Capitolo Uno*, Kindle Ed.)

ti^{6,7}. Inoltre, i Big Data assumono una forma parecchio variegata: non esiste un solo formato in entrata, non esiste un formato unico di uscita. Peraltro, ne fanno parte dati grezzi e dati che sono stati già trattati.

Considerato quindi che non possono essere accomunati dalla fonte – fortemente eterogenea – dal contenuto – anch’esso disomogeneo – o dalla forma che assumono – altrettanto variegata – gli studiosi tendono a definire i Big Data elencando un numero variabile di proprietà che, per comodità, vengono ricomprese sotto l’etichetta di “4 v”.

La prima di esse è rappresentata dalla quantità, ovvero dal *volume*. Per provare ad avere idea delle dimensioni assunte da questo fenomeno, basti considerare che la sua unità di misura è rappresentata dallo *zettabyte*⁸, la cui capacità di archiviazione corrisponde a 36.000 anni di video in hd. Ovvero, ad una pila composta da circa 250 miliardi di dvd.

Il secondo elemento caratteristico è rappresentato dalla *velocità* di raccolta, trasmissione e archiviazione. Quest’ultima ha superato di gran lunga la nostra capacità di analisi, per questo motivo, la maggior parte dei dati viene semplicemente archiviata in vista di un utilizzo futuro.

La terza “v” è l’iniziale della parola *varietà* e fa riferimento alla mancanza di omogeneità – contenutistica e formale – di cui ci siamo già occupati.

La quarta caratteristica è infine il *valore*. Nel considerare quest’ultimo concetto non bisogna però commettere l’errore di pensare esclusivamente al valore economico, ovvero alla valutazione che il mercato attribuisce a specifici *data assets*, risulta al contrario opportuno prenderne in considerazione anche la grande utilità pubblica ed il valore lato sensu politico. Ad esso è dedicato il prossimo paragrafo.

⁶ A tal riguardo, Agata C. Amato Mangiameli illustra e commenta un significativo studio condotto presso la Stanford University grazie alla quale un team di ricercatori, “a partite da più di 50 milioni di immagini su 200 città mappate da Google Street View [...]” è stato in grado di fornire importanti indicazioni demoscopiche. Più esattamente, i ricercatori hanno utilizzato un algoritmo “a rete neurale convulzionale (*convolutional neural network*, ConvNet) in grado di processare 50 milioni di immagini in due settimane”. Sfruttando questa gigantesca mole di dati, i ricercatori hanno provato ad indagare le preferenze dei cittadini, stabilendo congrue relazioni statistiche tra il modello di un’auto, il contesto in cui è solita spostarsi, e l’orientamento politico del suo conducente (AGATA C. AMATO MANGIAMELI - MARIA N. CAMPAGNOLI, *Strategie digitali. #diritto_educazione_tecnologie*, Torino, Giappichelli, 2020 p. 58)

⁷ Avremo modo di considerare la questione più avanti, *infra* § 4. Per una prima e avvincente ricostruzione sulla predittività degli algoritmi, si veda ALBERT L. BARABÁSI, *Lampi. La trama nascosta che guida la nostra vita*, Torino, Einaudi, 2011.

⁸ Ad avviso di L. FLORIDI, l’avvento degli zettabyte (1000 esabyte) sarebbe uno dei fattori che annunciano la nascita della iperistoria. Più esattamente, l’“età zettabyte dell’iperistoria” rappresenterebbe un momento di passaggio tra i big data “ciechi” e quelli “dotati di vista”. L’autore non manca di notare come tutto questo implichi un forte consumo energetico e un altrettanto robusto impatto ambientale, rimarcando come nel 2000 i centri di deposito dati consumassero lo 0,6% dell’elettricità mondiale, mentre nel 2007 le ICT sono state responsabili dell’emissione di 830 milioni di tonnellate di anidride carbonica. Nel 2008 hanno prodotto una quantità di anidride carbonica maggiore di quanta ne hanno prodotto, complessivamente, l’Argentina e l’Olanda (*La quarta rivoluzione. Come l’infosfera sta trasformando il mondo*, Milano, Raffaello Cortina, 2014).

3. Chi controlla le informazioni, controlla il mondo

Sul finire del XXI secolo, Daniel Bell preconizzò “il controllo sui servizi di comunicazione” sarebbe divenuto presto una importante “fonte di potere”, mentre l’accesso alla comunicazione si sarebbe trasformato in una imprescindibile “condizione della libertà”. Queste osservazioni furono riprese ed approfondite da Jean-François Lyotard che, nel suo lavoro più celebre, affermò che la gestione delle informazioni avrebbe rappresentato una questione di fondamentale importanza per il “nuovo mondo post-moderno”⁹. A distanza di qualche anno, possiamo affermare che avevano entrambi ragione: le informazioni sono divenute, oggi, tutto ciò di cui abbiamo bisogno.

In primo luogo, si tratta di una inestimabile fonte di ricchezza. Mi riferisco a due fenomeni distinti e tuttavia connessi. Prima di tutto, penso alle criptovalute, apice di un processo di smaterializzazione e di virtualizzazione della moneta che certamente affonda le sue radici nei secoli passati. In secondo luogo, alludo alla interconnessione globale dei mercati finanziaria che consente agli speculatori di tradurre la rapidità con cui hanno ricevuto un’informazione in denaro sonante – reale o virtuale che sia. L’informazione è inoltre salute. Da un lato, le campagne di prevenzione e le raccolte fondi a favore della ricerca trovano sul web, ed in particolar modo nei social network, un proficuo terreno di coltura e di diffusione; dall’altro la medicina sempre più legata agli strumenti informatici, non solo dal punto di vista diagnostico, ma anche per quanto concerne i servizi offerti ai pazienti – basti pensare che la maggior parte dei centri clinici consente la prenotazione telematica di visite ed esami, nonché la consultazione dei referti on line – con evidenti benefici in termini di raccolta e conservazione dei dati.

L’informazione è infine potere, come sanno benissimo i politici che, da sempre, intrattengono strettissimi legami con il cinema, la televisione e, più in generale, con il mondo dell’editoria.

“Governare”, in ultima istanza, significa essere in grado di controllare le informazioni: non esiste istituzione democratica o partito politico che non possa risultare letalmente danneggiato da una campagna di disinformazione, dalla artata diffusione di una notizia falsa o, più semplicemente, scomoda; non esiste Paese che non debba temere la diffusione di opinioni pericolose per la tutela dell’ordine pubblico e della sicurezza nazionale.

Per tutti questi motivi dovrebbe ormai risultare chiaro che il web non è un “semplice” mezzo di comunicazione *per* le masse. Esso è infatti strutturalmente acentrico, libero e democratico – per non dire “anarchico”¹⁰ -; consente a chiunque di condi-

⁹ BELL, D., *Sociological Journeys: Essays 1960-1980*, Heinemann, London, 1980, 43, 51; LYOTARD, J.-F., *La condizione post-moderna. Rapporto sul sapere*, Feltrinelli, Milano, 1997, 31. Per un commento, RIFKIN, J., *L’era dell’accesso. La rivoluzione della new economy*, Mondadori, Milano, 2013, 290 e ss.

¹⁰ Si veda, a tal riguardo, AGATA C. AMATO MANGIAMELI, *Diritto e Cyberspace*, Torino, Giappichelli, 1998; ID., *Informatica Giuridica*, Torino, Giappichelli, 2010, 1-17; AGATA C. AMATO MANGIAMELI - G. SARACENI,

vedere il proprio pensiero, divulgando notizie, informazioni e teorie, alternative o contrarie rispetto a quanto gradito a governi e grandi gruppi editoriali. Il suo chiaro ed apparentemente preminente aspetto mediatico riverbera in maniera determinante sulla sovranità statale, mettendone sotto scacco una prerogativa a dir poco fondamentale¹¹.

A maggior riprova di ciò, le dittature temono i social network come la peste e fanno di tutto per provare a limitare l'accesso; mentre le democrazie sono state costrette a venire a patti con le più importanti società informatiche in ragione del loro sempre maggiore potere politico.

Non intendo qui richiamare l'attenzione *solo* sulla grande capacità che le piattaforme informatiche hanno di archiviare "a futura memoria" qualsiasi foto, filmato o opinione espressa dai cittadini; non mi riferisco esclusivamente al fatto che molte e sempre più sofisticate piattaforme sono in grado di seguire in tempo reale la navigazione degli utenti, mettendone sotto una lente di ingrandimento gli interessi, le preferenze e le abitudini¹²; intendo soprattutto alludere al fatto che l'analisi dei Big Data può condurre a previsioni statisticamente consistenti sul comportamento futuro degli utenti; consentendo alle istituzioni e alle imprese di attuare su queste basi condotte dal carattere discriminatorio¹³. A dirla tutta, le grandi società informatiche non faticano eccessivamente ad indovinare cosa faranno o penseranno gli internau-

I reati informatici. Elementi di teoria generale e principali figure criminose, Torino, Giappichelli, 2015; AGATA C. AMATO MANGIAMELI - MARIA N. CAMPAGNOLI, *Strategie digitali*, cit., in particolare, 3-28; L. FLORIDI, *La quarta rivoluzione*, cit.; D. KAYE, *The Global Struggle To Govern The Internet*, New York, Columbia Global Reports, 2019.

¹¹ Come aveva ben compreso H. RHEINGOLD già agli albori della rete, "L'importanza politica delle comunicazioni telematiche sta nella capacità di mettere in crisi l'esistente monopolio della gerarchia politica sui mezzi di comunicazione potenti, rivitalizzando in tal modo la partecipazione democratica del cittadino. La previsione di Ben Bagdikian [...] è che alla fine del secolo "cinque-dieci giganti aziendali controlleranno la maggior parte dei più importanti periodici, libri, canali radiotelevisivi, film, incisioni e videoregistrazioni del mondo". Questi nuovi signori dei media possiedono il potere immenso di determinare quali informazioni sul mondo vanno distribuite alla maggior parte della gente [...] La soluzione militante è l'uso della telematica per creare reti informative planetarie alternative. La distribuzione delle reti di telecomunicazione, unita alla disponibilità di computer a prezzi ragionevoli, consente di muoversi nell'infrastruttura tradizionale per mezzi di reti alternative" (*Comunità virtuali: parlare, incontrarsi, vivere nel ciber spazio*, posizione 364 di 698, kindle edition)

¹² Imprescindibile, a tal riguardo, il riferimento a D. LYON, *L'occhio elettronico. Privacy e cultura della sorveglianza*, Milano, Feltrinelli, 1997; Z. BAUMAN - D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, Roma-Bari, Laterza, 2015; D. LYON, *La cultura della sorveglianza. Come la società del controllo ci ha resi tutti controllori*, Roma, Luiss University Press, 2020.

¹³ La più preoccupante applicazione di questo principio potrebbe senza dubbio verificarsi in ambito penalistico. Se la predittività degli algoritmi venisse portata alle sue più estreme e logiche conseguenze, essa consentirebbe di individuare in anticipo i probabili criminali, lasciando ai politici ed alle forze dell'ordine il dilemma se sia più corretto intervenire preventivamente, al fine di evitare una futura vittima, o non sia più giusto limitare la libertà dei cittadini esclusivamente in ragione di ciò che essi hanno effettivamente già fatto - piuttosto che sulla base di calcoli statistici predittivi. Su questo spinoso dilemma, cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *Big data*, cit., 215 e ss; ANNA M. MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali*, «Archivio Penale», 1/2021, 1-37.

ti in futuro, visto che possono orientarne significativamente gli atteggiamenti ed i pensieri – basti pensare al fenomeno delle *fake news* ed al modo in cui esse abbiano già inciso su epocali movimenti di opinione, falsando nettamente il libero sviluppo delle democrazie¹⁴.

Per tutti questi motivi, alcuni autori parlano oggi di *algocrazia*, lasciando ad intendere che la libertà dei cittadini, la loro uguaglianza ed i loro diritti fondamentali – sempre più intimamente connessi agli sviluppi del *world wide web*¹⁵ - siano gravemente minacciati dagli algoritmi informatici – facile paravento dietro il quale si nasconderebbero strategie che, in realtà, vengono adottate da esseri umani, istituzioni ed aziende, tanto potenti (quanto virtualmente irresponsabili).

4. Una gabbia di cristallo

Sul finire del XVIII secolo, Jeremy Bentham ha descritto ed anticipato, nel *Panopticon*, una caratteristica a dir poco fondamentale della nostra attuale condizione sociale.

I concetti essenziali della teoria benthamiana sono architettonici e psicologici ad un tempo. L'autore immagina infatti un istituto di detenzione a pianta circolare, in cui il controllore è alloggiato in una stanza centrale, dalla quale è in grado di osservare, in qualsiasi momento, ciò che accade nelle celle dei detenuti - essendo queste ultime ben visibili e sempre illuminate. Inoltre, grazie ad un sistema di tubi di stagno, egli può far sentire la propria voce all'interno delle celle, ascoltando a sua volta la voce dei detenuti. Oppure, può restare in silenzio ad origliare.

L'architettura del *Panopticon* favorisce dunque un controllo costante, verticale e unidirezionale, per cui il carceriere è in grado di osservare senza essere visto ed ascoltare senza essere ascoltato. Tutto ciò, al fine di indurre nei detenuti uno stato di psicosi paranoide che, con il passare del tempo, li avrebbe portati ad interiorizzare - e dunque rispettare rigorosamente - l'ordine e la disciplina. In poche parole: l'angoscia causata dal pensiero di poter essere visti e quindi sanzionati avrebbe agito, ad avviso di Bentham, come un potentissimo dissuasore, spingendo i reclusi verso la più compiuta e mansueta obbedienza.

Il modello benthamiano, dal quale prendono le mosse molti e qualificati studi, è stato criticato, perché l'unico controllore non avrebbe potuto osservare costantemente tutti i detenuti e dunque non avrebbe potuto sanzionarne tutte le violazioni: nel momento in cui i detenuti avessero compreso, grazie all'esperienza diretta, che

¹⁴ A tal riguardo, G. RIVA, *Fake News. Vivere e sopravvivere in un mondo post-verità*, Bologna, Mulino, 2018; R. GREIFENENDER - MARIELA E. JAFFÉ - N. SCHWARZ (a cura di), *The Psychology of Fake News. Accepting, Sharing and Correcting Misinformation*, New York, Routledge, 2021.

¹⁵ Con riguardo al rapporto tra diritti fondamentali e web, mi permetto di rimandare a G. SARACENI, *Digital Divide and Fundamental Rights*, «Humanities and Rights Global Network Journal», 2 (1) 2020, pp. 66-91, <https://doi.org/10.24861/2675-1038.v2i1.27>.

la sanzione non seguiva necessariamente ad ogni infrazione, il controllo avrebbe definitivamente perso il suo effetto paranoide e dunque la capacità di influenzarne ed educare il contegno¹⁶.

In realtà, dal punto di vista strettamente psicologico, la critica non risulta così corretta come potrebbe apparire *prima facie*. Sin dagli albori, gli studi sull' apprendimento operante hanno infatti dimostrato che l'essere umano risulta maggiormente condizionato – nelle sue scelte ed azioni – quando il rinforzo (positivo o negativo che sia) è *eventuale* e *casuale*, piuttosto che costante. Ciò a dire, il giocatore d'azzardo viene attratto e catturato da un meccanismo in cui le ricompense sono relativamente rare, e tuttavia non riesce a liberarsi dalla compulsione - che lo costringe a sedersi al tavolo per girare ancora un'altra carta. Il rinforzo negativo immaginato da Bentham è dunque perfettamente in grado di condizionare il comportamento dei detenuti. Per la teoria dell'apprendimento, ciò che conta è che la punizione, seppur non certa, sia tale da intimidire e dunque da dissuadere i soggetti interessati dal desiderio di correre il rischio.

A prescindere dalla valenza psicologica del *Panopticon*, che meriterebbe altro e diverso contesto per essere adeguatamente approfondita, è certo che il modello immaginato da Bentham possieda una forte valenza filosofica e un altrettanto nitida carica simbolica, in ragione delle quali costituisce, ancora oggi, il metro di paragone con cui sono chiamate a confrontarsi molte e variegiate teorie.

Dalla società *post-panottica* descritta da Deleuze e Guattari già negli anni '70, alla più attuale *panopticommodity* cui fa riferimento David Lyon; dall'*Oligopticon* immaginato da Bruno Latour, al *ban-opticon* su cui insiste Didier Bigo, sembra infatti che gli studiosi non possano davvero fare a meno di confrontarsi con il modello benthamiano¹⁷ - vuoi per affermare il suo definitivo superamento, vuoi per meglio descrivere, attraverso un gioco di concordanze e differenze, la condizione in cui versa la società contemporanea.

La maggior parte degli autori insiste sul fatto che, a differenza di quanto accadeva nel modello benthamiano, incentrato su di un meccanismo coatto, siano oggi gli stessi sorvegliati a consegnare volontariamente la propria privacy nelle mani dei

¹⁶ Come riporta, correttamente, Perri, “Le critiche al *Panopticon* muovevano dalla considerazione che, pur essendo una struttura pensata per funzionare con un unico sorvegliante, quindi molto economica in termini di gestione, non si poteva escludere che qualcuno sarebbe potuto sfuggire alla sanzione perché magari, in quel momento, il sorvegliante non lo stava osservando. Nel *Panopticon* vi è, come già illustrato, una percezione del controllo, ma non è detto che questo controllo venga effettivamente esercitato in un preciso momento. Moltiplicando questa ipotesi per un numero cospicuo di volte, è evidente che ne risulterebbe minata la credibilità stessa del sistema panottico” (P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, Milano 2020, 8).

¹⁷ Come rileva, giustamente, D. LYON, “Quando si inizia a studiare il tema della sorveglianza, l'idea del Panopticon appare decisamente brillante. Essa offre, a un primo livello, una teoria sul funzionamento della sorveglianza e, a un altro livello, una soluzione per collocare la sorveglianza nella vicenda della modernità. Il Panopticon ha un ruolo fondamentale in Foucault che, come è noto, vide nella struttura panottica di Bentham la chiave per comprendere l'ascesa delle moderne società dotate di autodisciplina” (*Sesto Potere. La sorveglianza nella modernità liquida*, Laterza, Roma-Bari 2014, 39).

controllori, assoggettando se stessi, spesso anche con entusiasmo, all'occhio indiscreto di una rete che tutto osserva, tutto registra e nulla dimentica. Ciò accade, ad avviso di Zygmunt Bauman, in ragione di una peculiare trasmutazione valoriale, per cui l'esigenza della privacy sarebbe stata sostituita dalla paura di essere esclusi (cosiddetta FOMO), tagliati fuori da quel mondo di relazioni digitali che rappresenta ormai l'imprescindibile ambito di crescita e di interazione sociale¹⁸. Possiamo tuttavia immaginare che non tutti gli utenti accettino di buon grado l'invadenza delle piattaforme informatiche e che il web nel suo complesso sia già pronto per un nuovo e rivoluzionario step evolutivo.

5. Il Metaverso. La rivoluzione prossima ventura

Molti studiosi immaginano che il Metaverso sia un progetto dell'azienda di Menlo Park, supponendo che si tratti di un nuovo social network legato in maniera imprescindibile all'utilizzo del visore 3d. In realtà la creatura di Zuckerberg sta al Metaverso come Facebook sta alla categoria Web 2.0 – o, se preferite, alla categoria Social Network. Possiamo legittimamente supporre che, ove la piattaforma di Meta fosse realmente predisposta e messa on line, avrà un grande successo e probabilmente finirà per essere identificata con il web 3.0 *tout court*. Tuttavia, dobbiamo rimarcare come già oggi esistano diversi siti che ne utilizzano l'innovativo protocollo di comunicazione.

On line troviamo infatti portali come *Decentraland*, *Sandbox* o *Stangelands*, che, sfruttando le tecnologie di registro distribuito (DLT), consentono ai propri utenti di interagire, tramite un avatar, all'interno di un ambiente virtuale altamente responsivo.

Per evitare di fare confusione, e trarre conseguentemente giudizi affrettati, dobbiamo tenere ben a mente che l'interfaccia grafica rappresenta la mera, e a ben vedere non troppo innovativa, superficie dell'architettura informatica interazionale che essa implica e sottende. Detto in altre parole, l'interfaccia grafica del Metaverso si limita a riproporre sotto una veste più accattivante un mondo virtuale vecchio ormai di vent'anni – considerato che Second Life fu messo per la prima volta on line nel lontano 2003.

Il fulcro del web 3.0 è invece rappresentato dall'utilizzo delle tecnologie a registro distribuito (DLT). Grazie alla blockchain, che di queste tecnologie rappresenta l'ap-

¹⁸ “Quel che oggi ci spaventa non è tanto la possibilità di un tradimento o di una violazione della privacy, quanto il suo opposto, il chiudersi delle vie di uscita da essa. L'area della privacy è diventata un luogo di reclusione e il titolare di questo spazio privato è condannato a cuocersi nel suo brodo in una condizione contrassegnata dall'assenza di ascoltatori entusiastici che non vedono l'ora di estrarre e strappare i nostri segreti dai forzieri della privacy [...] *Sembra che non avvertiamo più alcuna gioia ad avere segreti*” (Z. BAUMAN, D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, Laterza, Roma-Bari 2014, 13, corsivo dell'autore.)

plicazione più celebre, gli utenti del Metaverso possono infatti interagire in maniera completamente anonima e relativamente sicura.

Gli aspetti essenziali della blockchain sono essenzialmente tre: 1) la tracciabilità delle informazioni in essa contenute; 2) la loro immodificabilità; 3) la loro condivisione. Essa è dunque equiparabile ad un libro mastro che sfrutta funzioni crittografiche per garantire la propria integrità, uno sconfinato database digitale distribuito tra i nodi di una rete, utile per la gestione delle transazioni e delle interazioni tra di essi.

L'avvento di questa tecnologia informatica determina interessanti e profonde ripercussioni nel mondo del diritto. Non a caso l'Unione Europea, in un documento del febbraio del 2017 significativamente intitolato *How blockchain technology could change our life*, ne ha preconizzato molti e proficui utilizzi. L'attenzione delle istituzioni europee sul tema è talmente elevata che, nel 2018, è stato istituito un Osservatorio ad esse dedicato; inoltre, nel mese di ottobre dello stesso anno, il Parlamento ha votato una risoluzione in cui invitava la BCE a predisporre una attenta analisi dei rischi connessi alla volatilità delle criptovalute, richiedendo al contempo alla Commissione di promuovere uno studio del quadro normativo dei singoli Stati membri in materia di smart contract.

Al fondo di tutti questi eterogenei atti normativi, si agita, in maniera sempre più evidente, la consapevolezza che le DLT possano ristabilire anarchia, anonimato e affidabilità, nelle interazioni virtuali, sfuggendo alla dittatura degli algoritmi ed alla dataveglia che essa implica ed alimenta: la sfida dei nuovi portali consiste quindi nel sottrarre i dati degli utenti all'occhio indiscreto dei governi ed al gioco crematistico del mercato.

Al posto di incardinare la sicurezza degli utenti sul tradizionale controllo up-bottom delle informazioni e delle interazioni, il Metaverso opta per una regolamentazione bottom-up, ovvero per un sistema di *governance* autogestito dagli utenti.

In ragione di quanto sin qui esposto e considerato, al netto dei problemi giuridici accennati con i quali saremo comunque chiamati a confrontarci in futuro, il Metaverso potrebbe quindi essere considerato come una 'risposta evolutiva' del web allo spinoso problema dei Big Data, ovvero, come il tentativo di costruire un ambiente virtuale interazionale definitivamente, privo di controlli, di strumentalizzazioni e di gabbie.

ARS DISTINGUENDI, DISCRIMINAZIONE E MACCHINE INTELLIGENTI

ARS DISTINGUENDI, DISCRIMINATION AND INTELLIGENT MACHINE

Angelo Costanzo¹

Abstract [IT]: L'ars distinguendi evita le disuguaglianze che derivano dalle erronee assimilazioni, ma il suo uso dipende dal livello di analisi al quale si colloca. Mediante la dissociazione delle nozioni fonda le argomentazioni giuridiche che risolvono le incompatibilità normative e quelle che affinano la scelta delle massime di esperienza per la ricostruzione dei fatti. Invece, non risulta che allo stato attuale gli algoritmi dalla razionalità artificiale del loro sviluppo, siano in grado di seguire percorsi che fuoriescano dalle direttrici della logica formale per entrare nel campo della argomentazione. In particolare, non aiutano a superare l'ambiguità esplicativa, che affligge l'uso delle informazioni statistiche concernenti classi di eventi.

Abstract [EN]: The ars distinguendi avoids the inequalities that derive from erroneous assimilations, but its use depends on the level of analysis at which it is placed. Through the dissociation of notions he finds the juridical arguments that resolve the normative incompatibilities and those that refine the choice of the maxims of experience for the reconstruction of the facts. On the other hand, it does not appear that at present the algorithms with the artificial rationality of their development are able to follow paths that go beyond the guidelines of formal logic to enter the field of argumentation. In particular, they do not help to overcome the explanatory ambiguity, which afflicts the use of statistical information concerning classes of events.

Keywords [IT]: ars distinguendi – incompatibilità normative – massime di esperienza – ambiguità esplicativa.

Keywords [EN]: Ars distinguendi – normative incompatibilities – maxims of experience – explanatory ambiguity.

Sommario: 1. Argomentazione e distinzione. – 2. Decisioni giudiziarie e algoritmi della razionalità artificiale. – 3. Per un uso non discriminatorio della razionalità artificiale.

¹ Consigliere della Corte di Cassazione.

1. Argomentazione e distinzione

1.1. L'ars distinguendi ha valore in tutti i settori della conoscenza ma nel diritto, in particolare, costituisce un necessario costante esercizio per cogliere la specificità dei casi e evitare le disuguaglianze che derivano dal trattare in modo simile situazioni invece dissimili, cioè differenziabili sulla base di un principio giuridico che sia pertinente alla fattispecie.

L'argomentazione che enfatizza le somiglianze è epiforica, perché produce un effetto di accumulo ma anche di possibile con-fusione di conoscenza, quando l'accrescersi dei dati rischia di risolversi in un loro mero affastellamento. Invece, l'argomentazione che evidenzia una dissomiglianza fra le situazioni svolge una contraria funzione diaforica che sta alla base della ars distinguendi ma rischia di disperdere possibili significative connessioni fra i dati. Allora, una corretta operazione di distinzione concettuale non cancella la base di similitudini da cui parte ma opera un meta-giudizio che si conclude attribuendo un prevalente rilievo alla differenza: così non disperde conoscenze ma le rielabora criticamente.

In questa direzione, la ricerca di ragioni per escludere quella che era ammessa come una somiglianza e tramutarla in una diversità essenziale può dipendere dai diversi livelli dell'analisi: due oggetti possono apparire simili a un dato livello ma a un altro possono differire.

In realtà, l'albero di Porfirio (quello delle ramificazioni concettuali) può svilupparsi in diversi modi e in modi diversi ci si può arrampicare o appollaiare sui suoi rami. La molla intellettuale che porta a associare o dissociare le nozioni nasce da una opzione interna alla psicologia e alla formazione culturale dell'interprete che può tradursi in un dato giuridicamente rilevante se è ancorata a circostanze fattuali significative in relazione ai dati normativi (ai principi soprattutto) offerti dall'ordinamento giuridico.

1.2. L'ars distinguendi sta alla base delle più importanti argomentazioni che si sviluppano nel campo giuridico.

1.2.1. Dalla compresenza di norme fra loro incompatibili può derivare una pluralità indefinita di conseguenze inconciliabili (*ex contradictione quodlibet sequitur*) e, quindi, inaccettabili come strumenti di regolazione sociale. Nella prassi le incompatibilità non vengono trattate in modo rigoroso ma sono affrontate solo se si palesano in un caso concreto in cui l'interprete deve necessariamente decidere come scioglierle perché norme fra loro incompatibili non possono essere co-applicate (non integralmente co-applicate) allo stesso fatto storico. Tuttavia, quando i criteri legislativi di risoluzione delle antinomie non soccorrono, è necessario servirsi degli strumenti non codificati, che tradizionalmente appartengono alla ars distinguendi. Anche in questo caso le incompatibilità possono elidersi in radice facendo leva su una distinzione concettuale (che non richiede una compiuta ramificazione dei contenuti delle idee): è sufficiente enfatizzare una differenza all'interno dell'elemento considerato (fatto storico e/o dato normativo) o fra i due elementi inizialmente associati, che elimina la possibilità di confrontare sullo stesso piano i termini dei quali

si deve vagliare la compatibilità.

1.2.2. Analogamente, il modo classico per rigettare una precedente decisione è fondato sulla distinzione concettuale (la cosiddetta dissociazione delle nozioni, secondo la terminologia di Perelman).

Mentre la conferma del precedente è basata sulla parificazione di due casi (disconoscimento di rilevanza giuridica alle diversità naturali fra i due casi), il distinguere (*distinguishing*) dal quale consegue la reiezione del precedente si fonda sulla enfaticizzazione delle differenze. Oppure, nel ricorso al precedente a contrario, si adduce un controesempio rispetto al caso esaminato e si argomenta nel senso che quest'ultimo va inquadrato, o comunque risolto, in modo diverso rispetto a quello del precedente.

1.2.3. Lo stesso meccanismo vale quando, nella ricostruzione dei fatti storici, si deve scegliere fra le massime di comune esperienza (delle quali non esiste un codice...) quella o quelle pertinenti al caso concreto per farne la base di avvio delle inferenze abduttive o, con ben maggiore elaborazione metodologica, quando nella ricerca scientifica o nell'applicazione della scienza acquisita di valuta di dovere arrestare lo sviluppo dell'inferenza induttiva per valorizzare un controesempio.

Il ricorso alle massime di esperienza (spesso inevitabile per la mancanza di strumenti di valutazione più rigorosi) comporta il rischio della fallace confusione fra generalità e generalizzazione insito nella tendenza a attribuire carattere di generalità a quelle che potrebbero rivelarsi mere indebite generalizzazioni, tanto più se si considera che esse si formano secondo vie non vigilate dal rigore del metodo scientifico perché non esiste un metodo che fondi una massima di comune esperienza che evoca l'*id quod plerumque accidit* secondo un giudizio che postula (ma non verifica sperimentalmente) la normalità del reiterarsi di un certo tipo di eventi (questo limite distingue l'abduzione su cui si fondano le massime di esperienza da quella a base delle leggi scientifiche).

Il ragionamento che raccorda una massima di comune esperienza al caso concreto risulta manifestamente illogico se l'individuazione di altre massime di esperienza di diverso contenuto, ma egualmente pertinenti al caso, palesa l'arbitrarietà della sua assolutizzazione. Molte argomentazioni si muovono lungo la linea del conflitto fra generalizzazione e particolarizzazione: in questo territorio l'enfaticizzazione delle particolarità del caso concreto su cui poggia la seconda è un prodotto dell'analisi e dell'*ars distinguendi* che ordinariamente è illuminante, ma risulta fuorviante se irrelata a specificità giuridicamente rilevanti.

1.2.4. Ancora, sappiamo che nelle aree di confine tra quel che è rilevante e quel che non è rilevante per il diritto si svolgono dinamiche che lo rinnovano: quanto più si sviluppa l'indagine critica tramite l'*ars distinguendi* tanto più possono emergere situazioni che producono eccezioni al quadro generale iniziale. Oppure che lo espandono, ampliando la considerazione della gamma degli interessi giuridicamente rilevanti e conducendo, se del caso, a una ricombinazione dei dati normativi vigenti per rimodularne la valenza in una composizione nuova secondo i modi del giudizio riflettente (sicché la logica trapassa in estetica).

In realtà, l'interpretazione accurata può aumentare l'incertezza del diritto perché solleva nuovi problemi rivelando complessità inattese [Quintiliano, Istituzione oratoria, II, XIII, 1]. L'interpretazione rigorosa dei fatti e delle norme può entrare in contrasto con l'aspirazione (psicologica e sociale) alla certezza del diritto. Attraverso questi percorsi, persino la disposizione legislativa più semplice può veicolare molteplici significati normativi. In ogni caso, le forme discorsive sono affidabili se riescono a rappresentare idoneamente ciò a cui si riferiscono, ma a volte, risultano fuorvianti rispetto all'oggetto delle loro intenzioni e chi ordinariamente lavora con le proposizioni rischia di scivolare inavvertitamente dal piano della realtà al piano delle mere formule linguistiche.

2. Decisioni giudiziarie e algoritmi della razionalità artificiale

2.1. Gli algoritmi dalla razionalità artificiale si prestano a essere usati in vari ambiti di interesse per le decisioni giudiziarie, ma non risulta che, allo stato attuale del loro sviluppo, siano in grado di seguire percorsi che fuoriescano dalle direttrici della logica formale per entrare nel campo della argomentazione.

Per altro verso, la maggior parte dei software che li implementano sono coperti da brevetti appartenenti a aziende private, sicché la comprensione dei meccanismi del loro funzionamento è solo parziale e questo pregiudica le esigenze di trasparenza e di verifica indipendente della qualità e affidabilità dei risultati da essi prodotti. Si ritiene che correlazioni statistiche tratte dai dati personali possano rendere meglio prevedibili i comportamenti degli individui riconducendoli allo spettro di possibilità riassunte da un profilo riconducibile a una categoria generale. Ma può anche avvenire che i big data non si traducano in elaborazioni statistiche ma si risolvano nella raccolta di una massa di variegate informazioni concernenti lo stesso individuo.

In ogni caso, l'utilizzo di tecniche di combinazione algoritmica e statistica dei dati personali dell'indagato o della persona offesa e di informazioni raccolte sul luogo del crimine pone problemi di bilanciamento tra le esigenze di indagine e il rispetto di principi costituzionali e di norme processuali – che nell'ordinamento italiano riguardano specificamente gli artt. 187 cod. proc. pen. (oggetto della prova), 133 cod. pen. (determinazione della pena), la prognosi sulle esigenze cautelare, 220, comma 2, cod. proc. pen. (divieto di perizia personologica) e il rispetto del diritto alla riservatezza – dei quali si interessa la Direttiva europea n. 680/2016 per la circolazione tra paesi europei dei dati personali ai fini di giustizia.

2.2. Tenendo conto anche (ma non soltanto) di questi aspetti, il Consiglio d'Europa, tramite la propria Commissione per l'efficacia della giustizia (CEPEJ), il 4 dicembre 2018 ha adottato la Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi che enuncia i seguenti principi: 1) rispetto dei

diritti fondamentali; 2) non discriminazione; 3) qualità e sicurezza; 4) trasparenza, imparzialità e correttezza; 5) garanzia del controllo umano.

Nel documento esplicativo allegato alla Carta etica si precisa che «l'uso di algoritmi di intelligenza artificiale nei sistemi giudiziari europei rimane principalmente un'iniziativa commerciale del settore privato, rivolta a compagnie assicurative, uffici e studi legali, avvocati e privati» e si osserva che l'utilizzo di tali algoritmi è utile «nel campo della giustizia civile, commerciale e amministrativa al fine di una risoluzione precontenziosa online delle controversie, purché un ricorso successivo al giudice rimanga possibile». Per i procedimenti penali, si avverte che anche se non sono specificamente progettati per essere discriminatori, gli algoritmi basati sull'intelligenza artificiale veicolano «il rischio di favorire la rinascita di teorie deterministiche a scapito delle teorie dell'individualizzazione della pena».

Inoltre, l'articolo 21 della Carta dei diritti fondamentali dell'Unione europea, vieta la profilazione finalizzata alla discriminazione di persone fisiche sulla base di specifiche categorie di dati personali .

2.3. Attualmente la fonte più estesa dei dati è internet, ma sono disponibili anche numerose banche-dati informatiche non necessariamente collegate alla rete.

I big data possono servire per giudizi retroduttivi o prognostici utili nella fase cautelare, nel giudizio e nella esecuzione della pena ma può ledere il diritto di difesa impedendo o rendendo difficoltoso per l'indagato o l'imputato contestare la veridicità delle informazioni utilizzate per il funzionamento degli algoritmi o la validità degli algoritmi stessi.

La Direttiva europea (considerando n. 27) valorizza l'uso una massa di informazioni esorbitanti rispetto a quelle tradizionalmente acquisibili: «nell'interesse della prevenzione, dell'indagine e del perseguimento dei reati, è necessario che le Autorità competenti trattino i dati personali raccolti a fini di prevenzione, indagine, accertamento o perseguimento di specifici reati al di là di tale contesto per sviluppare conoscenze delle attività criminali e mettere in collegamento i vari reati».

Viene così esplicitamente riconosciuta la tecnica di indagine definita Criminal Analytics che consente di elaborare sistemi di polizia predittiva che forniscono concreti utili apporti pratici ma può confliggere con le esigenze di tutela della riservatezza (per la mole di dati personali raccolti), e con il divieto di discriminazione (se i fattori di pericolosità vengono connessi a caratteristiche etniche, o religiose o sociali). Inoltre, può produrre degli effetti disfunzionali agli stessi fini mirati perché i suoi sistemi si auto-alimentano coi dati prodotti dal loro stesso utilizzo. Per questa via possono innescarsi circoli viziosi: per esempio, se i controlli e i pattugliamenti della polizia si intensificano nelle zone in cui si prevede maggiore probabilità di commissione dei reati, cresce il tasso di rilevazione dei reati in quelle zone e questo alimenta l'opinione circa la loro pericolosità, ma, per un meccanismo opposto, altre zone rischiano di rimanere o di diventare zone franche per la commissione di reati. In ogni caso l'uso di tali sistemi serve alla prevenzione dei reati attraverso l'intervento attivo della polizia ma non persegue la riduzione del crimine con il contrasto dei fattori criminogeni.

2.4. Allo sviluppo delle indagini con metodi algoritmici affidati alle macchine il Pubblico ministero è autorizzato dall'art. 358 cod. proc. pen. per forme di investigazioni atipiche (cioè non riconducibili nel Titolo V del Libro V) utilizzando l'aggettivo indefinito «ogni» per qualificare l'attività di indagine. Tuttavia, gli art. 357 e 391-sexies, cod. proc. pen. richiedono che l'attività della Polizia giudiziaria sia documentata relativamente a «tutte le attività svolte, comprese quelle dirette alla individuazione delle fonti di prova». In particolare, l'art. 360 cod. proc. pen., richiede che l'indagato sia messo in grado di intervenire con il suo difensore nel caso di accertamenti tecnici non ripetibili.

Avviatosi un procedimento penale, per l'essenziale contraddittorio sulla prova non basta la disponibilità, da parte della difesa, del manuale d'uso del software e dei dati personali dell'imputato. Infatti: gli algoritmi di funzionamento, nella traduzione digitale della teoria scientifica di base, potrebbero aver codificato un processo diverso da quello teorizzato; la conoscenza del codice sorgente offre un indice del modo in cui il sistema è costruito, ma non necessariamente esplicita direttamente il modo in cui esso funziona; se il computo si basa su meccanismi di autoapprendimento, che portano il software a ricavare le regole non da un diagramma impostato dall'esperto ma dall'immagazzinamento di grandi quantità di dati che gli vengono somministrati, lo stesso progettatore del software potrebbe non essere in grado di spiegare compiutamente e, quindi, di giustificare, gli output del modello utilizzato, sicché risulterebbe ardua la validazione ex post del percorso che ha generato il dato che si intende utilizzare come prova. Questa situazione si traduce, allo stato, in una violazione della parità di condizioni che, secondo la giurisprudenza della Corte europea dei diritti dell'uomo si realizza se è inibita la possibilità concreta di contestare e criticare le prove contrarie.

Pertanto, occorre delimitare l'ampiezza della rilevanza probatoria dei risultati degli algoritmi che, per questa ragione, vanno sottoposti ai canoni prescritti dalle norme processuali rispetto alle prove indiziarie.

L'art. 22 del regolamento 2016/679/UE, il cui contenuto è sostanzialmente riprodotto dall'art. 11 della direttiva 2016/680/UE richiede che i provvedimenti siano emessi con coinvolgimento umano nell'itinerario della decisione: a questo scopo «il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico. Il controllo dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza per modificare la decisione (...) e prendere in considerazione tutti i dati pertinenti»

Ma è insufficiente un semplice controllo umano sull'output prodotto dal software anche per la necessità di applicare il canone di cui all'art. 192, comma 2, cod. proc. pen., alla stregua del quale le risultanze derivanti dall'algoritmo andrebbero intese, in ogni caso, come meri indizi, che necessiterebbero di riscontri e di conferme da rinvenirsi negli ulteriori elementi di prova già raccolti nel processo.

Per evitare che nel processo si arrivi a discutere su informazioni offerte da macchine più o meno intelligenti ma non sorrette da adeguata validazione scientifica sarebbe preferibile avvalersi preliminarmente del filtro indicato dall'art. 189 cod. proc.

pen. (che riguarda le prove atipiche o innominate, escluse dal codice precedenti): «Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova». Questo principio dettato espressamente per i processi penali può valere per tutte le procedure giudiziarie e amministrative.

3. Per un uso non discriminatorio della razionalità artificiale

3.1. I sistemi di razionalità artificiale possono essere discriminatori non soltanto per i pregiudizi incorporati nei dati utilizzati ma anche per i pregiudizi metodologici dei loro progettisti.

Inoltre, possono essere affetti da errori tecnici di funzionamento materiale o di altro genere non escludibili a priori e che devono attivare, in una qualche sua graduazione, il principio di precauzione.

La loro segretezza ostacola la verificabilità e la sottoposizione al controllo della comunità scientifica. Pertanto, l'utilizzo di un software in giudizio non dovrebbe ammettersi senza la previa valutazione della sua idoneità: gli algoritmi devono essere pubblici perché i metodi utilizzati per sviluppare inferenze non possono essere criptati e brevettati, come non lo sono gli argomenti che si spendono nei processi. Ulteriori cautele si richiedono se si considera la possibilità, che alcuni sistemi sembrano avere, di individuare autonomamente caratteri distintivi suscettibili di generare (secondo quale ratio?) nuove classi di selezione e raggruppamento di informazioni.

3.2. In realtà, i rischi più gravi che i sistemi di razionalità artificiale presentano sono quelli connessi alle opzioni metodologiche che essi veicolano e che possono concorrere a produrre forme di non-discriminazione nel senso, negativo, di non-discernimento.

3.2.1. Quel che è essenziale considerare è che per il giudizio risulta inadeguato e fuorviante un utilizzo indiscriminato di probabilità statistiche.

Nella logica giudiziale gli algoritmi elaborati dalla razionalità artificiale possono aggiungersi ma non sostituirsi ai metodi inferenziali ordinari considerati dall'art. 192, comma 1, cod. proc. pen.; anzi, devono essere ricondotti nel loro alveo logico. In particolare, i criteri di valutazione della prova indiziaria sono plurimi e indeterminati per cui, specialmente in un processo indiziaro, sarebbe impossibile per un algoritmo stabilire se alcuni indizi possano essere considerati «gravi, precisi e concordanti» ex art. art. 192, comma 2, cod. proc. pen.

Soprattutto non pare che, allo stato attuale di sviluppo dell'intelligenza artificiale, un algoritmo possa comprendere la regola di giudizio fissata dall'art. 533, comma 1, cod. proc. pen. e basata sul principio per il quale per condannare occorre una prova

che vada “oltre ogni ragionevole dubbio”: la elaborazione statistica dei dati per sua struttura non può affrontare la soglia del ragionevole dubbio.

In generale, le elaborazioni statistiche si fondano su generalizzazioni tratte da una base empirica che, quand’anche estesa, costituisce soltanto una parte del tutto. Inoltre, esse sono connesse al contesto di riferimento e una legge statistica – proprio perché ammette eccezioni – non giustifica compiutamente un giudizio di necessità causale, neppure se afferma una elevata probabilità statistica perché la probabilità che rileva nel processo è la probabilità logica ossia la provabilità degli eventi.

In definitiva: il rapporto causale si istituisce sempre fra eventi singoli e sarebbe manifestamente illogico assumere che la spiegazione di un evento storico si possa ottenere soltanto sulla scorta di una propensione generale. La spiegazione causale di un evento è sempre storica: la causa è descritta da condizioni iniziali singolari all’interno di un contesto che ne costituisce il necessario quadro di riferimento. Questa conclusione concorda perfettamente con l’idea che spiegare un evento vuol dire spiegare come e perché l’evento è accaduto ossia raccontarne la storia.

Anche la semplice (a prescindere dalle sue cause) ricostruzione di un evento (di qualcosa che è già accaduto) richiede una analisi del complesso delle plurime circostanze o condizioni singolari che precedono il suo prodursi. Inoltre, non può mai escludersi a priori che l’evento ordinariamente attribuito a una data causa si sia invece realizzato in altro modo, sotto altre circostanze, sulla base di altre condizioni. Ancora: al di là delle semplificatorie schematizzazioni, esistono serie causali anomale rispetto ai modelli conoscitivi ordinari e ai casi più ricorrenti.

In realtà, un evento singolo non è mai completamente spiegabile in tutte le sue caratteristiche, lo è solo per certi suoi limitati aspetti delineati nella forma di una proposizione che li descrive: quali aspetti siano destinati a essere scelti dipenderà dal contesto dell’indagine e dalle norme giuridicamente rilevanti.

In particolare, quando si deve valutare quale sia il grado di probabilità di un singolo evento sorge il problema dell’ambiguità esplicativa, che concerne l’uso delle informazioni statistiche concernenti classi di eventi. Può accadere che si profilino due spiegazioni statistico-induttive entrambe legittime, con premesse che possono essere entrambe vere), di due eventi tra loro incompatibili: per una spiegazione probabilistica con explanans vero che conferisce la quasi-cerchezza di un particolare evento, ci sarà spesso un argomento concorrente, avente la stessa forma probabilistica e con premesse egualmente vere, che rende comunque probabile la non evenienza dell’evento medesimo.

3.2.2. Ogni strumento che fornisce informazioni e ne agevola la organizzazione è un arricchimento ma, al contempo, può ridurre l’attenzione verso le specificità dei casi concreti e quindi può essere fonte di discriminazioni e, comunque, di acrisia.

Il sistema giuridico-tecnologico deve permettere di rendersi conto di come lo strumento giunge a delineare i profili degli individui e come la ipotizzata comprensione delle loro caratteristiche si inserisce sulle decisioni che possono incidere sulla sfera giuridica e personale. Esiste un interesse giuridicamente rilevante a conoscere la logica dello strumento informatico utilizzato. A questo scopo può non essere indi-

spensabile la piena ostensione dell'algoritmo utilizzato, ma necessita almeno poter conoscere come e quali dati circolano tramite l'appartato tecnologico e le sue utilizzazioni.

Inoltre, risulta che parte della logica che governa i processi automatizzati nei sistemi elettronici non è traducibile in linguaggi proposizionali e che alcune logiche autoprodotte dell'intelligenza artificiale non sarebbero al momento comprensibili mediante gli ordinari modelli comunicativi.

Se le cose stanno davvero così, allora il diritto deve irregimentare massimamente il ricorso a sistemi di intelligenza artificiale perché, a queste condizioni, essi non sono utilizzabili nei processi.

In definitiva, non può dimenticarsi che alla base del ragionamento statistico sta la logica induttiva che è indispensabile per la conoscenza, sia nelle forme della comune esperienza che in quelle della ricerca scientifica, ma veicola nella sua struttura il germe della fallacia logica.

La dialettica processuale, che affina l'ars distinguendi, serve anche a svolgere una funzione antidiscriminatoria perché l'ostensione delle ragioni è un antidoto alla cripticità di molti ragionamenti (le discriminazioni esplicite non sono più insidiose di quelle che rimangono implicite o latenti).

3.2.3. Mentre nel caso della polizia predittiva e preventiva l'utilizzo delle macchine intelligenti sembra offrire più svantaggi che vantaggi (purché non incentivi pigritia nell'uso della ragione umana) cautele maggiori si impongono nella fase delle indagini per il rischio di inquinare logicamente le prove acquisibili, fornendo dati indiziari, a volte ambigui, da vagliare attentamente per evitare di inserire nel ragionamento argomenti che possono rivelarsi fuorvianti.

Invece, per quanto prima considerato, non pare che – allo stato attuale dell'arte che le produce – le cosiddette macchine intelligenti possano fornire apporti significativi per sviluppare il ragionamento probatorio nel processo (soprattutto nel processo penale); non tali, comunque, da bilanciare i vari rischi che esse producono.

Questo non significa escludere una loro utilità, ma suggerisce di attendere che la cultura che le accompagna si evolva sino a raggiungere livelli adeguati a un uso sociale e giuridico in cui i vantaggi prevalgano sulle controindicazioni.

Invece, sotto altro versante, sarebbe utile affinare il ricorso a sistemi esperti – quelli che operano secondo una logica pienamente controllata da coloro che li progettano e da chi (studiando e aggiornandosi) si mette in grado di comprenderli – che potrebbero essere proficuamente utilizzati per una verifica della correttezza logica di alcune delle argomentazioni che riguardano la prova dei fatti, individuando fallacie formali nel ragionamento e, anzitutto, le sue illogicità deduttive manifeste.

A tal fine, però, si richiede una purificazione del linguaggio con cui vengono espresse le argomentazioni probatorie in modo da curarne adeguatamente la forma logica e renderle trattabili dai programmi che utilizzano sistemi logici esperti. Anche questo comporta una evoluzione culturale nella formazione dei giuristi.

PERSONA E RETE: LA GARANZIA DEI DIRITTI FONDAMENTALI NELLO SPAZIO CIBERNETICO

Claudia Cipolloni¹

Abstract [IT]: Nel presente contributo, l'A. mira ad analizzare alcune delle conseguenze prodotte dalla rivoluzione tecnologica e, in particolare, dallo sviluppo della "rete", sull'evoluzione del rapporto tra Stato e persona e quindi sul nesso costituzionalistico tra autorità e libertà. A tal proposito, peculiare attenzione è dedicata alle trasformazioni che la "rete" avrebbe prodotto sulla condizione antropologica dell'uomo e, per l'effetto, sulla proiezione giuridica della persona, impattando – spesso in maniera pregiudizievole – sulla garanzia dei diritti e delle libertà fondamentali dell'individuo. Tutto ciò chiama in causa l'esigenza di sottoporre la governance di Internet ad una nuova e diversa sistemazione dei rapporti tra poteri pubblici e privati, con l'obiettivo di orientare la sua dimensione regolatoria verso il riconoscimento del primato della persona umana e dell'anteriorità logica dei suoi diritti e delle sue libertà fondamentali.

Abstract [EN]: In this contribution, the A. aims to analyze some of the consequences produced by the technological revolution and, in particular, by the development of the "network", on the evolution of the relationship between state and person and therefore on the constitutional link between authority and freedom. In this regard, particular attention is dedicated to the transformations that the "network" would have produced on the anthropological condition of man and, as a result, on the legal projection of the person, impacting – often in a prejudicial manner – on the guarantee of rights and freedoms fundamentals of the individual. All this calls into question the need to subject Internet governance to a new and different arrangement of relations between public and private powers, with the aim of orienting its regulatory dimension towards the recognition of the primacy of the human person and of prior art. logic of its fundamental rights and freedoms.

Keywords [IT]: Rete – Stato – persona – costituzionalismo – diritti fondamentali.

Keywords [EN]: Network – State – person – constitutionalism – fundamental rights

Sommario: 1. Riflessioni a partire dall'evoluzione del nesso costituzionalistico tra autorità e libertà al confronto con i nuovi processi globali. – 2. La nascita della *Rete*: le conseguenze della rivoluzione informatica sulla (de)costruzione del rapporto tra Stato e persona. – 2.1. *Segue*: le conseguenze della rivoluzione informatica sulla

¹ Ricercatrice di Diritto Costituzionale presso la Facoltà di Giurisprudenza dell'Università degli Studi di Teramo.

persona. Estensione e frammentazione degli spazi di libertà. – 3. Per una costituzionalizzazione dello spazio cibernetico.

1. Riflessioni a partire dall'evoluzione del nesso costituzionalistico tra autorità e libertà al confronto con i nuovi processi globali

L'indagine sulla relazione tra *Persona* e *Rete* non può che prendere forma a partire da una breve ricostruzione in merito all'evoluzione del rapporto tra *Stato* e *Persona* al confronto con i nuovi processi globali del XXI° secolo, allo scopo di esaminare alcune delle conseguenze prodotte dal fenomeno della globalizzazione tecnologica e, in particolare, dall'avvento di *Internet* sul principio personalista.

Una relazione, quella instauratasi tra autorità e libertà, che, come noto, è stata forgiata dalla dottrina del costituzionalismo moderno (non per caso definita come una “tecnica della libertà contro il potere arbitrario”²) nel senso di funzionalizzare l'esercizio del potere pubblico al riconoscimento e alla protezione dei diritti e delle libertà fondamentali dell'uomo, incastonando la legittimazione dello Stato moderno sulla capacità dell'ordine politico di realizzare la tutela della persona³; per utilizzare una famosa espressione di Giorgio La Pira: “*Lo Stato per la persona e non la persona per lo Stato*: ecco la premessa ineliminabile di uno Stato essenzialmente democratico”⁴. Un principio, quello di funzionalizzazione dell'autorità alla garanzia della libertà, che, più precisamente, si è consolidato con l'evoluzione dello Stato costituzionale di diritto, in seno al quale i diritti inviolabili della persona sono stati ritenuti logicamente e sostanzialmente preordinati agli assetti costitutivi dell'ordinamento statale⁵;

² N. Matteucci, *Organizzazione del potere e libertà. Storia del costituzionalismo moderno*, Bologna, 2016, 20. Analogamente, J.K. Lieberman, *Constitutionalism*, in *The Encyclopedia of Political Thought*, 2014, 730: “*Constitutionalism rejects arbitrary government; it recognizes and respects people's rights despite the contrary will of officials or even popular majorities*”; U.K. Preuss, *Constitutionalism*, in E. Craig (Ed.), *The shorter routledge encyclopedia of philosophy*, London and New York, 2005, 147: “*Constitutionalism comprises a set of ideas, principles and rules, all of which deal with the question of how to develop a political system which excludes as far as possible the chance of arbitrary rule*”.

³ E ciò sul presupposto per il quale la legittimità del potere - e cioè la causa ultima di giustificazione - risiede non già nella sua imposizione *al* corpo sociale ma nella sua accettazione *dal* corpo sociale; in tal senso, emerge la funzione precipua del diritto costituzionale, che è quella di dare alla comunità un ordine politico che sia vissuto intrinsecamente come *giusto* da parte degli uomini e in cui, per primi, siano assicurati il mantenimento della pace, la garanzia dei diritti fondamentali, il rispetto della regola democratica e l'adesione ai comuni valori di solidarietà e di libertà: cfr. G. Lombardi, *Legalità e legittimità* (voce), in *Nov.mo Dig. It.*, vol. IX, Torino, 1963, 577 s.

⁴ On. G. La Pira, *Relazione sui principii relativi ai rapporti civili*, Commissione per la Costituzione, Prima Sottocommissione, disponibile all'indirizzo http://legislature.camera.it/_dati/costituente/lavori/relaz_proposte/I_Sottocommissione/03nc.pdf.

⁵ In proposito, A. Pace, *Problematica delle libertà costituzionali. Lezioni. Parte generale*, II ed., Padova,

un'affermazione di valore che è stata consacrata all'art. 2 della Costituzione là dove la garanzia dei diritti inviolabili dell'uomo si compenetra con il riconoscimento della dimensione "sociale", e non più strettamente individualistica, della persona umana, la cui piena estrinsecazione necessita dell'intreccio di salde legature all'interno delle formazioni sociali⁶.

Più esattamente, la tessitura del nesso costituzionalistico di strumentalità tra potere e persona, e dunque tra autorità e libertà, comporta, da un lato, che l'esercizio dei pubblici poteri, limitato attraverso il diritto nella sua arbitrarietà⁷, assuma una prospettiva di servizio nei confronti della persona⁸ e, dall'altro lato, che la persona riconosca nell'organizzazione statale uno strumento essenziale e privilegiato per la tutela dei suoi diritti e delle sue libertà fondamentali⁹.

1992, 1 ss.; S. Mangiameli, *Il contributo dell'esperienza costituzionale italiana alla dottrina europea*, in A. Pace (a cura di), *Corte costituzionale e processo costituzionale. Nell'esperienza della rivista "Giurisprudenza costituzionale" per il cinquantesimo anniversario*, Milano, 2006, ora in Id., *I diritti costituzionali: dallo Stato ai processi di integrazione*, Torino, 2020, 175 ss.; A. Baldassarre, *Diritti inviolabili* (voce), in *Enc. giur.*, vol. XI, Roma, 1989, 1, anche in Id., *Diritti della persona e valori costituzionali*, Torino, 1997, 1 ss.

⁶ O. Condorelli, *Intervento*, in *La Costituzione della Repubblica nei lavori preparatori della Assemblea Costituente*, Segretariato generale della Camera dei Deputati, Roma, 1970, vol. I, seduta del 15 marzo 1947, 445: "Si svolge tutto un travaglio spirituale dal secolo XIX a questo secolo, che pone in evidenza il carattere sociale e storico dell'uomo: l'individuo non è che una astrazione. La realtà sostanziale (...) non è questo scarnito individuo (...) ma l'uomo sociale. (...) Da ciò un nuovo concetto di libertà (...). La libertà, intesa non più in senso soltanto negativo, ma anche e più in senso positivo, cioè come possibilità data all'uomo di attuare sé stesso, di svolgere la sua personalità".

⁷ Sul principio della limitazione del potere quale elemento strutturale dello Stato di diritto si v. E. Gianfrancesco, *Il principio dello Stato di diritto e l'ordinamento europeo*, in S. Mangiameli (a cura di), *L'ordinamento europeo. I principi dell'Unione*, Milano, 2006, 235 ss.

⁸ N. Matteucci, *Costituzionalismo*, in *Enciclopedia delle Scienze Sociali*, vol. II, Roma, 1992, 523, il quale osserva: "il costituzionalismo è la tecnica delle libertà: è cioè, quella tecnica giuridica attraverso la quale ai cittadini viene assicurato l'esercizio dei loro diritti individuali e, nel contempo, lo Stato è posto nella condizione di non poterli violare. Se le tecniche variano secondo i tempi e le tradizioni di ciascun paese, l'ideale delle libertà del cittadino resta il fine ultimo in vista del quale queste tecniche vengono preordinate e organizzate". Nondimeno, appare utile riflettere sulla considerazione che ogni ordine, fondato sulla regolamentazione di un gruppo umano, "non è una semplice espressione di dominio, ma uno strumento posto al servizio dei soggetti": così si esprime S. Mangiameli, *Ordinamento giuridico*, in Id. (a cura di), *Dizionario di Diritto costituzionale*, Milano, 2008, 97 ss., ora anche in Id., *I diritti costituzionali: dallo Stato ai processi di integrazione*, cit., 1 ss. Sempre sul tema della limitazione, C.-H. McIlwain, *Costituzionalismo antico e moderno*, Bologna, 1990, 44: "[...] in tutte le sue fasi successive il costituzionalismo ha una qualità essenziale: è una limitazione legale del governo, è l'antitesi del governo arbitrario [...] il più antico, il più persistente e più duraturo dei caratteri essenziali del vero costituzionalismo resta ancora quello che era all'inizio, la limitazione del governo mercè il diritto".

⁹ U. Allegretti, *I diritti fondamentali fra tradizione statale e nuovi livelli di potere*, in P. Barcellona, A. Carrino (a cura di), *I diritti umani tra politica filosofia e storia*, Tomo II, *I diritti umani nella costruzione del nuovo ordine mondiale*, Napoli, 2003, 9: "nell'esperienza della modernità, i diritti fondamentali sono, per il loro riconoscimento e protezione, strettamente associati allo stato", e più nel dettaglio, alla sua dimensione organizzativa, "in quanto cioè trovano nell'organizzazione, e dunque nel potere statale, lo strumento, uno strumento essenziale, per tutto ciò di cui hanno bisogno". Analogamente, A. D'Atena, *Le stagioni del costituzionalismo nel suo rapporto con la tutela dei diritti fondamentali*, in *Dir. soc.*, n. 1/2017, 8 s.: "La prima tecnica di tutela di cui il costituzionalismo fa uso per garantire i diritti fondamentali è quella della loro copertura organizzativa. (...) Parlando,

Al contempo, non potrà sfuggire l'osservazione che proprio "l'affermazione dei diritti (...) [sia] risultata storicamente uno dei veicoli principali di rafforzamento e di legittimazione della sovranità"¹⁰ al punto da ritenersi che "oltre alla determinazione territoriale del diritto, lo Stato ha prodotto di fatto anche una determinazione territoriale dei diritti"¹¹.

Tuttavia, non v'è chi non veda come la predetta raffigurazione del rapporto tra autorità e libertà rischia di essere, se non proprio incrinata, quantomeno sottoposta a dura prova dall'emergere dei nuovi processi globali di interdipendenza economico-finanziaria, scaturiti a partire dagli anni Ottanta del secolo scorso, e caratterizzati dalla predominanza del mercato sulla politica e della ragione economica sul potere decisionale degli Stati.

La globalizzazione, infatti, rappresenterebbe "una sorta di fuoriuscita dell'economia da questo contenitore statale e una tendenziale affermazione della sua autonomia e autosufficienza rispetto al processo politico. I confini territoriali non valgono più per un'economia che tende ad essere «leggera», svincolandosi dal territorio, e che detiene le leve per condizionare le società in senso globale (...). Parallelamente, l'economia diventa veicolo di significativi mutamenti nell'area della sovranità e disegna nuovi percorsi per le istituzioni giuridiche"¹².

Quella globale, dunque, è una *rivoluzione spaziale* che ha impresso una più evidente trasformazione sulle categorie politico-giuridiche della statualità, innescando microprocessi di "denazionalizzazione" di alcune componenti e capacità che erano state pensate e costruite come esclusivamente nazionali¹³.

Infatti, secondo una delle rappresentazioni più accreditate, la globalizzazione avrebbe innescato un "processo di trasferimento di poteri dagli stati ai mercati"¹⁴, orien-

nel contesto del costituzionalismo, di copertura organizzativa, si fa riferimento alla circostanza che l'elenco dei diritti da solo non è in grado di conseguire gli scopi in funzione dei quali è stato concepito. A questo fine è indispensabile una "certa" organizzazione del potere statale". Osserva ancora M. Michetti, *Territorio e organizzazione del potere. Livelli di governo e legittimità dello Stato*, Torino, 2021, 91: l'esperienza storica del costituzionalismo si consolida nell'incedere di un fenomeno che muove "attorno all'idea della limitazione del potere, che leviga costantemente il concetto di sovranità e sviluppa un pensiero anti-assolutistico di potere, affidandone la distribuzione alle Carte costituzionali ove per la prima volta al principio monarchico viene contrapposto il principio democratico".

¹⁰ C. Galli, *Spazi politici. L'età moderna e l'età globale*, Bologna, 2001, 80.

¹¹ *Ibidem*.

¹² M.R. Ferrarese, *Le istituzioni della globalizzazione. Diritto e diritti nella società transnazionale*, Bologna, 2000, 8.

¹³ Cfr. S. Sassen, *Territorio, autorità, diritti*, Milano, 2008, 201 ss. Analogamente, U. Beck, *Che cos'è la globalizzazione. Rischi e prospettive della società planetaria*, trad. it., Roma, 1999, 30, sostiene che il processo di globalizzazione può anzitutto identificarsi con quello di "de-nazionalizzazione, ovvero l'erosione, ma anche la possibile trasformazione dello Stato nazionale in uno Stato transnazionale".

¹⁴ Così M.R. Ferrarese, *Le istituzioni della globalizzazione*, cit., 7. V. Roppo, *Verso un mondo globalizzato: trasformazioni economiche, mutamenti sociali, risposte politiche*, in *Pol. dir.*, n. 3/2001, 515 s.: "Fenomeni di internazionalizzazione e interdipendenza planetaria dei processi economici si erano avviati già da prima: quanto meno da Bretton Woods (1944). Ma la globalizzazione che si avvia da metà degli anni '70 segna un salto di qualità, l'affermarsi di un nuovo paradigma che trasforma

tando una collocazione del politico al di fuori delle sedi istituzionali, in gran parte statali, tradizionalmente deputate all'esercizio del potere decisionale; un processo di indebolimento degli Stati che avrebbe replicato i suoi effetti anche sull'attività di produzione normativa laddove, a dispetto del monopolio sul diritto rivendicato dalle autorità statali, si è invece registrata una tendenza sempre più marcata verso la privatizzazione dei meccanismi di produzione giuridica e verso la creazione di ordini spontanei di (de)regolazione prevalentemente ispirati alla tecnica del *soft law*.

Una condizione sulla quale avrebbe esercitato un impatto decisivo l'evoluzione tecnologica e, più oltre, l'accresciuta digitalizzazione delle nuove tecnologie di informazione e di comunicazione che, mediante una decompressione delle coordinate spazio-temporali, avrebbero decostruito il *nomos* della terra proiettando l'autorità statale entro la dimensione reticolare dello *spazio cibernetico* e scardinando quella unità di ordinamento e di localizzazione sulla base della quale è stata elaborata la concezione dello Stato moderno.

2. La nascita della Rete: le conseguenze della rivoluzione informatica sulla (de)costruzione del rapporto tra Stato e persona

Se “lo spazio-territorio ha inaugurato un tempo-prima e un tempo-dopo la fondazione, la delimitazione, la recinzione, il confine tra esterno e interno; nello spazio-movimento del cibernazio, il tempo è scandito dall'accelerazione e dall'ubiquità dei contatti, ormai tutti all'interno dei circuiti propri dello spazio virtuale”¹⁵, recando con sé l'annullamento, in uno con la dimensione spaziale, dello stesso elemento temporale; perdendo di ogni consistenza la distinzione tra “vicino” e “lontano”, tra “presente” e “passato”; invocandosi il nuovo e diverso imperativo del “qui” e “ora”¹⁶. Si comprende perciò come il *medium* della rivoluzione spaziale dell'età globale¹⁷, che è per definizione una rivoluzione dello sconfinamento, della de-spazializzazio-

radicalmente gli assetti precedenti: perché gli sviluppi innescati da Bretton Woods avevano per protagonisti le autorità politiche nazionali, mentre dopo Rambouillet la spinta propulsiva e la direzione di marcia vengono da forze microeconomiche: dagli «spiriti» (o dai «demoni») dell'impresa e del mercato”.

¹⁵ A.C. Amato Mangiameli, *Un nuovo spazio. Il cyberspace*, in Id., M.N. Campagnoli, *Strategie digitali#diritto_ educazione_ tecnologie*, Torino, 2020, 10.

¹⁶ Sulla profondità del cambiamento temporale innescato dalla globalizzazione si v. ancora M.R. Ferrarese, *Il diritto al presente. Globalizzazione e tempo delle istituzioni*, Bologna, 2002, la quale, in estrema sintesi, afferma che “questo cambiamento temporale si può riassumere in una presenza ipertrofica del presente” (9).

¹⁷ Cfr. L. Gallino, *Sui rapporti tra la globalizzazione e lo sviluppo della rete*, in *Jura Gentium*, 2005, 1, a parere del quale “la Rete è diventata il principale strumento della globalizzazione”.

ne, ma anche, e soprattutto, della de-regolazione¹⁸, possa essere pianamente identificato con la rivoluzione informatica del XX secolo; “[l]a *rete telematica* è il simbolo estremo dell’alleanza tecno-economica: spazio artificiale senza confini, non luogo, dove la volontà del profitto, *sradicata e de-territorializzata*, si esprime oltre gli Stati e oltre il diritto degli Stati. Si determina così un divario, una ‘sfasatura’, di estensione: *tecnica ed economia non sono co-estensive a politica e diritto*: quelle, indefinitamente spaziali; questi, definitamente territoriali”¹⁹.

Difatti, la rivoluzione tecnologica di *Internet* non ha funzionato soltanto come acceleratore storico dei processi di dislocazione della politica ma, a ben riflettere, ha costituito essa stessa il perno di quella virtualizzazione sulla quale si è innestato il tronco del processo di globalizzazione, sì da ritenersi che la “rete” possa essere definita e tematizzata a pieno titolo come lo “strumento”²⁰, il “catalizzatore”²¹ o, addirittura, l’“essenza”²² della globalizzazione.

L’evidenza di una tale considerazione diventa tangibile già solo riflettendo sulle condizioni di pensabilità della rivoluzione internettiana che, come noto, è una rivoluzione prodottasi nella sfera de-territorializzata del *cyberspazio*²³; una sfera che è il *non-luogo* per antonomasia, avulso da ogni radicamento territoriale²⁴: “[q]ualsiasi cosa che si muova a una velocità vicina a quella dei segnali elettronici è praticamente libera da vincoli connessi al territorio all’interno del quale ha avuto origine, verso il quale si dirige, attraverso il quale passa”²⁵.

¹⁸ Scriveva N. Poulantzas, *L'état, le pouvoir, le socialisme*, Paris, 1978, trad. it. *Il potere nella società contemporanea*, Roma, 1979, in un passo citato da M. Castells, *Il potere delle identità*, Milano, 2014, 325: “La specificità dello Stato capitalista consiste nel fatto che esso assorbe il tempo e lo spazio sociali, determina le metriche spazio-temporali e monopolizza l’organizzazione del tempo e dello spazio, facendoli diventare, attraverso la sua azione, reti di dominio e di potere”. Obietta invece Castells che oggi lo Stato ha perso l’esercizio del potere di controllo sullo spazio e sul tempo, eluso dai flussi globali di capitali e merci così come dalla tecnologia, dalla comunicazione e dall’informazione (325).

¹⁹ N. Irti, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2006, 135.

²⁰ N. Di Nardo, A.M. Zocchi, *Internet. Storia, tecnica, sociologia*, Torino, 2004, 195.

²¹ P. Costanzo, *Il fattore tecnologico e le sue conseguenze*, in *Rass. parl.*, n. 1/2012, 811.

²² A. Baldassarre, *Globalizzazione contro democrazia*, Roma-Bari, 2002, 6, si da ritenere che la rivoluzione informatica abbia comportato un mutamento qualitativo dei fenomeni di integrazione e interdipendenza nel più ampio processo di globalizzazione.

²³ Tra i primi a confortare una rappresentazione del *cyberspazio* come di un “luogo”, seppure autonomo e distinto rispetto a quello reale, sono stati John Perry Barlow e Mitchell Kapor in un manifesto pubblicato nel 1990 per la fondazione dell’Electronic Frontier Foundation e intitolato “*Accross the Electronic Frontier*”, ove si legge che “*Over the last 50 years, the people of the developed world have begun to cross into a landscape unlike any which humanity has experienced before. It is a region without physical shape or form. It exists, like a standing wave, in the vast web of our electronic communication systems. It consists of electron states, microwaves, magnetic fields, light pulses and thought itself*”. Il manifesto è disponibile all’indirizzo <https://www EFF.org/it/pages/across-electronic-frontier>.

²⁴ Come meglio puntualizzato da N. Irti, *Norma e luoghi. Problemi di geo-diritto*, cit., 61, la rete telematica “costituisce e determina il proprio ‘spazio’: lo spazio telematico, che è un non-luogo, poiché i ‘luoghi’ appartengono a terra mare aria”.

²⁵ Z. Bauman, *Dentro la globalizzazione. Le conseguenze sulle persone*, Bari-Roma, 2020, 63.

Inoltre, accanto al profilo della de-spazializzazione emerge quello della de-centralizzazione, poiché la “rete” - anche attraverso l'utilizzo della tecnica di commutazione di pacchetto per la circolazione dei dati - si configura come una struttura reticolare acefala²⁶ che non conosce gerarchie di scala, nella quale tutti i nodi della rete telematica appaiono tra loro interconnessi secondo le logiche proprie di una scalarità orizzontale²⁷.

Ciò che ne è derivato è stata l'esaltazione della natura profondamente libertaria di *Internet*, associandosi alla sua architettura de-spazializzata e de-centralizzata l'idea della “rete” come di un ordine spontaneo, non sottoponibile a un processo di eteronormazione regolato dalle autorità statali; un'idea vieppiù confortata dalla presunzione di una supposta incapacità degli Stati di regolare un fenomeno che, come

²⁶ Ad aggettivare la struttura di *Internet* come acentrica e acefala è P. Costanzo, *Internet*, voce in *Dig. Disc. Pubbl.*, Torino, 2000, 348.

²⁷ Una proprietà, quella della de-centralizzazione, che appare essere connaturata all'origine del fenomeno internettiano, collocabile al tempo della Guerra Fredda, quando il Dipartimento di Difesa americano commissionò un progetto di ricerca con l'obiettivo di fronteggiare il primato tecnico-scientifico nel frattempo conquistato dall'Unione Sovietica dopo il lancio del primo satellite artificiale della storia, lo *Sputnik I*, avvenuto il 4 ottobre 1957. Nello specifico, gli studi condotti dall'agenzia *Arpa* (Advanced Research Projects Agency) - istituita nel 1958 dal Presidente Eisenhower - mossero nella direzione di creare una più ampia rete di comunicazione (*Arpanet*), articolata al suo interno in una pluralità di nodi, che avrebbe dovuto garantire una rapida interconnessione tra le risorse informatiche e agevolare così la trasmissione dei progressi sperimentati nel campo della ricerca scientifica. Altra parte della letteratura affaccia invece l'ipotesi che la nascita della “rete” sia stata determinata dalla preminente necessità di garantire la stabilità delle comunicazioni tra autorità politiche e militari degli Stati Uniti in caso di attacco nucleare. In proposito, M. Calvo, F. Ciotti, G. Roncaglia, M.A. Zela, *Internet 2000. Manuale per l'uso della rete*, Roma-Bari, 2000; N. Di Nardo, A.M. Zocchi, *Internet. Storia, tecnica, sociologia*, Torino, 2004. Le precondizioni della nuova configurazione topologica della rete, elaborate sugli studi per primo condotti da *Paul Baran*, furono dunque individuate nell'assenza di ogni autorità centrale e nella “ridondanza della connessione al nodo adiacente” (N. Di Nardo, A.M. Zocchi, *Internet. Storia, tecnica, sociologia*, cit., 27): per far questo, era necessario che “ogni nodo potesse raggiungere qualsiasi altro con una molteplicità di percorsi” e avesse “conseguentemente l'autorità di originare, scambiare e ricevere messaggi in modo autonomo” (N. Di Nardo, A.M. Zocchi, *Internet. Storia, tecnica, sociologia*, cit., 27), applicando un concetto di rete a commutazione di pacchetto (*packet data switching*) affatto diverso da quello della commutazione di circuito, prevalentemente impiegato per la rete telefonica. Un metodo di trasmissione che, come spiega B. Carotti, *Il sistema di governo di Internet*, Milano, 2016, 3, è “in grado di scomporre un'informazione in blocchi più piccoli, spedirli separatamente e, quindi, assemblarli nuovamente nel punto di destinazione. La commutazione ha consentito di individuare caso per caso il ‘tragitto’ più appropriato: i canali di comunicazione non dovevano essere stabiliti *a priori*, ma scelti sul momento, in base alla disponibilità”. Corollario del progetto sviluppato con la creazione della rete *Arpanet* fu, intorno alla metà degli anni Settanta, l'idea di un sistema di reti interconnesse, identificato con l'acronimo di *Internet* (*Interconnected Network*), che avrebbe dovuto assicurare un collegamento fra più reti di elaboratori e non solo tra i nodi dell'unica rete allora esistente (cfr. N. Di Nardo, A.M. Zocchi, *Internet. Storia, tecnica, sociologia*, cit., 40 ss.). Più esattamente, *Arpanet* venne impiegata quale spina dorsale della nuova rete *Internet*, ufficialmente datata al primo gennaio 1983, e concepita alla stregua di un sistema unico di reti tra loro interconnesse grazie all'utilizzo del protocollo TCP/IP (*Transmission Control Protocol - Internet Protocol*) quale architettura privilegiata di comunicazione. Sul punto, e per rilievi di maggiore tecnicità, si rinvia, oltre ai già citati M. Calvo, F. Ciotti, G. Roncaglia, M.A. Zela, *Internet 2000. Manuale per l'uso della rete*, cit. e N. Di Nardo, A.M. Zocchi, *Internet. Storia, tecnica, sociologia*, cit., anche a G. Corasaniti, *Diritti nella rete. Valori umani, regole, interazione tecnologica globale*, Milano, 2006; A. Oddenino, *La governance di Internet fra autoregolazione, sovranità statale e diritto internazionale*, Torino, 2008, 23 ss.

quello cibernetico, è eretto sul mito della extra-territorialità, suscettibile di replicarsi al di là dei confini normativi e giurisdizionali degli Stati²⁸.

Una teoria che, agli inizi degli anni '90, è stata professata con particolare vigore anche da *John Perry Barlow* (membro e fondatore dell'EFF) il quale, nella *Dichiarazione sull'Indipendenza del Cyberspazio*, sostenne la natura intrinsecamente anarcoide della "rete", rivendicando la sua indipendenza rispetto ai "governi del mondo industriale, stanchi giganti di carne e di acciaio"²⁹.

Dunque, la percezione della "rete" come di un ordine spontaneo avrebbe fatto emergere, soprattutto alle origini del fenomeno internettiano, una certa difficoltà per gli Stati di governare lo spazio cibernetico, la cui regolazione è risultata prevalentemente ad appannaggio dei gestori delle piattaforme digitali i quali hanno finito con il concentrare nelle loro sacche di potere l'esercizio di molte funzioni pubblicistiche e para-costituzionali, connesse all'esercizio delle libertà fondamentali degli utenti e ai loro limiti. E questo non solo con riferimento all'attività di regolazione ma anche al potere di sorveglianza, a quello censorio o all'amministrazione della giustizia³⁰,

²⁸ Così come osservato da A. Soro, *Persone in rete. I dati tra poteri e diritti*, Roma, 2018, 17: "l'intervento statale è reso più complesso dalla capacità delle nuove tecnologie di scardinarne i presupposti essenziali: in primo luogo la territorialità, quale criterio di competenza e applicazione della legge. È infatti evidente come le coordinate tradizionali dei regimi giuridici – in particolare l'applicazione della legge su base territoriale e il suo riflesso sulla giurisdizione – stentino ad affermarsi ancora rispetto a una dimensione, quale quella digitale, dematerializzata e quindi capace di prescindere dai confini degli Stati e delle relative giurisdizioni".

²⁹ Così J.P. Barlow, *A Declaration of the Independence of Cyberspace*, disponibile all'indirizzo <https://www.eff.org/it/cyberspace-independence>: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather".

³⁰ Paradigmatico è l'esempio inerente alla costituzione del *Facebook's Oversight Board*, ossia il Comitato per il controllo istituito da *Facebook* nel settembre del 2019 ed entrato nell'esercizio delle sue funzioni nel marzo del 2020. Come affermato nell'atto costitutivo, lo scopo del Comitato per il controllo è quello di "proteggere la libertà di espressione prendendo decisioni autonome e basate su principi determinati riguardo contenuti importanti ed emettendo pareri consultivi relativi alle normative sui contenuti di Facebook", con particolare riferimento alla supervisione sulle attività di moderazione dei contenuti o sospensione e disabilitazione di *account* effettuate da *Facebook*. Per quanto formazioni di tal genere siano state apprezzate quali "forme embrionali di garanzia", preordinate al consolidamento, nel mare della "rete", di "isole di legalità autogarantita" (G. Azzariti, *Costituzionalismo e crisi dello Stato-Nazione. Le garanzie possibili nello spazio globalizzato*, in AA.VV., *Costituzionalismo e globalizzazione. Atti del XXVII Convegno annuale. Salerno, 22-24 novembre 2012*, Napoli, 2014, 153) non può tacersi della considerazione, pure ampiamente sottolineata in dottrina, per la quale un simile "processo di privatizzazione della giustizia digitale" (O. Pollicino, *L'autunno caldo della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *federalismi.it*, n. 19/2019, 11), svincolato dal controllo statale, implicherebbe la devoluzione, in capo ad organismi privi di ogni legittimazione democratica, del potere di effettuare delicate operazioni di bilanciamento tra i diritti fondamentali in gioco che in uno Stato di diritto sono invece rimesse agli organi legislativi - stabilmente inseriti nel circuito democratico-rappresentativo - e alle autorità giurisdizionali, nel rispetto del principio di legalità. In argomento si v. più diffusamente A. Iannotti della Valle, *La giurisdizione privata nel mondo digitale al tempo della crisi della sovranità: il "modello" dell'Oversight Board di Facebook*, in *www.federalismi.it*, n. 26/2021, 144 ss.; G. Cerrina Feroni, *L'Oversight Board di Facebook: il controllo dei contenuti tra procedure private e norme pubbliche*, 16 febbraio 2021, disponibile all'indirizzo <file:///C:/Users/Utente/Downloads/GarantePrivacy-9542545-1.4.pdf>. Criticità al modello di cui si

erodendo alcuni tra i compiti e le funzioni statuali tradizionalmente preordinati alla tutela della persona.

In questa prospettiva, può cogliersi agevolmente la trasformazione che la “rete” ha prodotto sulla concezione dello Stato come di un aggregato monolitico e centripeto di potere, disarticolando quella convergenza tra *Ordnung* e *Ortung* sulla quale si è innestato il dogma della sovranità territoriale.

Piuttosto, sembra emergere una certa subalternità degli Stati al confronto con una oligarchia di organismi internazionali specialistici e di altri attori privati (fra i quali appunto le *Big Tech*) che, *in luogo* delle autorità statali e al di fuori di ogni processo decisionale democratico, oggi presiedono alla regolazione e al funzionamento delle piattaforme digitali, dando origine a un fenomeno di privatizzazione della *governance* di *Internet* che rischia di arrecare un più serio e grave pregiudizio alla garanzia dei diritti fondamentali della persona.

Non è un caso che i *social media*, e più in generale le *Big Tech*, siano da più parti ricondotti entro la categoria dei *poteri privati* e cioè di quel potere “che è *privato* per quanto concerne la sua fonte (...) e i soggetti cui spetta, ma che, proprio all’atto del suo esercizio si realizza con quelle forme di coerenza e di autorità avvicinati sostanzialmente alle categorie amministrativistiche in senso lato che sono proprie dei *poteri di diritto pubblico*”³¹.

Difatti, i nuovi poteri privati intrattengono con gli utenti (e in particolar modo con le persone fisiche) rapporti fortemente asimmetrici, per cui “le parti non sono in quella posizione di simmetria che appare (...) quale giustificazione costante dell’autonomia privata, ma l’una si trova per ragioni economiche e sociali, in una *posizione dominante* mentre l’altra è in posizione *debole*”³².

2.1. Segue: le conseguenze della rivoluzione informatica sulla persona. Estensione e frammentazione degli spazi di libertà

Alla luce di quanto sinora illustrato, appare evidente che la *persona* costituisce l’altro polo di riferimento nella relazione tra autorità e libertà sulla quale si sono prodotte le trasformazioni più vistose conseguenti al processo di globalizzazione cibernetica; difatti, la rivoluzione informatica avrebbe sortito i propri effetti anche

discorre, con particolare riferimento all’istituzione del *Facebook’s Oversight Board*, sono espresse da M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, Relazione tenuta in occasione del Convegno annuale dell’Associazione “Gruppo di Pisa” - Evento web, *Il diritto costituzionale e le sfide dell’innovazione tecnologica*, Genova, 18-19 giugno 2021, in *La Rivista “Gruppo di Pisa”*, n. 2/2021, 174 ss., il quale afferma che “l’istituzione e il concreto funzionamento dell’Oversight Board vorrebbe condurre all’evaporazione dei diritti costituzionali statali e al superamento dei delicati bilanciamenti consegnati alle Costituzioni democratiche figlie del costituzionalismo” (176).

³¹ G. Lombardi, *Potere privato e diritti fondamentali*, Torino, 1970, 87. In argomento, si v. più di recente C. Bologna, *Libertà di espressione e riservatezza «nella rete»? Alcune osservazioni sul mercato delle idee nell’agorà digitale*, in *La Rivista Gruppo di Pisa*, fascicolo speciale n. 3/2021

³² G. Lombardi, *Potere privato e diritti fondamentali*, cit., 86 s.

sulla condizione antropologica dell'uomo³³, investendo per intero la sfera psichica e sociale dell'individuo³⁴, e, non da ultimo, il suo orizzonte spaziale³⁵, che oggi si staglia su una dimensione *altrove* rispetto a quella concezione *naturalistica* attraverso la quale l'uomo ha configurato lo spazio della sua esistenza come un ambito naturale e fisico delimitato da confini³⁶; d'altronde, “[p]er il fatto che abitiamo un mondo in ogni sua parte tecnicamente organizzato, la tecnica non è più oggetto di una nostra scelta, ma è il nostro ambiente, dove fini e mezzi, scopi e ideazioni, condotte, azioni e passioni, persino sogni e desideri sono tecnicamente articolati e hanno bisogno della tecnica per esprimersi”³⁷.

Mutamenti che, per conseguenza, si sono riverberati anche sulla proiezione giuridica della persona e, in particolare, sul perimetro costituzionale del principio personalista, realizzando sia una “estensione” sia una “frammentazione” degli spazi di libertà. Dal primo punto di vista, è innegabile che la “rete” sia diventata per l'individuo un luogo di esperienza e di interazione sociale³⁸, una vera e propria “tecnologia di libertà”³⁹ che dischiude nuovi spazi relazionali entro i quali l'individuo esprime la

³³ D'altro canto, e a conferma della poliedricità - anche sociologica - del fenomeno, la globalizzazione cibernetica è stata intesa come un “processo di estensione ‘globale’ delle relazioni sociali fra gli esseri umani, tale da coprire lo spazio territoriale e demografico dell'intero pianeta” (secondo la definizione di D. Zolo, *Globalizzazione. Una mappa dei problemi*, Roma-Bari, 2004, 3); un “processo sociale - fortemente influenzato dallo sviluppo tecnologico, dalla crescente rapidità dei trasporti e dalla ‘rivoluzione informatica’ - che ha dato vita a una vera e propria rete mondiale di connessioni spaziali e di interdipendenze funzionali” (D. Zolo, *Globalizzazione*, cit., 4), mettendo in contatto fra loro un numero sempre crescente di persone e di eventi; è in questo senso che “si parla di ‘contrazione’ della dimensione spaziale e di quella temporale come una delle *human consequences* della globalizzazione soggettivamente più percepite” (D. Zolo, *Globalizzazione*, cit., 4).

³⁴ Cfr. M. McLuhan, *Gli strumenti del comunicare. Mass media e società moderna*, trad. di E. Capriolo (titolo originale *Understanding Media*), Milano, 2002, 9: “[n]elle ere della meccanica, avevamo operato un'estensione del nostro corpo in senso spaziale. Oggi, dopo oltre un secolo di impiego tecnologico dell'elettricità, abbiamo esteso il nostro stesso sistema nervoso centrale in un abbraccio globale che, almeno per quanto concerne il nostro pianeta, abolisce tanto il tempo quanto lo spazio”.

³⁵ Rifletteva anzitempo C. Schmitt, *Terra e mare. Una riflessione sulla storia del mondo*, trad. di G. Gurisatti (titolo originale *Land und Meer. Eine weltgeschichtliche Betrachtung*), II ed., Milano, 2002, 59: “[o]gni volta che, grazie a una nuova avanzata delle forze storiche e alla liberazione di nuove energie, nuove terre e nuovi mari fanno il loro ingresso nell'orizzonte della coscienza collettiva umana, mutano anche gli spazi dell'esistenza storica. Nascono allora nuovi parametri e nuove dimensioni dell'attività storico-politica, nuove scienze, nuovi ordinamenti, una nuova vita di popoli nuovi o rinati. Questo ampliamento può essere talmente profondo e sorprendente da comportare il mutamento non solo delle misure e dei parametri, non solo dell'orizzonte esterno degli uomini, ma anche della struttura del concetto stesso di spazio. Allora si può parlare di una rivoluzione spaziale”.

³⁶ Cfr. A. Baldassarre, *Globalizzazione contro democrazia*, Roma-Bari, 2002, 10 s.

³⁷ U. Galimberti, *Psiche e techne. L'uomo nell'età della tecnica*, Milano, 2002, 34.

³⁸ Sebbene U. Galimberti, *Psiche e techne*, cit., 45, avverta che i nuovi mezzi di comunicazione abbiano esonerato l'uomo da un'esperienza diretta e personale del mondo, modificando “il nostro *modo di fare esperienza*: non più in contatto con il mondo, ma con la rappresentazione mediatica del mondo che rende vicino il lontano, presente l'assente, disponibile quello che altrimenti sarebbe indisponibile”.

³⁹ C. Caruso, *L'individuo nella rete: i diritti della persona al tempo di internet*, in *Forum di quad. cost.*, 28 aprile 2013, 2.

propria personalità⁴⁰; è in quest’ottica, per esempio, che le comunità di utenti aggregate nei *social networks* sono state da più parti considerate alla stregua di una formazione sociale ai sensi dell’art. 2 Cost⁴¹.

Vero è che la tessitura di “reti sociali”⁴² ha amplificato le possibilità di azione organizzata degli individui, i quali si servono della tecnologia per perorare e diffondere l’eco di alcune questioni che, oltre lo schermo della piazza virtuale, si materializzano nella piazza reale attraverso manifestazioni pubbliche di massa⁴³: senz’altro nota è la stagione delle “primavere arabe” ma, ancor prima di essa, è opportuno ricordare la grande manifestazione contro i vertici dell’Organizzazione mondiale del commercio svoltasi a Seattle nel 1999 là dove, per la prima volta, si è avuto contezza del ruolo delle reti sociali quale fattore collante della partecipazione *online* e *offline*⁴⁴.

È evidente, perciò, come la “rete” abbia altresì costituito uno strumento di rinnovamento della partecipazione democratica della società civile alla vita politica nazionale, al punto che espressioni quali democrazia “digitale” o democrazia “elettronica” sono utilizzate sempre più spesso (seppure impropriamente) come sinonimi di democrazia “diretta”⁴⁵ o “democrazia di massa”⁴⁶. Ciò avrebbe senz’altro contribuito ad alimentare quella crisi di legittimazione che ormai da tempo investe i partiti politici e le istituzioni rappresentative, incapaci di assolvere a quella funzione di “cerniera”⁴⁷ tra elettori ed eletti che i Costituenti hanno invece demandato agli

⁴⁰ Cfr. A. Soro, *Persone in rete. I dati tra poteri e diritti*, cit., 26, il quale obietta che *Internet* da “mezzo qual era, al pari di ogni tecnologia, è divenuto la nuova dimensione entro cui si svolge la personalità di ciascuno: è la realtà in cui si esercitano e si negano i diritti, si dispiegano le libertà e responsabilità”.

⁴¹ Tale è la prospettiva di indagine suggerita, tra gli altri, da P. Passaglia, *Le formazioni sociali e Internet*, in T. E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, Milano, 2017, 50 ss. Parimenti P. Marsocci, *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in *Rivista AIC*, n. 1/2015, 16, la quale afferma: “Non c’è dubbio allora che il web abbia enormemente agevolato la nascita, l’azione e il ricambio continuo di formazioni sociali (...). In particolare, i *social network* – reti sociali *on line* costituite da gruppi di persone connesse tra loro da diversi legami sociali – sono a mio parere un fenomeno inquadrabile nella categoria tradizionale delle formazioni sociali (...)”.

⁴² L’espressione è di S. Rodotà, *Una rete per i diritti*, in Id., *Il diritto di avere diritti*, Roma-Bari, 2020, 381.

⁴³ Cfr. S. Rodotà, *Una rete per i diritti*, cit., 381 ss.

⁴⁴ *Internet* è stato altrimenti definito da M. Castells, *Il potere delle identità*, cit., 166 ss., come un “agorà permanente del movimento”; “una nuova forma sociale di interazione, mobilitazione e presa delle decisioni. È una nuova cultura politica - networking significa assenza di centro e, quindi, di autorità centrale – che implica la relazione istantanea tra il locale e il globale, tale per cui il movimento può pensare localmente, conservando la propria identità e i propri interessi, e agire globalmente, laddove sono le fonti del potere. (...) In ogni caso, non si tratta di una rete puramente elettronica. La rete collega le dimensioni locali e i luoghi che diventano siti simbolici di eventi e controeventi”.

⁴⁵ In proposito, si v. P. Costanzo, *La «democrazia digitale» (precauzioni per l’uso)*, in *Dir. pubbl.*, n. 1/2019, 71 ss., spec. nota 1.

⁴⁶ Sul tema, V. Frosini, *La democrazia nel XXI secolo*, Macerata, 2010, 23 ss.

⁴⁷ Cfr. F. Pizzetti, *Partiti politici e nuove tecnologie (Intervento in occasione del XXIII Convegno annuale dell’Associazione Italiana dei Costituzionalisti – Partiti politici e società civile a sessant’anni dall’entrata in vigore della Costituzione – Alessandria, 18 ottobre 2008)*, in *federalismi.it*, n. 21/2008,

strumenti di mediazione partitica e politica⁴⁸.

In questa prospettiva, assume un rilievo nodale la questione sottesa alla portata espansiva che le nuove tecnologie digitali avrebbero dispiegato sulla libertà di manifestazione del pensiero⁴⁹ e ciò sulla base della comune osservazione che *Internet* costituisce uno strumento privilegiato ai fini della più ampia e libera circolazione del pensiero⁵⁰, empiricamente apprezzabile non solo sotto il profilo della disponibilità di nuovi spazi funzionali alla *diffusione* della libertà di espressione ma anche all'esercizio della *libertà di informazione*⁵¹, quest'ultima intesa nella duplice accezione *attiva* (diritto di informare) e *passiva* (diritto a essere informati)⁵².

Un nesso, quello intercorrente tra la libertà di manifestazione del pensiero e la democraticità dell'ordinamento, che pure è stato ampiamente sottolineato dalla dottrina costituzionalistica italiana e, in particolare, da *Carlo Esposito* il quale, nel commento all'art. 21 Cost., ha affermato "che non la democraticità dello Stato ha per conse-

3.

⁴⁸ Così come scrive C. Esposito, *I partiti nella Costituzione italiana*, in Id., *La Costituzione italiana. Saggi*, Padova, 1954, 228, a proposito dell'art. 49 Cost.: "Tale disposizione, facendo dei partiti il tratto di unione tra il popolo e gli investiti del potere, lo strumento attraverso cui i cittadini possono influire sulle decisioni dei governanti e possono concorrere con continuità ed organicità alla determinazione delle direttive politiche, attribuisce ai partiti una funzione basilare nella vita della nostra democrazia rappresentativa".

⁴⁹ Al punto da ritenersi, secondo un'affermazione ormai ricorrente in dottrina, che "la libertà di espressione sembra essere quella che per eccellenza si collega alla Rete. In altri termini, tra le molte libertà esercitate per mezzo del nuovo strumento, forse quella di manifestazione del pensiero è quella che ha subito una maggiore influenza, nel senso che proprio grazie all'apertura del nuovo spazio virtuale, l'esercizio della libertà in questione si è modificato ed esteso come forse nessun'altro" (così C. Melzi d'Eril, G. Enea Vigevari, *Lo statuto dell'informazione su Internet*, T. E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, cit., 249 s.).

⁵⁰ ...ciò che costituirebbe, a giudizio di A. Pace, M. Manetti, *Art. 21. La libertà di manifestazione del proprio pensiero*, in G. Branca, A. Pizzorusso (a cura di), *Commentario della Costituzione*, Bologna-Roma, 2006, la *ratio* sottesa al riconoscimento della libertà in parola: "le ragioni ideali del riconoscimento di questa libertà dovrebbero essere rinvenute non tanto nel «valore» della persona umana (...) quanto nel valore che possiede, in sé e per sé, *la più ampia e più libera circolazione delle idee*, per i vantaggi (...) che alla collettività derivano da tale più ampia circolazione delle idee in termini di maggiori conoscenze, di abitudine alla tolleranza e di possibilità sia di confronto che di critica".

⁵¹ Di particolare spessore è l'indagine condotta sul tema dell'informazione nell'era delle nuove tecnologie da A. Amato Mangiameli, *Un nuovo bene: l'informazione*, in Id., M.N. Campagnoli, *Strategie digitali #diritto_educazione_tecnologie*, cit., 37 s.: "Il cittadino democratico ideale sembrerebbe identificarsi con il cittadino totalmente informato. D'altra parte, l'informazione è, in ogni caso, strumento di arricchimento e veicolo formidabile di quella cittadinanza democratica che è una delle principali conquiste della modernità".

⁵² Con riferimento all'enucleazione di un "diritto all'informazione", parte della dottrina ha invero espresso dubbi e perplessità circa una sua possibile coesistenza con la libertà di informare del giornalista, al punto da ritenersi che non sia ammissibile il riconoscimento di "un diritto dei privati a essere informati – sia nel senso più generico di un diritto ad una informazione il più possibile seria e imparziale, sia nel senso, più ristretto e specifico, della pretesa all'ottenimento di una data notizia": così A. Pace, *La libertà «della» informazione come valore comprensivo del diritto di liberamente informare e della libertà di informarsi. Fondamento e limiti del diritto dei privati ad essere informati*, in Id., M. Manetti, *La libertà di manifestazione del proprio pensiero*, in *Commentario della Costituzione*, cit., 346 s.

guenza il riconoscimento di quella libertà, sicché possa determinarne la funzione ed i limiti, ma che le ragioni ideali del riconoscimento di quella libertà (e cioè del valore della persona umana) porta tra le tante conseguenze anche alla affermazione dello Stato democratico⁵³.

Granitico è dunque l'orientamento, rinsaldato più di recente anche dalla Corte costituzionale con la sentenza n. 206 del 2019, per il quale “[n]on vi è dubbio che la libertà di manifestazione del pensiero (...) costituisce un valore centrale del nostro sistema costituzionale, come è stato riconosciuto non solo dalla stessa Assemblea costituente (...) ma successivamente anche da questa Corte, che ha evidenziato da tempo il rapporto tra libertà di manifestazione del pensiero e regime democratico, affermando che la prima è «coesistente al regime di libertà» garantito dalla Costituzione» (sentenza n. 11 del 1968), «pietra angolare dell'ordine democratico»⁵⁴; sì da essere determinata e qualificata tra i «principi fondanti della forma di Stato delineata dalla Costituzione, i quali esigono che la nostra democrazia sia basata su una libera opinione pubblica e sia in grado di svilupparsi attraverso la pari concorrenza di tutti alla formazione della volontà generale»⁵⁵.

Tuttavia, se è vero che l'evoluzione tecnologica abbia permesso di solcare nuovi orizzonti nel processo di ramificazione degli spazi di libertà, è altrettanto indubbio che l'utilizzo degli strumenti informatici abbia determinato l'insorgere di nuove minacce per la garanzia delle libertà individuali; e questo non solo con riferimento ad uno degli aspetti più noti e indagati come quello relativo alla protezione dei dati personali e al diritto all'autodeterminazione informativa (nella duplice dimensione del diritto all'oblio e del diritto alla deindicizzazione⁵⁶) nell'odierna società tecnologica della data-veglanza.

Accanto ad essi, infatti, vengono in rilievo altre e numerose problematiche che, per esempio, si connettono ancora una volta all'esercizio della libertà di manifestazione del pensiero *online*, spesso raffigurata in “rete” come una “libertà individuale senza mediazioni di sorta”⁵⁷, non di rado utilizzata dagli utenti per veicolare sia messaggi di incitamento all'odio (cd. *hate speech*) sia opinioni o notizie diffamatorie suscettibili-

⁵³ C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958, 12.

⁵⁴ Corte costituzionale, sentenza n. 206 del 2019, p.to 5 del *Considerato in diritto*.

⁵⁵ Corte costituzionale, ordinanza n. 132 del 2020, p.to 7.1 del *Considerato in diritto*.

⁵⁶ Entrambe le fattispecie, dapprima enucleate sulla scorta dell'evoluzione giurisprudenziale della Corte di giustizia dell'Unione europea - che ha fatto applicazione della teoria dell'efficacia diretta e orizzontale dei diritti previsti all'art. 8 della CDFUE - e successivamente positivate all'art. 17 del Regolamento generale sulla protezione dei dati personali, richiamano l'attenzione sulla peculiarità del ruolo assolto dai prestatori di servizi nell'odierna società dell'informazione, suscitando più di una criticità in merito all'ingerenza dei poteri tecnologici sul complesso di diritti e libertà fondamentali che formano il patrimonio irrettabile della personalità umana. Sul tema dell'efficacia orizzontale dei diritti riconosciuta da parte della Corte di giustizia, O. Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in *MediaLaws*, n. 3/2018.

⁵⁷ Tale è il rilievo di P. Caretti, A. Cardone, *Diritto dell'informazione e della comunicazione nell'era della convergenza*, Bologna, 2019, 254; negli stessi termini si esprime T.E. Frosini, *Il diritto all'oblio e la libertà informatica*, in Id., *Liberté égalité Internet*, Napoli, 2019, 112.

li di arrecare un più serio e grave pregiudizio alla sfera della reputazione individuale e quindi alla dignità della persona.

Peraltro, nonostante la diffusione in “rete” di notizie diffamatorie costituisca una delle fattispecie di maggiore pervasività nello spazio cibernetico, è d’obbligo segnalare come il legislatore nazionale abbia mancato di elaborare un’apposita disciplina sanzionatoria che consenta alla vittima di beneficiare di più specifici rimedi riparatori del danno derivante dalla pubblicazione in “rete” di un contenuto diffamatorio. Una mancanza che, di recente, è stata sottolineata a più riprese anche dalla Corte costituzionale la quale, sia nell’ordinanza n. 132 del 2020 sia nella sentenza n. 150 del 2021, ha particolarmente insistito sugli “effetti di rapidissima e duratura amplificazione degli addebiti diffamatori determinata dai social networks e dai motori di ricerca in internet, il cui carattere lesivo per la vittima (...) e per tutte le persone a essa affettivamente legate risulta grandemente potenziato rispetto a quanto accadeva anche solo in un recente passato”⁵⁸.

Lo stesso dicasi a proposito delle condotte discriminatorie che si producono in “rete” e per mezzo della “rete”, destinate a riverberarsi sulla tutela del principio di eguaglianza nella duplice veste formale e sostanziale. Solo a titolo di esempio, si pensi ad alcune tecniche di intelligenza artificiale che, specialmente nella fase di costruzione della decisione algoritmica, possono risolversi in pregiudizio di talune categorie protette con il rischio di distorsioni discriminatorie. Altrettanto discriminatorie risultano essere le attuali condizioni di accesso alla “rete”, evidenziandosi una forte disparità tra coloro che fruiscono agevolmente dei nuovi strumenti di informazione e comunicazione digitali e coloro che, al contrario, sono esclusi dall’accesso o dal migliore utilizzo delle tecnologie informatiche, accentuandosi per questa via la forbice di quel divario digitale (meglio noto come *digital divide*⁵⁹) che, inevitabilmente, si ripercuote sulla garanzia del principio di eguaglianza sostanziale (come bene è stato posto in luce dalla Corte costituzionale nella sentenza n. 307 del 2004); un principio, quello di eguaglianza sostanziale, che invece, in collegamento con quello di libertà, dovrebbe rappresentare la pietra angolare di ogni esperienza statutale democratica⁶⁰.

⁵⁸ Corte costituzionale, ord. n. 132 del 2020, p.to 7 del *Considerato in diritto*.

⁵⁹ Per una definizione del quale, G. Saraceni, *Digital divide and fundamental rights*, in *Humanities and Rights*, Global Network Journal, vol. 2 (2020) Issue 1, 67: “The term ‘digital divide’ refers to the many and dangerous inequalities which characterize contemporary society regarding the access to – and the use of – ICT”.

⁶⁰ Cfr. A. Ruggeri, *Società tecnologicamente avanzata e Stato di diritto: un ossimoro costituzionale?*, in *Consulta online*, n. 3/2020, 286: “l’ignoranza informatica si traduce in un *distanziamento tecnologico* che a sua volta produce un effetto - mi viene da dire - di *distanziamento costituzionale* tra chi ne è afflitto e chi invece ne è immune, allargandosi pertanto in modo irrimediabile la forbice tra coloro che possono far valere i loro diritti ed esercitare i doveri sugli stessi gravanti e coloro che sono a ciò impossibilitati, con palese violazione, in primo luogo, degli artt. 2 e 3, specie nella sua declinazione sostanziale, e quindi, dei disposti che in seno alla stessa Carta ne danno specificazione-attuazione”. In senso analogo G. De Minico, *Accesso a Internet tra mercato e diritti sociali nell’ordinamento europeo e nazionale*, in Id., *Libertà in rete. Libertà dalla Rete*, Torino, 2020, 210: “L’accesso alla rete, così inteso, rende uguali coloro che tali non erano a causa delle differenti condizioni di partenza: agisce come una leva capace di rimuovere gli ostacoli materiali ed economici che si frappongono

Peraltro, con riferimento alla prima delle fattispecie richiamate (attinenti alla violazione del principio di eguaglianza formale), non può trascurarsi la considerazione che le potenzialità discriminatorie dell'intelligenza artificiale, soprattutto per la peculiarità delle sue caratteristiche, stentano ad essere inquadrare entro le previsioni forgiate dal diritto antidiscriminatorio e, in particolare, entro la bipartizione tra le categorie della discriminazione diretta e indiretta, poiché il legame tra il soggetto agente e la condotta discriminatoria tende ad essere molto più labile che nella realtà, evidenziandosi più di una criticità in tema di accertamento e addebito della responsabilità giuridica⁶¹ (non a caso, si parla di un *accountability gap*, ad eccezione della pratica del *masking* in cui il programmatore pone in essere una discriminazione intenzionale). Tuttavia, ad oggi, le pratiche di discriminazione artificiale non hanno ancora rinvenuto un'apposita collocazione normativa e la tutela delle persone offese viene per lo più garantita dagli organi giudiziari attraverso le categorie del diritto antidiscriminatorio classico (come nel caso Deliveroo⁶²), sebbene con il rischio di applicazioni ondivaghe ed erranti tra i giudici di merito; un rischio vieppiù accentuato dalla "novità" dei fenomeni di discriminazione algoritmica e dall'incapienza della disciplina antidiscriminatoria attualmente in uso.

Altrettanto può ritenersi a proposito delle politiche di contrasto al fenomeno del *digital divide* che, pur prescindendo dalla dibattuta questione teorica circa la configurabilità o meno di un nuovo diritto costituzionale di accesso alla "rete"⁶³, necessiterebbero (forse) di un più accorato impegno da parte delle istituzioni pubbliche e degli attori privati allo scopo di ridurre quel divario digitale che è generato tanto da una matrice di tipo sociale, culturale ed economica quanto da una ragione di tipo infrastrutturale⁶⁴. Una diseguaglianza digitale che è affiorata in tutta la sua gravità

al pieno sviluppo della persona (art. 2 Cost.), consentendole l'effettivo esercizio delle libertà fondamentali (...). La missione equilibratrice del diritto di accesso, in definitiva, lo rende funzionale all'uguaglianza sostanziale, di cui all'art. 3 Cost.". Come bene posto in luce anche da L. Gallino, *Sui rapporti tra la globalizzazione e lo sviluppo della rete*, in *Jura Gentium*, 2005, 2: "la dimostrata impossibilità di fruire dei suddetti benefici da parte di numerose persone e gruppi, a causa delle difficoltà economiche o culturali che incontrano nell'uso di Internet, giunge a configurare forme originali di disuguaglianze globali, quelle tra "info-poveri" e "info-ricchi". Simili disuguaglianze rischiano di essere non meno radicali e foriere di conseguenze negative di quelle tradizionali di reddito e di ricchezza".

⁶¹ In argomento, si v. più estesamente C. Nardocci, *Intelligenza artificiale e discriminazioni*, in *Gruppo di Pisa*, n. 3/2021, 9 ss.

⁶² Trib. Bologna, ord. 31/12/2020.

⁶³ Paradigmatico è il riferimento alla proposta formulata da Stefano Rodotà in ordine all'inserimento di una nuova disposizione costituzionale, l'art. 21 *bis*, che così avrebbe recitato: "Tutti hanno eguale diritto di accedere alla rete Internet, in condizioni di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale". Sul tema, si veda più esattamente S. Rodotà, *Un Articolo 21-bis per Internet*, consultabile all'indirizzo <http://archivio.articolo21.org/2183/notizia/un-articolo21bis-per-internet-.html>, a parere del quale "La proposta di un art. 21-bis (...) va proprio nella direzione di ribadire e espandere i principi costituzionali riguardanti l'eguaglianza e la libera costruzione della personalità". In senso analogo, G. Azzariti, *Internet e Costituzione*, in *Costituzionalismo.it*, n. 2/2011, 3.

⁶⁴ Secondo alcune recenti stime, riportate da A. Alù, A. Longo, *Cos'è il digital divide, nuova*

proprio durante l'emergenza pandemica: ad esempio, dalla lettura del Rapporto Agcom del 2020⁶⁵ emerge che quasi dieci studenti su cento tra quelli intervistati hanno lamentato di non possedere dispositivi idonei allo svolgimento delle lezioni a distanza mentre venticinque su cento hanno evidenziato problemi di velocità della connessione da casa.

Inutile dire quanto e come simili criticità siano destinate ad impattare sulla garanzia del principio di eguaglianza sostanziale, erodendo il fulcro dello Stato costituzionale democratico.

Piuttosto, l'indefettibilità di un intervento normativo a garanzia delle libertà digitali, tuttora vulnerate dall'anomia, appare essere tanto più necessaria solo riflettendo sull'introduzione di alcune fattispecie di reato che sono state tipizzate dal legislatore allo scopo di garantire alla persona una tutela più efficace rispetto ad alcune forme di pregiudizio derivanti dallo spazio cibernetico: fra tutte, particolare rilievo assume la previsione del reato di "Diffusione illecita di immagini o video sessualmente espliciti" (meglio noto come *revenge porn*) rubricato all'art. 612 *ter* c.p. e introdotto con legge n. 69 del 2019 (il cd. Codice rosso).

Lo stesso può ritenersi a proposito della legge n. 71 del 2017 con la quale sono state dettate "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" così come della fattispecie di cui all'art. 600-*quater* I c.p. ("Pornografia virtuale"), criminalizzata con legge n. 38 del 2006.

A tal riguardo, è interessante sottolineare come gli interventi legislativi qui richiamati siano stati sollecitati da alcuni casi di cronaca di particolare gravità⁶⁶ che hanno contribuito ad evidenziare con forza l'urgenza di elaborare appositi strumenti giuridici idonei a salvaguardare la persona da alcune fattispecie pregiudizievoli che rischiano di assumere connotati di maggiore disfunzionalità proprio per effetto della loro realizzazione nello spazio cibernetico, ove "le informazioni e i contenuti (...) acquisiscono, pressoché immediatamente, una capacità di permanenza e di volatilità del tutto particolari"⁶⁷.

Tutte caratteristiche che, come sopra ricordato, sono state bene evidenziate anche dalla Corte costituzionale la quale, seppure con riferimento alla fattispecie della diffamazione *online*, ha sollecitato il tempestivo intervento del legislatore e, in par-

discriminazione sociale (e culturale), in *agendadigitale.eu*, 13 marzo 2020, il *digital divide* di primo livello, consistente nella mancata copertura di banda larga fissa ad almeno 2 Megabit, interesserebbe circa il 5,6 per cento della popolazione italiana; più alta, invece, risulterebbe la percentuale della popolazione (tra il 20 e il 40 per cento) colpita dal *digital divide* di secondo livello, ossia dalla mancata copertura di banda ultralarga.

⁶⁵ Autorità per le garanzie nelle comunicazioni, *Le comunicazioni nel 2020. L'impatto del coronavirus nei settori regolati. Allegato alla Relazione annuale*, Giugno 2020, consultabile all'indirizzo <https://www.agcom.it/documents/10179/19267334/Allegato+6-7-2020+1594044962316/36cae229-dcac-4468-9623-46aabd47964f?version=1.0>

⁶⁶ Come quello che ha tristemente coinvolto, conducendola al suicidio, la giovane Tiziana Cantone, vittima della diffusione in rete di alcuni video amatoriali che la ritraevano in un momento di intimità.

⁶⁷ Così M.N. Campagnoli, *Social media e information disorder: questioni di ecologia comunicativa in Rete (Parte Terza – Il revenge porn)*, in *Dirittifondamentali.it*, n. 3/2020, 307.

ticolare del Parlamento “quale naturale depositario delle scelte in materia penale in una società democratica”⁶⁸, con l’obiettivo di prefigurare un più equilibrato sistema di tutela dei diritti in gioco; ciò sul presupposto che, in ordinamenti ispirati alla regola democratica, la decisione sui diritti e sui doveri deve essere concepita come una decisione *politica* che non può essere affidata (o almeno non esclusivamente) ai giudici⁶⁹.

Un insegnamento che non può essere smarrito soprattutto se si ragiona, in chiave progettuale, della *governance* di *Internet* e della necessità di ricercare gli strumenti più utili a garantire una tutela certa ed effettiva dei diritti fondamentali della persona nello spazio cibernetico; una certezza che sino ad oggi è mancata (e manca tuttora) soprattutto perché, in assenza di una forte e consolidata guida eteronoma da parte dei pubblici poteri, il giudice e non il legislatore si è imposto quale figura di riferimento per la tutela dei diritti e delle libertà inviolabili.

E infatti, non potrà sfuggire la considerazione che per quanto il diritto giudiziario abbia assunto un ruolo imprescindibile nel processo di costituzionalizzazione multi-livello, esso rimane pur sempre un diritto largamente guidato dalla fattualità e dunque largamente incerto e imprevedibile nel suo dipanarsi⁷⁰, con il rischio (neppure troppo infrequente) di affermazioni ondivaghe e quasi schizofreniche da parte degli organi di giustizia.

Ciò appare essere tanto più evidente in un campo, come quello delle libertà digitali, che riflette una più significativa diversità di approccio tra l’impostazione filo-garantista delle Corti continentali e quella filo-libertaria della Corte Suprema degli Stati Uniti d’America; una diversità che si è manifestata con particolare vigore in relazione alla tutela della libertà di espressione in *Internet*⁷¹ laddove, mentre la giurisprudenza europea ha posto maggiormente l’accento sui rischi derivanti dall’utilizzo delle tecnologie digitali, la Corte statunitense ha invece esaltato le potenzialità della “rete” quale strumento di massima esplicazione della libertà di manifestazione del pensiero, garantita dal primo emendamento alla Costituzione⁷².

⁶⁸ Corte costituzionale, sentenza n. 37 del 2019, p.to 7.3. del *Considerato in diritto*.

⁶⁹ Cfr. M. Luciani, *Costituzionalismo irenico e polemico*, in *Giur. cost.*, n. 4/2006, 1663.

⁷⁰ In argomento, per ulteriori considerazioni in merito all’incidenza delle nuove tecnologie informatiche sulla rapida e “caotica” evoluzione del diritto di matrice giurisprudenziale, si v. F.G. Pizzetti, *Internet e la natura «caotica» del diritto giurisprudenziale*, in *Pol. dir.*, n. 3/2001, 467 ss.

⁷¹ Sul tema più specifico della “divergenza” giurisprudenziale sulla protezione da accordarsi alla libertà di espressione *online* si v. O. Pollicino, *Tutela dei diritti fondamentali nell’era digitale e contesto valoriale: una indagine transatlantica*, in *mediaLaws*, n. 2/2018, 39 ss.; M. Bassini, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali*, Roma, 2019, 163 ss.

⁷² Emblematica è la sentenza della Corte Suprema sul caso *Internet* del 26 giugno 1997, con la quale la Corte ha esaminato la legittimità costituzionale del *Communications Decency Act* (CDA) nella parte in cui la legge proibiva la trasmissione su *Internet* di messaggi osceni, indecenti o palesemente offensivi, per gli standards della comunità, a destinatari minori di anni diciotto. A giudizio della Corte, l’ambiguità delle prescrizioni del CDA, congiuntamente alla durezza delle sanzioni penali ivi previste, avrebbe impattato pregiudizievolemente sulla garanzia della libertà di espressione, vietando la circolazione di una quantità notevole di materiali che gli adulti avrebbero avuto il diritto, costituzionalmente garantito, di fruire e scambiarsi reciprocamente e ciò sul

Ne consegue che l'insufficienza di un modello *prettamente* giurisdizionale di tutela

presupposto, ampiamente ribadito nella sua giurisprudenza, che "forme di espressione e contenuto sessualmente indecenti, ma non oscene, sono protette dal primo emendamento". D'altro canto, l'esigenza di proteggere i bambini da materiali nocivi non avrebbe legittimato, a parere dei giudici, una soppressione ingiustificatamente ampia ed estesa di forme di espressione destinate agli adulti. Così argomentando, la Corte ha concluso nel senso di ritenere che: "I fatti accertati dimostrano che l'espansione di Internet è stata, e continua a essere, fenomenale. È tradizione della nostra giurisprudenza costituzionale presumere, in mancanza di prove contrarie, che la regolamentazione pubblica del contenuto delle manifestazioni del pensiero è più probabile che interferisca con il libero scambio delle idee piuttosto che incoraggiarlo. L'interesse a stimolare la libertà di espressione in una società democratica è superiore a qualunque preteso, non dimostrato, beneficio della censura". Altro esempio paradigmatico è la sentenza del 16 aprile 2002 sul caso *Ashcroft* con la quale la Corte Suprema ha dichiarato l'incostituzionalità del *Child Pornography Prevention Act* (CPPA del 1996), in quanto ritenuto lesivo della libertà di espressione dei cittadini. Nella specie, il CPPA estendeva il divieto di possedere o distribuire materiale pornografico infantile anche a immagini che ritraevano "bambini virtuali", ovverosia video o foto di adulti i quali, mediante l'utilizzo di mezzi informatici, vengono ad essere rappresentati come bambini, suscitando così l'impressione che i minori siano coinvolti in attività sessualmente esplicite. La Corte ha tuttavia ritenuto che la proibizione apparisse ingiustificata poiché la fattispecie, ricondotta dalla legge nella più ampia categoria della pornografia infantile, non avrebbe implicato un coinvolgimento reale di bambini nella produzione di materiale pornografico; per conseguenza, la disposizione impugnata non avrebbe legittimato una siffatta restrizione della libertà di espressione garantita dal Primo Emendamento. Puntualizza meglio la Corte che "La pornografia infantile virtuale non è 'intrinsecamente correlata' all'abuso sessuale sui bambini" e che "[l]a distribuzione di descrizioni o altre raffigurazioni di condotta sessuale, non altrimenti oscena, che non implicano performance dal vivo o riproduzioni fotografiche o visive di esibizioni dal vivo, conserva la protezione del Primo Emendamento". In senso diametralmente opposto, invece, si colloca la soluzione prescelta dal nostro ordinamento laddove, come sopra ricordato, con legge 6 febbraio 2006, n. 38, recante "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia", il legislatore ha invece introdotto il reato di pornografia virtuale di cui all'art. 600-*quater* I c.p. Quella della pornografia virtuale è dunque una fattispecie incriminatrice volta a sanzionare il possesso e la distribuzione di immagini pedopornografiche realistiche, ossia di immagini che rappresentino un minore impegnato in atteggiamenti sessuali espliciti, in quanto tali immagini potrebbero essere utilizzate per sedurre soggetti minori o per incoraggiarli a partecipare ad attività sessuali. Sul tema, particolare interesse riveste la decisione della Corte di Cassazione penale, sez. III, del 13 gennaio 2017, n. 22265, nella quale i giudici, in evidente difformità con la soluzione resa dalla Corte Suprema al caso *Ashcroft*, hanno affermato che non risulta "corretto interpretare la disposizione sulla pedopornografia virtuale nel senso che quando la pedopornografia venga realizzata senza l'utilizzazione di 'minori reali' non sussisterebbe alcun concreto pericolo per la personalità e lo sviluppo del minore, atteso che il bene giuridico tutelato non è costituito unicamente dalla libertà sessuale del bambino le cui sembianze siano state impresse nella fotografia o siano state riprese nel filmato (...). I beni giuridici tutelati dalla fattispecie in oggetto sono da individuare nella intangibilità della personalità dei soggetti minorenni e nel rispetto dei tempi e modi di sviluppo della loro personalità, beni ai quali il legislatore ha inteso assegnare una tutela rafforzata (...)". Argomentando sulla base di un'interpretazione conforme alla lettura degli strumenti internazionali sulla criminalità informatica vincolanti per l'Italia, la Corte prosegue ancora osservando che "qualunque interpretazione volta ad escludere la rilevanza penale delle condotte di detenzione (ed ancor più di diffusione) di tale materiale in forza della considerazione che non risultino rappresentati soggetti "realmente esistenti", risulta, nella sostanza, interpretazione abrogatrice e *contra legem* della stessa fattispecie penale, che ha equiparato la pedopornografia virtuale alla pedopornografia su supporto cartaceo. Il momento discriminante non sta, quindi, nella elaborazione sofisticata di immagini di carattere tridimensionale, ma nel fatto che l'elaborazione grafica effettuata, evochi la rappresentazione di situazioni reali, ossia di atteggiamenti sessuali che offrono lo svolgimento di attività sessuali nelle quali i bambini sono ridotti al rango di meri oggetti sessuali, di giocattoli sessuali con i quali e sui quali, compiere atti a valenza sessuale".

dei diritti fondamentali della persona evoca la necessità, ormai non più procrastinabile, di un più capillare e diffuso intervento del decisore politico⁷³ in funzione regolatoria del sistema di governo di *Internet*⁷⁴ affinché il principio di legalità, quale strumento di controllo e limitazione del potere (anche digitale), inneschi un processo di costituzionalizzazione dello spazio cibernetico⁷⁵ che restituisca un saldo ancoraggio alla questione dei diritti fondamentali in “rete”: detto in altri termini, “*the rule of law as expressed by sovereign states must be supreme over technological claims*”⁷⁶.

3. Per una costituzionalizzazione dello spazio cibernetico

L'immagine scaturente dalle osservazioni testé condotte è quella di una persona che nello spazio cibernetico appare fortemente dimidiata quanto alla garanzia dei suoi diritti e delle sue libertà fondamentali, evidenziandosi uno scollamento tra il mondo *offline* e lo spazio *online*, nel quale i diritti e le libertà inviolabili sembrano beneficiare di un minore grado di tutela anche per effetto della mancata, scarna o tardiva regolazione dei fenomeni cibernetici da parte dei pubblici poteri.

Pertanto, lo slittamento del baricentro dalla *persona* ai *poteri*, registratosi nell'era digitale, esprime l'esigenza, non più rinviabile, di dare forma giuridica a un rinnovato progetto di emancipazione politica dei diritti fondamentali, affinché la *governance* dello spazio cibernetico (attraverso il paradigma della *etero* o *co-regolazione*⁷⁷) sia

⁷³ Parimenti, O. Pollicino, *L'algoritmo e la nuova stagione del costituzionalismo digitale: quali sfide per il giurista (teorico e pratico)?*, intervista a cura di R. Conti e F. De Stefano, in *Giustizia insieme*, 15 aprile 2021, 5.

⁷⁴ In senso analogo, D. De Grazia, *L'Internet Governance tra tecnica, politica e diritto*, in *Inf. dir.*, n. 1/2009, 44: “I tempi sono maturi perché la gestione della Rete sia finalmente informata al rispetto di un principio di legalità o di una *rule of law*”.

⁷⁵ Riferendosi, con tale espressione, al “*process of production of norms aiming to ensure the protection of fundamental rights and the balancing of powers within that context*” (così E. Celeste, *Digital constitutionalism. Mapping the constitutional response to digital technology's challenges*, in *Hiiig Discussion Paper Series*, 2018, 16).

⁷⁶ J.R. Reidenberg, *Technology and Internet jurisdiction*. University of Pennsylvania Law Review, vol. 153, 1951, 2005, Fordham Law Legal Studies Research Paper No. 79, disponibile all'indirizzo <https://ssrn.com/abstract=691501>, 1969.

⁷⁷ È infatti opinione corrente, ampiamente sostenuta da una larga schiera di commentatori, che il modello della eteroregolazione debba essere declinato, più esattamente, secondo le logiche di una “*co-regulation*”, ispirata al *multi-stakeholderism*, assicurando il coinvolgimento dei soggetti privati nel processo di produzione delle fonti di regolazione autoritativa e promuovendo una *governance* di *Internet* che sia trasparente e responsabile, collaborativa e partecipativa. In argomento, e più diffusamente, S. Rodotà, *Una Costituzione per Internet?*, in *Pol. dir.*, n. 3/2010, 343 s.; G. De Minico, *Internet. Regola e anarchia*, Napoli, 2012, 14; A. Oddenino, *Il problema della governance internazionale della rete*, in M. Durante, U. Pappagallo (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, 2012, 48; V. De Rosa, *La formazione di regole giuridiche per il «cyberspazio»*, in *Diritto dell'informazione e dell'informatica*, n. 1/2003, 361 ss.; P. Laghi,

orientata in direzione dei postulati del moderno costituzionalismo, primo fra i quali il riconoscimento del primato della persona e dell'anteriorità logica dei suoi diritti e delle sue libertà fondamentali, costituenti il patrimonio irriducibile della dignità umana⁷⁸.

L'esperienza empirica, infatti, sta a dimostrare come il progresso tecnologico imponga di essere guidato nel suo sviluppo verso il rispetto di quei principi sui quali è stata edificata l'architettura dello Stato costituzionale di diritto, rappresentando i diritti fondamentali al centro del potere informatico⁷⁹.

In questa nuova e diversa luce riemerge insostituibile il ruolo del paradigma statale poiché lo Stato, nonostante le trasformazioni subite per effetto del processo di globalizzazione cibernetica, continua ad incarnare una realtà politica potente⁸⁰ che si configura come il più autentico e privilegiato interprete della tradizione del costituzionalismo democratico⁸¹; e dunque di quella tradizione che ha limitato il potere in funzione e al servizio della persona.

È perciò evidente come il segno delle mutazioni in corso operi - o dovrebbe operare

Cyberspazio e sussidiarietà, Napoli, 2015.

⁷⁸ È perciò necessario, come osserva anche F. Lanchester, *La stella polare del costituzionalismo*, Editoriale, in *Nomos*, n. 1/2018, 3, che i valori e principi del costituzionalismo continuino ad essere una vera e propria *stella polare* del cambiamento in atto.

⁷⁹ F. Viola, *Tecnica, etica e diritti umani*, in A.C. Amato Mangiameli (a cura di), *Persone e Stati. Le conseguenze della "globalizzazione" e della innovazione tecnologica*, Milano, 2006, 148: "Non si tratta, infatti, come spesso si ritiene, semplicemente di autorizzare l'applicazione di certi progressi tecnologici alla natura umana (o alla natura in generale) oppure di vietarli. Più in profondità si tratta di far sì che il mondo tecnologico sia umanizzato, cioè entri a far parte dell'insieme narrativo della vita umana, senza squilibri nell'esistenza dei singoli e dei gruppi sociali".

⁸⁰ Cfr. A.C. Amato Mangiameli, *Stati post-moderni e diritto dei popoli*, Torino, 2004, 65 s.: "Se è vero che nel contesto di una società internazionale complessa (...) mutano la natura e il ruolo dello Stato, altrettanto vero è che le pressioni sociali e culturali (al contrario delle economiche) rendono tutt'oggi lo Stato e la nazione *realità politiche potenti*, capaci pur sempre di fronteggiare all'occorrenza le diverse logiche e le complesse dinamiche della globalizzazione". Parimenti, riflettendo sulle trasformazioni subite dallo Stato nella mondializzazione, U. Allegretti, *Diritti e stato nella mondializzazione*, Enna, 2002, 17, afferma: "Certamente le sue funzioni e le sue strutture cambiano e il ruolo stesso non è più quello di prima. Ma il suo peso resta imponente: molti lo riconoscono e non ritengono prevedibile che il suo deperimento debba compiersi rapidamente. Si osserva dunque che esso va «ripensato» piuttosto che superato". V. Roppo, *Verso un mondo globalizzato: trasformazioni economiche, mutamenti sociali, risposte politiche*, in *Pol. dir.*, n. 3/2001, 520: "La politica: ecco il punto cruciale in cui inevitabilmente s'imbatte il discorso sulla globalizzazione. Per parte mia, non esito ad affermare con chiarezza che la politica può e deve misurarsi con la realtà della globalizzazione, senza patire la *deminutio* che vorrebbero infliggerle le ideologie della globalizzazione. Alla politica (...) deve rivendicarsi un ruolo decisivo per contrastare gli aspetti viziosi della globalizzazione, e valorizzarne gli aspetti virtuosi". Analogamente S. Cassese, *La democrazia e i suoi limiti*, Milano, 2017, 48: "gli Stati dimostrano di sapersi adattare al nuovo contesto, dominato dalla globalizzazione. Come è stato osservato, gli Stati sono camaleonti, capaci di mutare; (...) Esso costituisce ancora la macchina di governo più potente, mostra una enorme capacità di espansione (...)".

⁸¹ Dello Stato quale "vettore dei principi del costituzionalismo" scrive M. Michetti, *Organizzazione del potere e territorio. Legittimità dello Stato e livelli di governo*, cit., 157: "Solo lo Stato potrebbe perciò dare e *trasferire* - attraverso il principio democratico, il principio pluralista e soprattutto la tutela dei diritti - "sostanza costituzionale" all'ordine globale o comunque indirizzare la globalizzazione verso la tradizione del costituzionalismo".

- non già nel verso di una de-costituzionalizzazione degli ordinamenti politici ma, piuttosto, nel senso di una costituzionalizzazione dell'ordine globale, mantenendo saldo e anzi espandendo quel nucleo indefettibile di principi che è racchiuso all'interno delle Costituzioni nazionali.

D'altronde, la deriva tecnocratica che è scaturita dal processo di globalizzazione tecnologica potrà essere arginata, o addirittura frenata, soltanto da un'espansione del paradigma costituzionale, riconoscendo la persona come "anello di congiunzione" della rete globale dei poteri e portando a compimento il progetto di integrazione politica, avviato nel secondo dopoguerra, che ha aperto la strada alla costituzionalizzazione dello scenario internazionale e sovranazionale⁸².

Ciò appare essere tanto più evidente se si analizza l'evoluzione del processo di integrazione sovranazionale e si riflette su come l'ordinamento europeo, istituito al solo scopo della costruzione del mercato comune e della tutela delle quattro libertà economiche ad esso afferenti, abbia assunto nel tempo - soprattutto per opera della Corte di Giustizia - i connotati di una vera e propria *comunità di diritto*, nella quale il rispetto dei principi e delle regole costituivi il fondamento dello Stato costituzionale di diritto è stato elevato tra i principi di struttura dell'ordinamento europeo, così come proclamato dalla stessa "clausola di omogeneità" di cui all'art. 2 TUE⁸³.

Analoghe osservazioni sembrano valere per l'ordinamento internazionale che, seppure a lungo imperniato su una concezione statocentrica e una visione assoluta della sovranità statale, è stato lambito anch'esso dalla forza pervasiva di un processo di

⁸² M.R. Ferrarese, *Il diritto al presente. Globalizzazione e tempo delle istituzioni*, cit., 114: "Oggi si assiste infatti alla composizione di numerosi fili di natura costituzionale, che, variamente intrecciati, accostati e combinati, determinano una tessitura costituzionale ininterrotta e sempre più estesa nel globo, ma tutt'altro che integra, priva di buchi, incertezze ed incoerenze. (...) E tuttavia, questa enorme tela costituzionale, fitta in alcuni punti e sottilissima in altri, bucherellata qui e là, non priva di smagliature vistose, estende ogni giorno il suo raggio di azione".

⁸³ Art. 2 TUE: "L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini". In argomento, S. Mangiameli, *Article 2*, in H.J. Blanke, Id. (a cura di), *TEU. A commentary*, Heidelberg, 2013; Id., *La clausola di omogeneità nel Trattato dell'Unione europea e nella Costituzione europea*, in Id. (a cura di), *L'ordinamento europeo. I principi dell'Unione*, Milano, 2006, 1 ss.

costituzionalizzazione⁸⁴ (il c.d. *constitutional international law*)⁸⁵ che ha rinnovato, anche sul piano strutturale⁸⁶, l'assetto della comunità internazionale, la cui azione è andata sempre più orientandosi verso il riconoscimento e la protezione dei diritti umani anche nei confronti degli Stati medesimi⁸⁷.

⁸⁴ Sul tema, si rimanda alle più ampie e approfondite riflessioni di S. Mangiameli, *Stato, integrazione europea e globalizzazione. Le nuove sfide del costituzionalismo*, in Id., *I diritti costituzionali dallo Stato al processo di integrazione*, cit., 250 ss., per il quale, sebbene “la volontà degli Stati, come strumento di azione del diritto internazionale, non si possa ignorare, si assiste progressivamente all'emersione dei principi democratici, della *rule of law* e dei diritti umani come presupposti del riconoscimento degli Stati nel diritto internazionale” (252). Più esattamente, i principi del costituzionalismo avrebbero indotto due trasformazioni fondamentali nel diritto internazionale: “per un verso, portano ad una diversa concezione dell'uso della forza e, per l'altro, promuovono un assetto internazionale, dove grazie all'emersione dei diritti, si assiste alla formazione di strutture e sistemi regionali di salvaguardia che sempre più permeano le relazioni tra gli Stati” (253). R. Bin, *Critica della teoria dei diritti*, Milano, 2018, 132: “L'internazionalizzazione sembra proseguire la strada della costituzionalizzazione dei diritti, consentendo lo sviluppo di una «nozione internazionale di Stato di diritto», una sintesi tra il *Rechtsstaat* e il *rule of law* che si basa su fattori diversi ma convergenti, quali la definizione di un minimo di regole fondamentali poste a beneficio di tutti gli uomini e opponibili agli stati, la cui sottomissione al diritto internazionale apre la prospettiva di una “giuridicizzazione” del rispetto dei diritti dell'uomo. È vero che il diritto internazionale, consuetudinario o pattizio che sia, è dominato dalle grandi potenze, ma il sistema dei diritti umani sembra capace di imporsi come una autorevole “lingua franca” che detta agli Stati degli standard relativi a come essi devono trattare coloro che sono sottoposti alla loro giurisdizione”. C. Focarelli, *Costituzionalismo internazionale e costituzionalizzazione della global governance: alla ricerca del diritto globale*, in *Pol. dir.*, n. 2/2011, 207 ss.: “Se si volesse sintetizzarne la sostanza, si potrebbe dire che il nuovo costituzionalismo internazionale pretende di costituzionalizzare, o di «costituire» come realtà, la *global governance* e il ruolo di attori e regole *non statali* a favore delle *popolazioni*, ossia dei governati anziché dei governanti, distanziandosi così dal modello c.d. di Westfalia che sarebbe invece dominato esclusivamente dagli Stati (e quindi anche dalla ragion di Stato). La prospettiva di fondo cambia da *state-centred* a *people-centred*” (215). A. Peters, *Global Constitutionalism*, in *The Encyclopedia of Political Thought*, First Edition, Hoboken, 2015, 2: “*Constitutionalization in this sense is an evolution from an international order based on some organizing principles, such as state sovereignty and consensualism, to an international legal order which acknowledges and has creatively appropriated principles and values of constitutionalism*”.

⁸⁵ Gli aspetti lessicali del fenomeno sono stati meglio puntualizzati da R. Bifulco, *La c.d. costituzionalizzazione del diritto internazionale: un esame del dibattito*, in *Rivista AIC*, n. 4/2014, il quale si sofferma più analiticamente sulla distinzione tra i concetti di *constitutional of international law*, *constitutionalism*, *constitution*, *international/global constitutional law*, *denationalization of constitutional law*.

⁸⁶ Si pensi, in particolare, alla creazione di numerosi Corti internazionali: tra le altre, la Corte europea dei diritti dell'uomo, la Corte internazionale di Giustizia, la Corte penale internazionale. Altrettanto emblematica del cambiamento intercorso nella comunità internazionale è l'evoluzione registratasi in tema di soggettività, mettendosi in discussione la questione dello Stato come esclusivo soggetto del diritto internazionale: cfr. A. Di Martino, *Il territorio: dallo Stato-nazione alla globalizzazione. Sfide e prospettive dello Stato costituzionale aperto*, Milano, 2010, 303 ss.

⁸⁷ Come osservato anche da M. Michetti, *Organizzazione del potere e territorio. Legittimità dello Stato e livelli di governo*, cit., 168, se si guarda al diritto internazionale, “l'evoluzione in senso costituzionale si è realizzata con il superamento della visione statocentrica, fondata esclusivamente sul ruolo sovrano degli Stati, cui è andata sostituendosi la centralità della persona, quale indiscusso baricentro dell'azione internazionale”. In senso analogo, V. Possenti, *Universalismo dei diritti e governance politica globale. Il cammino verso una società politica planetaria*. Relazione al convegno di studio promosso dal Centro Interdipartimentale di Ricerca sui Diritti Umani/Cirdu: *Governance globale e diritti dell'uomo. Come possiamo prendere sul serio i diritti nel XXI secolo?* (Venezia, 17-19 novembre 2005), 8, il quale adotta l'espressione “*sovranità internazionale liberale*”

Permane, dunque, la forza prescrittiva di quelle affermazioni di valore attraverso le quali le Costituzioni, *pro praeterito*, hanno sagomato l'ordinamento concreto e, *pro futuro*, hanno modellato un armamentario teorico utile e sufficiente - nella sua perdurante attualità - a fronteggiare le sfide della globalizzazione⁸⁸, ivi compreso il riconoscimento e la tutela di quelli più comunemente noti come i "diritti dell'età tecnologica"⁸⁹; il problema diventa, semmai, quello di portare ad effetto il contenuto precettivo delle disposizioni costituzionali, impegnando la "capacità progettuale della politica"⁹⁰ nell'incastonare il nuovo ordine globale sulla pietra angolare del principio personalista.

per rappresentare l'approdo a un nuovo ordine "che estende alla sfera internazionale la visione liberale di porre limiti al potere politico e all'attività di governo, e pensa l'ordine internazionale entro il paradigma di un multilateralismo cooperante entro le norme che, regolando lo *jus ad bellum* e il quadro dei diritti umani, circoscrivono l'uso del potere coercitivo". Da questo punto di vista, è apparsa senz'altro cruciale l'adozione di svariate Carte e Dichiarazioni internazionali per il riconoscimento dei diritti degli individui, anche nei confronti degli Stati: solo a titolo di esempio, si ricordi la *Dichiarazione universale dei diritti umani*, adottata e proclamata dall'Assemblea Generale delle Nazioni Unite il 10 dicembre 1948; la *Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali*, firmata nel 1950 dal Consiglio d'Europa; la *Convenzione sullo statuto dei rifugiati*, approvata in una speciale Conferenza delle Nazioni Unite tenutasi a Ginevra nel 1951; il *Patto internazionale relativo ai diritti civili e politici* e il *Patto internazionale sui diritti economici, sociali e culturali*, approvati dall'Assemblea generale dell'ONU il 16 dicembre 1966; la *Convenzione delle Nazioni Unite sui diritti delle persone con disabilità*, approvata dall'Assemblea Generale delle Nazioni Unite il 13 dicembre 2006; la *Convenzione sui diritti dell'infanzia*, approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989. In argomento si v. pure A. Barbera, *Le basi filosofiche del costituzionalismo*, in Id. (a cura di), *Le basi filosofiche del costituzionalismo*, Bari-Roma, 1997, 37 ss., il quale rileva: "tali dichiarazioni superano la tradizionale concezione del diritto internazionale come diritto che riguarda esclusivamente i rapporti fra Stati e tendono invece a fare emergere la soggettività dei cittadini e dei popoli" (38).

⁸⁸ Cfr. M. Luciani, *Dottrina del moto delle costituzioni e vicende della Costituzione repubblicana*, in *Osservatorio sulle fonti*, n. 1/2013, 2: "la prospettiva che le costituzioni abbracciano non è quella statica. Le costituzioni (...) sono un fatto dell'uomo, e poiché è la storia la dimensione in cui l'uomo vive ed opera, la tensione *ad aeternitatem* delle costituzioni implica l'accettazione della prospettiva dinamica, nel senso che esse debbono raccogliere la sfida della storia e del cambiamento". Più di recente, ad esprimere un apprezzamento positivo sulla "forza" della Costituzione italiana è stato E. Cheli, *Il rendimento storico della costituzione italiana*, in *Dir. pubbl.*, n. 1/2021, 185 ss.

⁸⁹ C. Faralli, *Diritto, diritti e nuove tecnologie*, Napoli, 2018, 18.

⁹⁰ M. Luciani, *Dottrina del moto delle costituzioni e vicende della Costituzione repubblicana*, cit., 8 s.

IA E PRIVACY: L'APPROCCIO CON IL MODELLO DAPPREMO E LE PROSSIME SFIDE

Nicola Fabiano¹

Abstract [ITA]: Il tema dell'intelligenza artificiale di per sé complesso non è esente dalle valutazioni di conformità alla disciplina normativa in materia di protezione dei dati personali e privacy. Il tentativo di individuare una definizione di intelligenza artificiale si rivela vano, sia in quanto il tema è molto discusso in dottrina, sia perché la recente proposta europea di Regolamento su AI definisce unicamente "sistemi di intelligenza artificiale". Tale definizione è decisiva in quanto determina l'orientamento del legislatore europeo verso la qualificazione dei sistemi di intelligenza artificiale come software. Da questa impostazione e dall'analisi della produzione documentale a livello istituzionale in Europa negli ultimi anni emergono aspetti che contribuiscono a qualificare il "tema" dell'intelligenza artificiale soprattutto con riferimento ai rischi. È preoccupante il mancato riferimento all'etica che, a nostro avviso, costituisce un elemento fondamentale e imprescindibile. Lo scenario che ne deriva va valutato alla luce della disciplina vigente a livello europeo in materia di protezione dei dati personali e privacy ed emergono profili di estremo interesse soprattutto nell'applicazione di alcuni principi come quello della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita. La nostra proposta è DAPPREMO, il Data Protection and Privacy Relationships Model che - basato su alta matematica e teoria degli insiemi - può costituire un approccio innovativo al tema della protezione dei dati personali.

Abstract [EN]: The complex topic of artificial intelligence in itself is not exempt from assessments of compliance with the regulatory framework for personal data protection and privacy. The attempt to identify a definition of artificial intelligence proves futile, both because the topic is much debated in doctrine and because the recent European proposal for a Regulation on AI defines only "artificial intelligence systems." This definition is decisive in that it determines the orientation of the European legislator toward qualifying artificial intelligence systems as software. From this approach and from the analysis of the documentary production at the institutional level in Europe in recent years, aspects emerge that contribute to qualifying the "theme" of artificial intelligence especially with reference to risks. Of concern is the lack of reference to ethics, which, in our view, constitutes a fundamental and indispensable element. The resulting scenario has to be evaluated in the light of the

¹ Nicola Fabiano, Avvocato cassazionista e Specialista in Diritto Civile, Professore a contratto all'Università di Ostrava - Sede di Roma.

existing European data protection and privacy regulations and profiles of extreme interest emerge especially in the application of certain principles such as data protection by design and protection by default. Our proposal is DAPPREMO, the Data Protection and Privacy Relationships Model, which--based on high mathematics and set theory--can be an innovative approach to the topic of personal data protection.

Keywords [ITA]: intelligenza artificiale – protezione dei dati personali – privacy – etica – dappremo.

Keywords [EN]: Artificial intelligence - data protection - privacy - ethics - dappremo.

Sommario: 1. Introduzione. – 1.1. Premesse. – 1.3. Necessità di un approccio multidisciplinare. – 2. È possibile definire l'intelligenza artificiale? – 2.1. Intelligenza artificiale e sistemi di intelligenza artificiale. – 2.2. La proposta di Regolamento UE sulla IA e il tentativo di individuare una definizione. – 3. Lo scenario europeo sull'intelligenza artificiale. – 4. Etica e intelligenza artificiale. – 5. 1. I rischi dell'intelligenza artificiale (cenni) e le sfide. – 6. 1. La nostra proposta: DAPPREMO – Data Protection and Privacy Relationships Model.

1. Introduzione

Norbert Wiener nel libro dal titolo *“Introduzione alla cibernetica. L'uso umano degli esseri umani”*² afferma:

“Generalmente noi crediamo che la comunicazione e il linguaggio siano diretti da persona a persona. È possibile tuttavia che una persona parli a una macchina, una macchina a una persona e una macchina a una macchina”

Norbert Wiener è unanimemente considerato il padre della cibernetica e dei controlli automatici adattivi e la definisce come “la disciplina che studia i processi riguardanti ‘la comunicazione e il controllo nell’animale e nella macchina”.

Le considerazioni contenute nel testo citato sono da reputarsi decisamente illuminanti e futuristiche, posto che il volume risale al 1950, epoca nella quale non esistevano i computer.

Il titolo dell'intervento descrive un percorso ricco di spunti di riflessione in merito ai rapporti tra l'uomo e l'intelligenza artificiale, che consentono di riflettere sui temi privacy, precisando che, quando qui utilizziamo il termine privacy, intendiamo riferirci alla disciplina deputata alla protezione delle persone fisiche, con riguardo al trattamento dati personali.

² Norbert Wiener, *Introduzione alla cibernetica. L'uso umano degli esseri umani*, Bollati Boringhieri; 3° edizione (3 maggio 2012), pag. 101.

1.1 Premesse

Riteniamo necessario evidenziare alcune considerazioni preliminari rispetto al tema oggetto del presente lavoro.

Per condurre un'analisi corretta è, innanzitutto, necessario fare riferimento al completo impianto normativo relativo alla protezione delle persone fisiche, con riguardo al trattamento dati personali.

È bene chiarire, inoltre, che, relativamente alle fonti normative nazionali ed europee, la disciplina sulla protezione dei dati personali non è unicamente il Regolamento (UE) 2016/679 (di seguito anche solo GDPR)³.

Tra le altre fonti europee e internazionali, ricordiamo, altresì, il Trattato sul Funzionamento dell'Unione europea (art. 16 par. 1)⁴, la Convenzione 108⁵.

Relativamente alle fonti interne, per ultimo ma non per importanza, il D.Lgs. 196/2003 (noto anche come “Codice Privacy”), così come modificato dal D.Lgs. 101/2018⁶.

Ulteriore aspetto riguarda la distinzione terminologica tra “protezione dei dati personali” (dalla lingua inglese, *data protection*) e “protezione delle persone fisiche con riguardo al trattamento dei dati personali”. Al riguardo, è bene sottolineare che non è giuridicamente corretto fare riferimento alla *protezione del dato*, posto che le norme vigenti disciplinano unicamente la protezione delle persone fisiche, non esistendo una specifica disciplina alla *protezione del dato*.

Per concludere, riteniamo indispensabile evidenziare che la protezione delle persone fisiche con riguardo al trattamento dei dati personali è diversa dalla *sicurezza*. Molto spesso si ritiene, infatti, che l'implementazione di misure di sicurezza molto forti equivalga a conseguire una conformità alla normativa in materia di protezione delle persone fisiche, con riguardo al trattamento dei dati personali.

Tale assunto è errato, e possiamo esprimerlo con la seguente formula:

Protezione delle persone fisiche con riguardo al trattamento dei dati personali ≠ Security

Indubbiamente è vero il contrario, posto che la disciplina in materia di protezione delle persone fisiche, con riguardo al trattamento dei dati personali, impone sia al titolare del trattamento sia al responsabile del trattamento di mettere in atto “*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato*”

³ [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 (regolamento generale sulla protezione dei dati).

⁴ [Trattato sul Funzionamento dell'Unione Europea \(TFUE\)](#) – Articolo 16(1) “Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano”.

⁵ [Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale \(Convenzione 108/1981\)](#).

⁶ [Decreto Legislativo 30 giugno 2003, n. 196](#).

al rischio del trattamento dei dati". Pertanto, è certo che il tema della sicurezza del trattamento dei dati personali delle persone fisiche è contenuta all'interno dell'intero corpo normativo e ne è parte integrante (art. 32 del GDPR).

1.2 Necessità di un approccio multidisciplinare

È noto che il GDPR ha sostituito e abrogato la Direttiva europea 95/46/CE che già disciplinava la protezione delle persone fisiche, con riguardo al trattamento di dati personali.

Il percorso evolutivo ha preso avvio già negli anni Novanta.

Pertanto, *in primis*, bisogna essere consapevoli del fatto che i tempi sono decisamente cambiati e, conseguentemente, è necessario essere pronti ad affrontare le sfide, conosciute e non, che l'innovazione tecnologica ci pone.

Il tema della privacy e della protezione dei dati personali costituisce una vera e propria nuova era, frutto di una profonda trasformazione giuridica, tecnologica e culturale. Non si tratta, infatti, di una mera evoluzione conseguente allo sviluppo di nuove tecnologie ma di una nuova fase evolutiva della "privacy"⁷ tradizionalmente intesa, sebbene connessa e consequenziale ad essa. A nostro avviso questa nuova era non coincide con il 25 maggio 2018, data della applicazione del GDPR, ma andrebbe cronologicamente collocata nel periodo iniziale del complesso procedimento di formazione del noto Regolamento Ue 2016/679.

I tempi sono cambiati. Alla luce di quanto detto, è evidente che oggi la protezione delle persone fisiche con riguardo al trattamento di dati personali e la privacy richiedono un approccio decisamente nuovo. In effetti, ci si può correttamente occupare di questo tema solo se si ha una visione ampia, tale da consentire di guardare oltre il nostro orizzonte culturale e professionale.

Ed è proprio su tale argomento che si dovrebbe cambiare mentalità, dovendo dotarci di un nuovo assetto concettuale e utilizzando un approccio c.d. *open-minded* che consenta un confronto innovativo con il "dominio" della protezione delle persone fisiche con riguardo al trattamento di dati personali.

2. È possibile definire l'intelligenza artificiale?

L'ambito dell'intelligenza artificiale, dal nostro punto di vista, non è ancora molto del tutto chiaro, sebbene si registri una consistente produzione soprattutto da parte della dottrina.

Il punto nodale, a nostro avviso, è capire se sia possibile individuare una definizione di "intelligenza artificiale", posto che tale è il tema oggetto di discussione.

⁷ Con questa espressione intendiamo riferirci sia alla riservatezza sia alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

In realtà, è determinante l'analisi sulla possibilità di definire l'intelligenza artificiale contenuta nel volume⁸ scritto da due eminenti scienziati che si sono occupati *ex professo* del tema in questione, Russell e Norvig, i quali descrivono gli aspetti principali che potrebbero essere presi in considerazione per una definizione di intelligenza artificiale.

A tal proposito, leggiamo⁹:

“Storicamente, i ricercatori si sono dedicati a diverse versioni di IA. Alcuni hanno definito l'intelligenza in termini di fedeltà alla performance umana, mentre altri preferiscono una definizione astratta e formale di intelligenza chiamata razionalità - in parole povere, fare la “cosa giusta”. Anche l'argomento stesso varia: alcuni considerano l'intelligenza come una proprietà dei processi interni di pensiero e ragionamento, mentre altri si concentrano sul comportamento intelligente, una caratterizzazione esterna. Da queste due dimensioni - umano vs. razionale e pensiero vs. comportamento - ci sono quattro possibili combinazioni, e ci sono stati aderenti e programmi di ricerca per tutti e quattro.”

Come emerge dal testo citato, non esiste una definizione di intelligenza artificiale, ma esclusivamente un campo di indagine su due dimensioni *“umano vs. razionale e pensiero vs. comportamento”* dalle quali possono scaturire quattro possibili combinazioni che dovranno a loro volta essere oggetto di analisi.

Orbene, proseguendo nella nostra indagine, consideriamo quanto affermato da Max Tegmark, nel suo libro dal titolo *“Vita 3.0. Essere umani nell'era dell'intelligenza artificiale”*¹⁰ poiché offre una analisi estremamente interessante. L'autore, descrivendo una controversia su *“Vita 3.0”*¹¹ e le scuole di pensiero sull'intelligenza artificiale, afferma:

“Cosa interessante, la controversia su Vita 3.0 ruota attorno non a una, ma a due domande distinte: quando e che cosa? Quando (eventualmente) succederà, e che cosa significherà per l'umanità? Da quel che vedo, esistono tre diverse scuole di pensiero e tutte vanno prese sul serio perché a ciascuna appartengono numerosi esperti di livello mondiale. [...] Il sacro graal della ricerca sull'IA è la costruzione di una “IA generale” (meglio nota come “intelligenza artificiale generale” o IAG) della massima ampiezza: in grado di realizzare praticamente qualsiasi fine, compreso quello dell'apprendimento.”

La posizione di Tegmark, che è stato anche il promotore del documento pubblicato

⁸ Stuart Russell – Peter Norvig, *Artificial Intelligence: A Modern Approach*, Pearson; 4th edition (13 maggio 2021)

⁹ La traduzione è nostra; il testo originario è il seguente: “ABC”.

¹⁰ Max Tegmark, *“Vita 3.0. Essere umani nell'era dell'intelligenza artificiale”*, Cortina Raffaello (19 aprile 2018).

¹¹ Secondo Tegmark: *“In breve, possiamo dividere lo sviluppo della vita in tre stadi, distinti in base alla capacità della vita di progettare se stessa: Vita 1.0 (stadio biologico): hardware e software evolvono; Vita 2.0 (stadio culturale): l'hardware evolve, gran parte del software è progettato; Vita 3.0 (stadio tecnologico): hardware e software sono progettati.”*

su Internet dal titolo “*An Open Letter - Research priorities for robust and beneficial artificial intelligence*”¹² (il cui primo firmatario è proprio Stuart Russell, unitamente ad a numerosi docenti universitari), pertanto, ci consente di confermare che non è possibile, ancora oggi, individuare una definizione di intelligenza artificiale.

Ai fini della nostra indagine, risulta interessante una parte della menzionata “*Open Letter*” e specificamente¹³:

*“La ricerca sull’intelligenza artificiale (AI) ha esplorato una varietà di problemi e approcci fin dal suo inizio, ma negli ultimi 20 anni circa si è concentrata sui problemi che circondano la costruzione di **agenti intelligenti** - sistemi che percepiscono e agiscono in qualche ambiente. In questo contesto, “intelligenza” è legata alle nozioni statistiche ed economiche di razionalità - colloquialmente, la capacità di prendere buone decisioni, piani o inferenze. L’adozione di rappresentazioni probabilistiche e decisionali e di metodi di apprendimento statistico ha portato a un ampio grado di integrazione e fertilizzazione incrociata tra l’IA, l’apprendimento automatico, la statistica, la teoria del controllo, le neuroscienze e altri campi. L’istituzione di quadri teorici condivisi, combinata con la disponibilità di dati e potenza di elaborazione, ha prodotto notevoli successi in vari compiti di componenti come il riconoscimento vocale, la classificazione delle immagini, i veicoli autonomi, la traduzione automatica, la locomozione su gambe e i sistemi di risposta alle domande. [...] Questa ricerca è per necessità interdisciplinare, perché coinvolge sia la società che l’IA. Spazia dall’economia, la legge e la filosofia alla sicurezza informatica, i metodi formali e, naturalmente, vari rami dell’IA stessa.”.*

Dal tenore del contributo citato, emergono diverse questioni di rilievo e, precisamente, il riferimento agli agenti intelligenti, l’interazione l’intelligenza artificiale e altri ambiti come le neuroscienze, l’interdisciplinarietà.

2.1 Intelligenza artificiale e sistemi di intelligenza artificiale

Il richiamo agli agenti intelligenti ci porta a dover sviluppare ulteriori riflessioni. Gli agenti intelligenti (i cosiddetti “*intelligent agents*”) sono, sostanzialmente, com-

¹² “[An Open Letter - Research priorities for robust and beneficial artificial intelligence](#)”.

¹³ La traduzione è nostra. Il testo originale è il seguente: “*Artificial intelligence (AI) research has explored a variety of problems and approaches since its inception, but for the last 20 years or so has been focused on the problems surrounding the construction of intelligent agents – systems that perceive and act in some environment. In this context, “intelligence” is related to statistical and economic notions of rationality – colloquially, the ability to make good decisions, plans, or inferences. The adoption of probabilistic and decision-theoretic representations and statistical learning methods has led to a large degree of integration and cross-fertilization among AI, machine learning, statistics, control theory, neuroscience, and other fields. The establishment of shared theoretical frameworks, combined with the availability of data and processing power, has yielded remarkable successes in various component tasks such as speech recognition, image classification, autonomous vehicles, machine translation, legged locomotion, and question-answering systems. [...] This research is by necessity interdisciplinary, because it involves both society and AI. It ranges from economics, law and philosophy to computer security, formal methods and, of course, various branches of AI itself.*”.

posti da hardware e software. I sensori, a seconda delle istruzioni che vengono fornite dal software, compiono determinate attività.

Riguardo ai sistemi intelligenti (i cosiddetti *Intelligent Systems*), ci si dovrebbe interrogare sul significato di tale espressione. Una parte della dottrina specialista della tematica¹⁴ ha definito i sistemi intelligenti facendo riferimento al concetto emerso nella tecnologia dell'informazione come un tipo di sistema derivato dalle applicazioni di successo dell'intelligenza artificiale, attraverso l'applicazione del Machine Learning ai processi artificiali.

La definizione proposta dalla dottrina citata è la seguente¹⁵:

“Un sistema intelligente opera in un ambiente con altri agenti possiede abilità cognitive come la percezione, il controllo delle azioni, il ragionamento deliberativo o l'uso del linguaggio, segue principi comportamentali basati sulla razionalità e le norme sociali, e ha la capacità di adattarsi attraverso l'apprendimento.”

Pertanto, è evidente che, quando si parla di sistemi intelligenti, si fa riferimento ai sistemi di intelligenza artificiale.

Dal tema dei sistemi intelligenti o sistemi di intelligenza artificiale, scaturisce la questione più rilevante che è relativa alla definizione di intelligenza artificiale.

2.2 La proposta di Regolamento UE sulla IA e il tentativo di individuare una definizione

L'Unione Europea ha deciso di porre le basi per disciplinare il tema relativo all'intelligenza artificiale mediante la ben nota *“proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione”*¹⁶, pubblicata il 21 aprile 2021.

Tale proposta di regolamento introduce, all'articolo 3, la definizione di “sistema di intelligenza artificiale” nei termini seguenti:

“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.

Il contenuto del citato articolo assume particolare rilievo, posto che non emerge una vera e propria definizione di intelligenza artificiale (e non ci sembra che sia

¹⁴ Martin Molina, “What is an intelligent system?”, Universidad Politécnica de Madrid, February 2022; il testo citato in lingua originale è il seguente: *“An intelligent system (1) operates in an environment with other agents, (2) possesses cognitive abilities such as perception, action control, deliberative reasoning or language use, (3) follows behavioral principles based on rationality and social norms, and (4) has the capacity to adapt through learning.”*.

¹⁵ La traduzione del testo è nostra.

¹⁶ Il testo della proposta è disponibile sul servizio europeo Eur-Lex a [questa pagina](#).

possibile, quanto meno ad oggi), ma il sistema di intelligenza artificiale o *artificial intelligence system*.

In realtà, tale definizione contenuta nell'articolo 3 non è "autosufficiente", poiché richiama semplicemente l'allegato I, il quale contiene riferimenti tecnici che circoscrivono il campo di applicazione della stessa definizione.

Dal nostro punto di vista, è corretto individuare una definizione di "sistema di intelligenza artificiale" piuttosto che di "intelligenza artificiale" per i motivi già esposti. Tuttavia, il richiamo all'allegato I appare restringere l'ambito di applicazione della definizione ad un preciso perimetro i cui confini sono, appunto, indicati nell'allegato in questione.

Pertanto, la nostra proposta è quella di presentare nel presente testo una definizione di "sistema di intelligenza artificiale" parzialmente diversa da quella della proposta EU, e precisamente:

"artificial intelligence system" (AI system) means software developed with techniques and approaches, including, but not limited to, machine learning approach, logic-and knowledge-based approaches, statistical approaches, Bayesian estimation, search and optimization methods."

La definizione da noi prospettata avrebbe il vantaggio di non restringere il campo di applicazione alle sole condizioni previste dall'allegato I, rendendo quindi più ampio lo spazio operativo. In realtà, la definizione contenuta nella citata proposta europea appare restrittiva e unicamente dipendente da criteri collegati al rischio.

3. Lo scenario europeo sull'intelligenza artificiale

Cosa è accaduto negli ultimi anni in Europa?

Proponiamo di seguito due immagini che riportano complessivamente la *timeline* dal 2015 al 2020 dei più rilevanti interventi istituzionali sull'intelligenza artificiale.

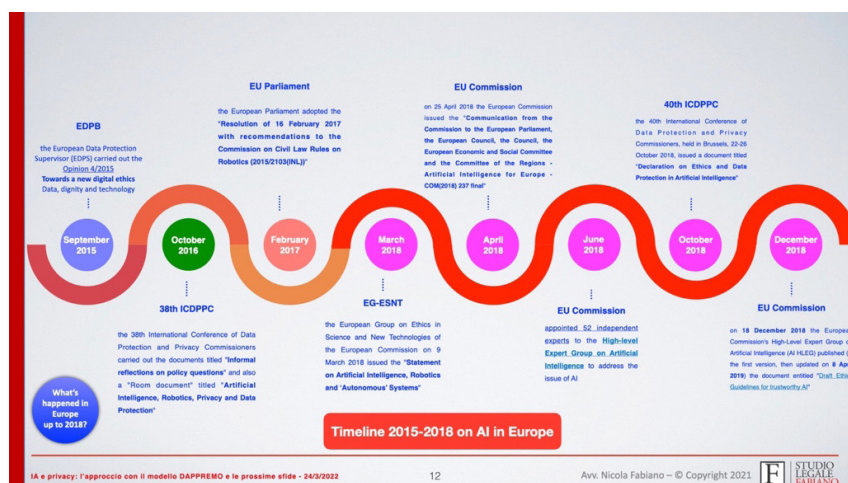


Figura 1 – Timeline 2015-2018

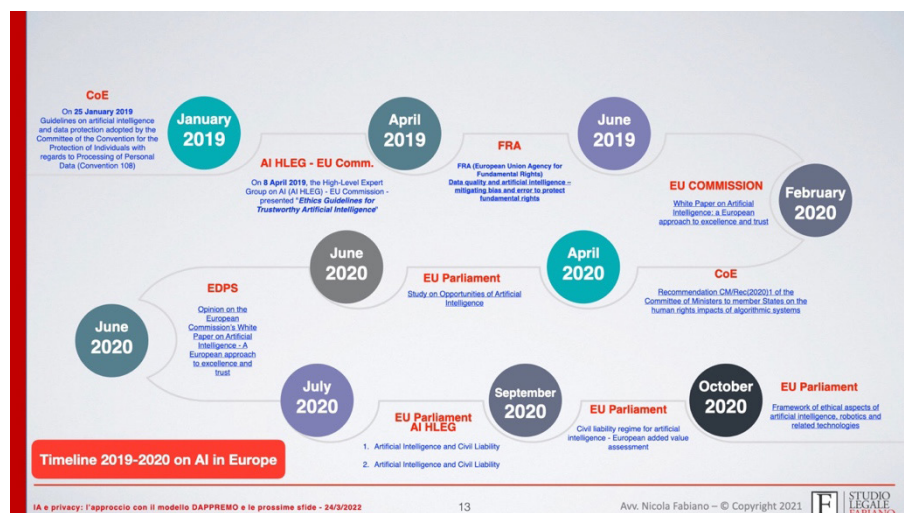


Figura 2 – Timeline 2019-2020

Com'è evidente, rileva un importante interesse istituzionale circa il rapporto tra l'intelligenza artificiale, la protezione dei dati personali e la privacy.

Mentre nel primo periodo, 2015-2018, gli interventi sono serviti a prendere posizione sul tema, successivamente, dal 2019 al 2020 si registra un loro aumento considerevole.

In sostanza, in Europa parte della attività istituzionale ha determinato una produzione documentale da vari organismi, specificamente – ma non unicamente – riferita ai rapporti tra protezione dei dati personali intelligenza artificiale.

Allo stesso tempo, riteniamo necessario e utile menzionare, altresì, il lavoro del CA-HAI “*Ad Hoc Committee on Artificial Intelligence*” che, nel mese di marzo 2021, ha pubblicato il report “*Artificial Intelligence in Public Sector*”¹⁷.

Da tale report emerge che le Agenzie del settore pubblico utilizzano il c.d. processo decisionale automatizzato nell'ambito della categoria dell'automazione assistita o condizionata. Inoltre, solo in pochi casi vengono automatizzati processi o servizi completi. Infine, viene dichiarato che non ci sono sistemi completamente autonomi in uso nel settore pubblico. Nel già menzionato report si legge che, rispetto al settore privato, il settore pubblico è in ritardo nell'adozione dell'intelligenza artificiale, anche se i governi stanno cercando di recuperare questo *gap* e, quindi, colmare il divario esistente. Infine, il report evidenzia che, secondo la mappatura iniziale dell'OCSE sull'IA, sono stati identificati cinquanta paesi - compresa l'UE - che hanno partecipato all'introduzione di strategie nazionali di intelligenza artificiale e trentasei di questi, invece, hanno presentato specifiche strategie per l'intelligenza artificiale nel settore pubblico¹⁸.

¹⁷ Il report è disponibile a questo URL <https://rm.coe.int/cahai-pdg-2021-03-subwg2-ai-in-public-sector-final-draft-12032021-2751/1680a1c066>

¹⁸ Il 23 settembre 2020, il Comitato dei Ministri ha approvato la prima relazione sui progressi compiuti. Il rapporto è disponibile a [questa pagina](#). Inoltre, si segnala la “[Raccomandazione CM/Rec\(2020\)1](#)”

Non possiamo sottacere il lavoro svolto dallo “*Special Committee on Artificial Intelligence in a Digital Age*” (AIDA) del Parlamento europeo che ha avuto una consistente produzione sul tema, della quale menzioniamo il più recente contributo dal titolo “*Report on artificial intelligence in a digital age (2020/2266(ini))*”¹⁹ del 5 aprile 2022 con il quale, dopo aver descritto dettagliatamente lo scenario attuale, si conclude con un significativo “*an urgent call for action!*”²⁰.

4. Etica e intelligenza artificiale

L’etica è un tema di primario rilievo anche in relazione ai rapporti tra intelligenza artificiale e privacy e protezione dei dati personali.

A tal proposito, menzioniamo la voce “*Ethics of Artificial Intelligence and Robotics*”²¹ della [Stanford Encyclopedia of Philosophy](#) che descrive il tema in maniera estremamente dettagliata e, sebbene si riferisca ai rapporti tra intelligenza artificiale e robotica, nondimeno affronta i seguenti aspetti dei quali ciascuno meriterebbe uno specifico approfondimento: Privacy e sorveglianza, Manipolazione del comportamento, Opacità dei sistemi di intelligenza artificiale, Bias nei sistemi decisionali, Interazione uomo-robot, Automazione e occupazione, Sistemi autonomi, Etica delle macchine, Agenti morali artificiali, Singolarità.

La complessità degli aspetti in cui si declina l’etica, consente in questa sede un mero richiamo alla sua necessaria considerazione anche in ambito protezione dei dati personali così come abbiamo evidenziato nella descrizione del nostro modello DAPPREMO.

[del Comitato dei Ministri agli Stati membri sull’impatto sui diritti umani dei sistemi algoritmici](#)” (Adottata dal Comitato dei Ministri l’8 aprile 2020 in occasione della 1373a riunione dei Ministri aggiunti), nonché la “[Raccomandazione CM/Rec\(2021\)8 del Comitato dei Ministri agli Stati membri sulla protezione delle persone fisiche con riguardo al trattamento automatico dei dati personali nel contesto della profilazione](#)” (Adottata dal Comitato dei Ministri il 3 novembre 2021 in occasione della 1416a riunione dei Ministri aggiunti).

¹⁹ Il report è disponibile a [questa pagina](#).

²⁰ Il 22 marzo 2022 il comitato speciale AIDA (*on Artificial Intelligence in a Digital Age*) del Parlamento europeo *ha adottato le proprie raccomandazioni finali*” e nel [comunicato stampa](#), fra l’altro, si legge “*Il testo avverte che l’UE è rimasta indietro nella corsa globale alla leadership tecnologica. Di conseguenza, c’è il rischio che in futuro gli standard vengano sviluppati altrove, spesso da attori non democratici, mentre l’UE deve agire come standard-setter globale in materia di IA. [...] L’UE non dovrebbe sempre regolamentare l’IA come tecnologia. Il livello di intervento normativo dovrebbe invece essere proporzionato al tipo di rischio associato all’utilizzo di un sistema di IA in un determinato modo.*”.

²¹ La voce “*Ethics of Artificial Intelligence and Robotics*” è disponibile a [questa pagina](#).

5. I rischi dell'intelligenza artificiale (cenni) e le sfide

Anche l'intelligenza artificiale non è esente da rischi, soprattutto se si analizza il rapporto con la protezione dei dati personali e la privacy.

Tra essi possiamo menzionare principalmente: bias e equità (com'è noto il bias potrebbe determinare incertezza sulla soluzione), automazione del lavoro, incidenti e considerazioni sulla sicurezza fisica, responsabilità dei sistemi intelligenti, uso malevolo dell'IA. Sono ben noti gli aspetti che riguardano gli incidenti, nonché le considerazioni sulla sicurezza fisica, senza escludere i profili di responsabilità per l'uso malevolo.

A tal proposito richiamiamo quanto previsto dalla proposta europea del 21 aprile 2021 che contempla i livelli di rischio dell'intelligenza artificiale.

Nei rapporti tra intelligenza artificiale e protezione dei dati personali non possiamo prescindere dai principi contenuti nel Regolamento UE 2016/679 (GDPR), tra i quali menzioniamo la trasparenza (che comporta l'adozione di un approccio eticamente orientato) secondo l'art. 5, il principio "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" (in inglese "*Data Protection by design and by default*") contenuto nell'art. 25.

In un simile scenario possiamo anche sommariamente intravedere le sfide che dobbiamo affrontare in questo ambito.

Indubbiamente, la prima delle sfide è acquisire la necessaria consapevolezza²², posto che con essa si è in condizioni di affrontare con il giusto approccio ogni possibile aspetto, anche con un approccio etico e tenendo anche in ottima considerazione il tema della sostenibilità.

Ci sono altre sfide connesse al rapporto tra intelligenza artificiale e protezione dei dati personali, tra le quali meritano di essere menzionate le neuroscienze e neurobioscienze. Infatti, il profilo della protezione dei dati personali merita adeguata collocazione nell'elevato valore della dignità umana. Pertanto, proteggere le persone fisiche con riguardo al trattamento dei dati personali comporta indubbiamente anche essere obbligati ad attuare un approccio eticamente orientato nel campo delle neuroscienze e delle neurobioscienze.

²² Rimandiamo al volume "[GDPR & Privacy: consapevolezza e opportunità. L'approccio con il Data Protection and Privacy Relationships Model \(DAPPREMO\)](#)", Firenze, 2020

6. La nostra proposta: DAPPREMO – Data Protection and Privacy Relationships Model

In uno scenario articolato e complesso come quello descritto, la nostra proposta è contenuta nel modello relazionale denominato DAPPREMO (acronimo di Data Protection and Privacy Relationships Model), basato sulla teoria degli insiemi e su alta matematica.

Il modello è centrato sulla disciplina in materia di protezione dei dati personali unitamente all'etica e si descrive matematicamente come relazioni di equivalenza e graficamente come un fibrato vettoriale. Nella riproduzione grafica, ogni punto di intersezione delle tangenti rappresenta un oggetto presente nella realtà che dovremmo prendere in considerazione ogni qualvolta esaminiamo un contesto nel quale c'è il tema della protezione dei dati personali.

Auspichiamo, quindi, di poter utilizzare un approccio alla protezione dei dati personali, e specificamente ai contesti nei quali sussiste un rapporto con l'intelligenza artificiale, innovativo che tenga conto della possibilità di analisi di ogni elemento presente nella realtà.

Così come in apertura abbiamo citato Norbert Wiener, concludiamo il nostro intervento allo stesso modo, lasciando alle parole del padre della cibernetica che così si esprimeva²³:

“Allorché le persone umane sono organizzate nel sistema che li impiega non secondo le loro piene facoltà di esseri umani responsabili, ma come altrettanti ingranaggi, leve e connessioni, non ha molta importanza il fatto che la loro materia prima sia costituita da carne e da sangue. Ciò che è usato come elemento in una macchina, è un elemento nella macchina. Sia che noi affidiamo le nostre decisioni a macchine di metallo o a quelle macchine viventi che sono gli uffici, i grandi laboratori, gli eserciti o le società industriali, non avremo mai la risposta giusta alle nostre domande a meno di non porre le domande giuste”.

²³ Norbert Wiener, Introduzione alla cibernetica. L'uso umano degli esseri umani, Bollati Boringhieri; 3° edizione (3 maggio 2012), pag. 228.

LA TUTELA DEL PROGRAMMA PER ELABORATORE NELL'AMMINISTRAZIONE ALGORITMICA

Alessia Palladino¹

Abstract [IT]: L'articolo si propone di indagare la morfologia della proprietà intellettuale nell'era dell'amministrazione algoritmica. Considerando che la pubblica amministrazione potrebbe non essere in grado di sviluppare internamente le tecnologie necessarie e dovrà procurarsele sul mercato, taluni hanno sostenuto che questi diritti potrebbero stimolare un predominio senza precedenti degli operatori privati sull'intero processo decisionale pubblico. Altri, compresa la giurisprudenza, rivendicano la divulgazione complessiva del codice sorgente per garantire trasparenza, libertà di informazione e impegno civico, in coerenza con le politiche di Open Government. Questo articolo tralascia il dibattito giuridico, sulla qualificazione del codice sorgente come atto amministrativo, recentemente avvenuto in Italia. Si propone di contribuire al dibattito sui problemi connessi dell'accessibilità al codice sorgente, al fine di comprendere se i diritti di proprietà intellettuale debbano soccombere ogni volta che si presentano soluzioni tecnologiche nelle attività amministrative.

Abstract [EN]: This article aims to investigate the morphology of intellectual property in the era of algorithmic administration. Considering that the public administration may not be able to develop the necessary technologies in-house and will have to procure them on the market, some have argued that these rights could spur unprecedented dominance of private actors over the entire public decision-making process. Others, including case law, claim overall disclosure of source code to ensure transparency, freedom of information, and civic engagement, consistent with Open Government policies. This article leaves out the legal debate, on the qualification of source code as an administrative act, that recently took place in Italy. It aims to contribute to the debate on the related problems of source code accessibility, in order to understand whether intellectual property rights should succumb whenever technological solutions are presented in administrative activities.

Keywords [IT]: intelligenza artificiale – algoritmi – software – open government – amministrazione algoritmica.

¹ Alessia Palladino, Dottore di ricerca in “Humanities and Technologies: an integrated research path”, Università degli Studi Suor Orsola Benincasa. Cultore della Materia in “Computer Law” [SSD IUS/20], presso Università degli Studi di Cagliari, Corso di Laurea in Computer Engineering, Cybersecurity and Artificial Intelligence.

Keywords [EN]: artificial intelligence - algorithms - software - open government - algorithmic administration.

Sommario: 1. L'intelligenza artificiale nel settore pubblico. Verso l'accountability amministrativa. – 2. La discriminazione algoritmica tra trasparenza, accountability e proprietà intellettuale. – 3. L'accountability amministrativa tra trasparenza, leale collaborazione e buona fede- – 4. Considerazioni conclusive.

1. L'intelligenza artificiale nel settore pubblico. Verso l'*accountability* amministrativa

Nel corso dell'ultimo decennio, l'intelligenza artificiale ha guadagnato slancio sia a livello europeo che nazionale², divenendo strumento sempre più pervasivo nella vita quotidiana³.

Com'è noto, essa offre diverse opportunità per creare valore in differenti ambiti. A livello sovranazionale, le politiche dell'Unione europea incoraggiano sempre più lo sviluppo dell'intelligenza artificiale e di tecnologie emergenti, corroborando gli intenti di sovranità digitale europea⁴ e fornendo diverse opzioni strategiche per affrontare le principali sfide tecniche e giuridiche⁵.

² Le tecnologie dell'informazione e della comunicazione (ICT) hanno guidato l'aumento della produttività europea dal 1995. Negli ultimi tre decenni, l'obiettivo di raggiungere la convergenza tecnologica ha offuscato i confini tra telecomunicazioni, radiodiffusione e IT. La Commissione ha presentato le principali proposte legislative nel 2015, lanciando il mercato unico digitale nel 2015, per promuovere il commercio elettronico, il diritto d'autore, la ePrivacy, l'armonizzazione dei diritti digitali, le norme IVA armonizzate e la cibersicurezza. Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia per il mercato unico digitale per l'Europa*, COM/2015/0192 final del 6.5.2015, consultabile all'indirizzo <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192>. Cfr. anche Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni, *Creare fiducia nell'intelligenza artificiale antropocentrica*, COM(2019) 168 final del 08.04.2019, consultabile all'indirizzo <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52019DC0168&from=EN>.

³ M.U.Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, And Strategies* (2016) *Harvard Journal of Law & Technology*, Volume 29, Number 2, Spring 2016; M. Craglia, et al, *Artificial Intelligence - A European perspective*, (2019), European Commission, Joint Research Centre, Artificial intelligence: European perspective, Publications Office; L. Floridi, *The Fourth Revolution, How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

⁴ M. Zalnieriute, L. Bennettmoses, G. Williams, *The Rule of Law and Automation of Government Decision-Making*, in *The modern law review* (2019), p. 425.

⁵ A questo proposito, diversi atti di soft law sono stati emanati dalle istituzioni europee. Si veda soprattutto la risoluzione del Parlamento Europeo del 20 ottobre 2020 sui diritti di proprietà intellettuale per lo sviluppo delle tecnologie di intelligenza artificiale, fino alla recente e più vincolante Proposta di Regolamento del Parlamento Europeo e del Consiglio recante Norme Armonizzate sull'Intelligenza Artificiale (in estrema sintesi, la cosiddetta "Legge sull'intelligenza artificiale") [Proposta di regolamento del Parlamento europeo e del Consiglio recante norme armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e che modifica alcuni atti

Anche il settore pubblico manifesta crescente interesse per l'impiego dell'intelligenza artificiale⁶.

L'impiego della tecnologia scuote le fondamenta dell'attività procedimentale – investendone, ad esempio, la fase istruttoria e decisionale –⁷, e mira a favorirne l'imparzialità, l'efficienza e la trasparenza, proponendo nuovi modelli di azione e di relazione della sfera pubblica (sulla scorta, tra l'altro, dei paradigmi dell'*E-government*⁸ e dell'*Open Government*⁹). Nondimeno, l'intelligenza artificiale può contribuire significativamente a migliorare la qualità dei servizi pubblici¹⁰, favorire la fiducia dei cittadini¹¹, aumentare l'efficienza e l'efficacia nell'erogazione del servizio¹², garantire previsioni più accurate a supporto dei processi decisionali anche in sistemi complessi¹³.

Ciononostante, se per un verso l'avvento dell'intelligenza artificiale espone a taluni rischi, connessi alla gemmazione di nuove forme di discriminazione¹⁴, tali criticità si

legislativi dell'Unione, COM/2021/206 def. del 21.04.2021, consultabile all'indirizzo <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206>.

- ⁶ I. Martin Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in Ist. Federalismo, 2009, p. 643.
- ⁷ G. Avanzini, *Intelligenza artificiale, machine learning e istruttoria procedimentale: vantaggi, limiti ed esigenza di una specifica data governance*, in F. Donati, A. Pajno, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, II, 2022, pp. 47-48.
- ⁸ Ex multis, cfr. G. Gometz, *Democrazia elettronica. Teoria e tecniche*, Edizioni ETS 2017; L. Torres, V. Pina, S. Royo, *E-Government and the transformation of public administration in EU countries: Beyond NPM or just a second wave of reforms?* in *Online Information Review*, 2005, p. 531 ss.; C.A. Hardy, S.P. Williams, *Assembling e-government research designs: A transdisciplinary view and interactive approach*, in *Public Administration Review*, 2011, p. 405 ss.; M.J. Moon, J. Lee, C.Y. Roh, *The evolution of internal IT applications and e-government studies in public administration: Research themes and methods*, in *Administration & Society*, 2014, p. 3 ss. V. OECD, *Open Government: The Global Context and the Way Forward*, *Oecd Publishing*, Paris, 2016, <http://dx.doi.org/10.1787/9789264268104-en>; L. Sartori *Open government: what else?*, in *Istituzioni del federalismo*, 3-4, 2013 p. 754.
- ⁹ Galetta Diana-Urania, *Open Government, Open Data e azione amministrativa*, in *Istituzioni del Federalismo* n. 3/2019 pp. 663-683.
- ¹⁰ Aa. Vv., *Artificial Intelligence and Environmental Decision Support Systems*, in *Applied Intelligence* 13/2000, pp. 77-91.
- ¹¹ A.L. Stein, *Artificial Intelligence and Climate Change*, (2020) *Yale Journal on Regulation*, Vol. 37, Issue 3, 890-939.
- ¹² P. Gowder, 'Transformative Legal Technology and the Rule of Law' (2018) - 68 *supp 1 University of Toronto Law Journal*, 82.
- ¹³ W. Eggers et al, *AI-augmented government: Using cognitive technologies to redesign public sector work* (2017) *Deloitte Center for Government Insights*, consultabile all'indirizzo https://www2.deloitte.com/content/dam/insights/us/articles/3832_AI-augmented-government/DUP_AI-augmented-government.pdf (ultimo accesso 3 gennaio 2022); J. W. Forrester & P.M. Senge, P. M., *Tests for building confidence in system dynamics models*, *TIMS Studies in the Management Sciences* 2018.
- ¹⁴ Cfr. J. Kleinberg – J. Ludwig – S. Mullainathan, C. R. Sunstein, *Discrimination in the Age of Algorithms*, in *Journal of Legal Analysis*, 2018, 113 ss.; B. Heinrichs, *Discrimination in the age of artificial intelligence*, *AI & Society*, 1, 2022, 143 ss. Le cause connesse alla verifica di fenomeni discriminatori sono molteplici. Per approfondimenti sul fenomeno dei cd. bias, cfr. S.G. MAYSON, *Bias In, Bias Out*, in *The Yale Law Journal*, 128, 2019, 2218 ss. Per ulteriori riflessioni sulla fallacia della computazione algoritmica, si v. anche T.B. Gillis, *The input fallacy*, in *Minnesota Law Review*, 106, 2022, 1175 ss.

acuiscono ogniqualvolta a farne uso è l'amministrazione pubblica, giacché quest'ultima potrebbe fungere da inconsapevole promotrice di potenziali discriminazioni, ovvero di pregiudizi e compromissioni dei diritti¹⁵.

Pertanto, un preliminare aspetto da constatare insiste sul duplice ruolo che l'Amministrazione algoritmica è chiamata ad asseverare, *i.e.* di garante della legalità e della legittimazione del proprio operato in un ecosistema soggettivo complesso. Si tratta di un aspetto che desta particolare interesse, che insiste sul rapporto tra tecnologia e agire amministrativo¹⁶ e si ricollega puntualmente alle esigenze di tutela del programma per elaboratore nell'amministrazione algoritmica¹⁷.

Nello scenario dell'amministrazione algoritmica si dovrebbe ragionare in termini di *accountability* pubblica: tale concetto non insiste unicamente sulla dimensione relazionale della Pubblica Amministrazione con il cittadino, ma coinvolge anche altri soggetti, specialmente se l'amministrazione si rende "algoritmica" attraverso l'acquisizione – mediante commessa pubblica – di *software* di tipo proprietario, lasciando in capo al privato appaltatore i diritti di proprietà intellettuale sul software e limitandosi all'acquisizione della facoltà d'uso, secondo le modalità dettagliate nella procedura di acquisizione oggetto della procedura di gara.

In sintesi, nell'ambito dell'amministrazione algoritmica l'*accountability* pubblica si declina in due differenti dimensioni relazionali, che investono principalmente il rapporto dell'amministrazione con il cittadino e con il programmatore/*software house*. Discorrere in termini di *accountability* nell'amministrazione algoritmica impone una disamina del fenomeno secondo una prospettiva *globale*, per valutare quali condotte dell'amministrazione siano idonee a pregiudicare non solo il cittadino, ma anche l'operatore economico. Si tratta di due dimensioni relazionali differenti, che tuttavia presentano alcuni punti di contatto, che sovente generano conflitto – in ragione degli interessi contrapposti – che insistono principalmente sul rapporto tra trasparenza amministrativa e protezione degli interessi commerciali ed industriali delle *software house*.

¹⁵ Per un'approfondimento sui rischi connessi all'impiego dell'intelligenza artificiale nel contesto della Big data analysis, si v. F. Costantino, *Rischi o opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in *Diritto pubblico* n. 1/2019, pp. 43 ss.

¹⁶ La rilevanza delle tecnologie nell'attività amministrativa a rilevanza esterna era stata già colta da Massimo Severo Giannini alla fine degli anni Settanta nel noto Rapporto sui principali problemi dell'amministrazione dello Stato. In particolare, si evidenziava che "i sistemi informativi non servono più alle amministrazioni per fatti di gestione interna ma servono proprio per amministrare, si proiettano cioè sempre più verso l'esterno". Cfr. M.S.Giannini, *Rapporto sui principali problemi dell'amministrazione dello Stato*, in *Foro italiano*, 1979, V, pp.289 ss.; si v. anche S. Civitarese Matteucci, L.Torchia, *La tecnificazione dell'amministrazione*, in S. . Civitarese Matteucci, L. Torchia (a cura di), *La tecnificazione*, Firenze University Press, Firenze, 2016, p. 10.

¹⁷ A. Cerrillo, How can we open the black box of public administration? Transparency and accountability in the use of algorithms, in *Revista Catalana de Dret Públic*, 2019, 58, p. 15. Cfr. anche J. Cobbe, *Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making*, in corso di pubblicazione su *Legal Studies* e disponibile al link <https://ssrn.com/abstract=3226913> o <http://dx.doi.org/10.2139/ssrn.3226913>, p. 3; D. Marongiu, *Inteligencia artificial y administración pública*, in C. García Novoa, D. Santiago Iglesias (a cura di), *4ª Revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*, Cizur Menor, Thomson Reuters Aranzadi, 2018, p. 395.

E per questo, alimentano il dibattito giurisprudenziale e dottrinale, sia per le ricadute sui diritti fondamentali, sia soprattutto per le implicazioni di carattere sistematico, che saranno illustrate nel prossimo paragrafo.

2. La discriminazione algoritmica tra trasparenza, *accountability* e proprietà intellettuale

Nella dialettica tra trasparenza amministrativa e tutela della proprietà intellettuale nell'amministrazione algoritmica possono evidenziarsi, segnatamente, almeno tre aspetti principali da cui il dibattito giurisprudenziale si è dipanato. In dettaglio, il dibattito trae origine dalla presunta discriminazione algoritmica causata da illegittima allocazione dei docenti¹⁸.

Il primo aspetto riguarda l'accessibilità del codice sorgente ogniqualvolta la titolarità dei diritti di proprietà intellettuale permane in capo all'operatore economico, ovvero alla *software house*.

Il secondo, invece, insiste sul consequenziale giudizio di bilanciamento dell'amministrazione, secondo canoni di proporzionalità, degli interessi giuridicamente rilevanti. In particolare, il giudizio di bilanciamento richiede di ponderare gli interessi rilevanti dell'operatore economico, connessi ai diritti di proprietà intellettuale sul software e alla tutela della segretezza dei codici sorgente; per altro verso, invece, esso richiede di valutare l'esatta latitudine del principio di trasparenza, da valutare sia in relazione ai diritti di difesa del soggetto pregiudicato dal provvedimento amministrativo basato sulla decisione algoritmica, quanto in ragione dell'interesse generale alla correttezza, all'efficienza dell'agire amministrativo, nonché all'imputabilità e verificabilità delle decisioni amministrative.

Infine, il terzo aspetto riguarda la tutela rimediabile in caso di decisioni basate su *software* non trasparenti.

In realtà, se valutati nella logica dell'*accountability* amministrativa, gli aspetti critici citati inducono una serie di osservazioni a carattere sistematico.

Quanto al primo aspetto critico - accessibilità del codice sorgente ogniqualvolta la titolarità dei diritti di proprietà intellettuale permane in capo all'operatore economico -, esso induce necessarie riflessioni sulle modalità di acquisizione di un software da parte della Pubblica Amministrazione, tipizzate dal legislatore.

¹⁸ Ex multis, Consiglio di Stato, sez. VI, sentenza 8 aprile 2019 n. 2270. Sul punto cfr. F. Laus *La tecnologia nella pubblica amministrazione: algoritmi e processi decisionali nei procedimenti amministrativi. Il caso della procedura di mobilità*, in *Il lavoro nelle pubbliche amministrazioni*, 2020, fasc. 3, pp. 49-72; I. Forgiione, *Il caso dell'accesso al software MIUR [Ministero dell'Istruzione, dell'Università e della Ricerca] per l'assegnazione dei docenti Nota a TAR LA - Roma sez. III bis 14 febbraio 2017, n. 3769*, in *Giornale di diritto amministrativo* n. 5/2018, pp. 647-662.

Com'è noto, il Codice dell'Amministrazione Digitale (CAD) cristallizza agli artt. 68¹⁹ e 69²⁰ le modalità di acquisizione del software e la titolarità dello stesso, attribuendo all'amministrazione la scelta della soluzione più adeguata tra quelle disponibili sul mercato: in questo senso, l'amministrazione potrà ricorrere sia a soluzioni di tipo *open source*, sia di tipo proprietario²¹.

L'impianto in esame non risulta scalfito né a seguito della riforma del 2016, né alla luce delle recenti Linee Guida dell'Agenzia per l'Italia Digitale ("AgID")²². Infatti, sebbene la riforma del 2016 mirasse a favorire la propensione avverso soluzioni aperte, per asseverare le esigenze di riuso del *software* da parte di altre pubbliche amministrazioni e contrarre in tal modo anche la spesa pubblica – assolvendo, al contempo, alle istanze di trasparenza e interoperabilità –²³, l'articolo 69 CAD prevede che l'amministrazione committente tenda ad acquisire – salvo che ciò risulti

¹⁹ L'articolo 68 (Analisi comparativa delle soluzioni) stabilisce al comma 1 che "Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato: a) software sviluppato per conto della pubblica amministrazione; b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione; c) software libero o a codice sorgente aperto; c-bis) software fruibile in modalità cloud computing; d) software di tipo proprietario mediante ricorso a licenza d'uso; e) software combinazione delle precedenti soluzioni".

²⁰ L'articolo 69 ("Riuso delle soluzioni e standard aperti") prevede invece che "Le pubbliche amministrazioni che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno l'obbligo di rendere disponibile il relativo codice sorgente, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali. 2. Al fine di favorire il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni, ai sensi del comma 1, nei capitolati o nelle specifiche di progetto è previsto, salvo che ciò risulti eccessivamente oneroso per comprovate ragioni di carattere tecnico-economico, che l'amministrazione committente sia sempre titolare di tutti i diritti sui programmi e i servizi delle tecnologie dell'informazione e della comunicazione, appositamente sviluppati per essa. 2-bis. Al medesimo fine di cui al comma 2, il codice sorgente, la documentazione e la relativa descrizione tecnico funzionale di tutte le soluzioni informatiche di cui al comma 1 sono pubblicati attraverso una o più piattaforme individuate dall'AgID con proprie Linee guida".

²¹ Per approfondimenti cfr. F. Martini, *Open source, pubblica amministrazione e libero mercato concorrenziale*, in *Dir. econ.*, 2009, p. 677; F. Bravo, *Software « open source » per la p.a. tra diritto d'autore, appalti pubblici e diritto dei contratti. la licenza pubblica dell'UE per i programmi a codice sorgente aperto*, in *Diritto dell'informazione e dell'informatica*, 2008, p. 865; F. Bravo, *Software "Open Source" e Pubblica Amministrazione. L'esperienza comunitaria e quella italiana tra diritto d'autore, appalti pubblici e diritto dei contratti*, in S. Bisi, C. Di Cocco (a cura di), *Open source e proprietà intellettuale: fondamenti filosofici, tecnologie informatiche e gestione dei diritti*, Bologna, 2008, pp. 61-150.

²² Linee Guida AgID "Linee guida acquisizione e riuso software PA", adottate con determinazione n. 115 del 9 maggio 2019, sono pubblicate in Gazzetta ufficiale, serie generale n.119 del 23 maggio 2019, consultabili all'indirizzo https://www.agid.gov.it/sites/default/files/repository_files/lg-acquisizione-e-riuso-software-per-pa-docs_publicata.pdf. Per approfondimenti cfr. A. Pioggia, *Sviluppo, acquisizione e riuso di sistemi informatici nelle pubbliche amministrazioni. Commento agli artt. 67-70 del D.Lgs. 82/2005*, in E. CARLONI (a cura di), *Codice dell'amministrazione digitale. Commento al D.Lgs. 7 marzo 2005, n. 82*, Rimini, Maggioli, p. 399.

²³ A.G. Orofino, *Open source e pubblica amministrazione*, in G. Cassano (a cura di), *Diritto delle nuove tecnologie informatiche e dell'Internet*, Milano, 2002, p. 1317.

particolarmente gravoso sotto il profilo tecnico – economico – la titolarità dei programmi informatici sviluppati per essa.

Pertanto, come precisato anche nelle Linee Guida dell'AgID²⁴, l'ostensione del codice sorgente – o il riuso del software – consegue necessariamente all'acquisizione della titolarità del software, ovvero a precise condizioni contrattuali ampliative delle mere facoltà d'uso²⁵.

Più precisamente, dunque, ogni amministrazione è tenuta a “garantirsi, in sede di negoziazione di un contratto volto a commissionare lo sviluppo di un software, all'esito dell'esecuzione del contratto, la piena ed esclusiva titolarità di tutti i diritti sul software oggetto di sviluppo”²⁶.

Ne consegue, pertanto, che la piena ed esclusiva titolarità dei diritti sul software non può essere oggetto di mera presunzione²⁷. Al contrario, le disposizioni contemplate nel CAD intercettano, seppur implicitamente, una rinnovata dimensione dell'*accountability* amministrativa, che si declina nella razionale scelta delle procedure di acquisizione del software, e nella correttezza e chiarezza dei rapporti contrattuali in fase di esecuzione del contratto. Nondimeno, *accountability* intesa come consape-

²⁴ L'AgID precisa che (pag.7) “Ai sensi dell'articolo 69 del CAD in materia di riuso, un'amministrazione deve considerarsi titolare di un software realizzato su proprie specifiche indicazioni ogni qualvolta che: (i) abbia commissionato tale soluzione - attraverso un contratto di appalto o altra fattispecie negoziale avente analoga natura, anche a prescindere dal titolo dato al contratto - e il contratto preveda l'acquisizione in capo ad essa di tutti i diritti di proprietà intellettuale e industriale sul software sviluppato su committenza della Pubblica amministrazione, o comunque non attribuisca tale titolarità in capo all'appaltatore o a terzi. (ii) il software sia stato realizzato da risorse interne all'amministrazione stessa”.

²⁵ Com'è noto, infatti, qualora l'amministrazione proceda all'acquisizione di software proprietari, essa acquisirà soltanto la facoltà d'uso del software, lasciando in capo al privato appaltatore i diritti di proprietà intellettuale. Sul punto cfr. F. Bravo, Appalti pubblici per la fornitura di beni e servizi nel settore ICT e tecniche di redazione contrattuale. Le linee guida del CNIPA, in questa Rivista, 2007, 1, pp. 103 ss.

²⁶ *Ibidem*, p. 8. Peraltro, si aggiunge che “La mancata acquisizione della titolarità dell'opera non può essere utilizzata per ottenere condizioni economiche più vantaggiose, poiché non costituisce comprovata ragione di carattere tecnico-economico ai sensi dell'articolo 69 comma 2 del CAD”.

²⁷ Come invece, sembra propendere Tar Lazio, Roma, sez. III bis, 21 marzo 2017, n. 3742, ove si afferma che “deve (...) presupporre che negli accordi contrattuali con la società (...) realizzatrice e sviluppatrice del programma informatico che regge l'algoritmo, vi sia una pattuizione specifica che attribuisce proprio all'amministrazione il predetto diritto o comunque che evidentemente alcun diritto all'utilizzo economico sia riconosciuto in capo alla società privata”. Similmente, anche la posizione del T.A.R. Lazio, Roma, sez. III, 21 marzo 2017, n. 3742 risulta condivisibile, giacché riduce aprioristicamente i diritti e le tutele della software house, ritenendo che “né il diritto di autore né la proprietà intellettuale precludono la semplice riproduzione, ma precludono, invece, al massimo, soltanto la riproduzione che consenta uno sfruttamento economico e, non essendo l'accesso lesivo di tale diritto all'uso economico esclusivo dell'opera, l'ostensione deve essere consentita nelle forme richieste da parte dell'interessato, ossia della visione e dell'estrazione di copia, fermo restando che delle informazioni ottenute dovrà essere fatto un uso appropriato, ossia esclusivamente un uso funzionale all'interesse fatto valere con l'istanza di accesso che, per espressa allegazione della parte ricorrente, è rappresentato dalla tutela dei diritti dei propri affiliati, in quanto ciò costituisce non solo la funzione per cui è consentito l'accesso stesso, ma nello stesso tempo anche il limite di utilizzo dei dati appresi, con conseguente responsabilità diretta dell'avente diritto all'accesso nei confronti del titolare del software”.

volezza dell'impianto normativo e delle modalità di acquisizione del software, alla luce della prassi applicativa in materia.

3. L'accountability amministrativa tra trasparenza, leale collaborazione e buona fede

L'analisi della casistica giurisprudenziale fiorita in materia consente di maturare ulteriori riflessioni sull'ostensione del codice sorgente e sul giudizio di bilanciamento degli interessi contrapposti. In effetti, l'*accountability* amministrativa non si esaurisce nella conoscenza – o nella consapevolezza – della normativa rilevante. Un secondo e consequenziale aspetto su cui occorre riporre attenzione, infatti, valorizza la trasposizione della scelta in ordine alle modalità di acquisizione nel bando di gara, che costituisce la *lex specialis* dei rapporti costituenti tra amministrazione, appaltatore e gli altri operatori concorrenti, partecipanti alla procedura ad evidenza pubblica.

In altri termini, come ribadito dalla sedimentata opinione giurisprudenziale, il bando di gara imprime un auto – vincolo per la stazione appaltante, che non conserva margini di discrezionalità nella loro concreta attuazione e non può disapplicarle, neppure quando alcune di queste regole risultino inopportune o incongrue o comunque superate, fatta salva la sola possibilità di procedere all'annullamento delle regole di gara nell'esercizio del potere di autotutela²⁸.

Lungi dal comprimere i diritti esclusivi dell'autore del software, è necessario che l'amministrazione, ogniqualvolta ricorre all'uso di software nello svolgimento dell'attività amministrativa, precisi le proprie posizioni, assicurando il coordinamento e la coerenza tra i singoli atti di gara.

Infatti, se è pur vero che l'impiego della tecnologia per migliorare l'efficienza e l'economicità non può andare a detrimento della trasparenza, tale affermazione, tuttavia,

²⁸ Cfr. ex multis Cons. Stato, Sez. V, 5 marzo 2020 n. 1604. In senso conforme anche Tar Lombardia-Milano, Sez. II, 26 giugno 2020, n. 1215, chiarisce che “Le prescrizioni stabilite nella *lex specialis* di gara vincolano non solo i concorrenti, ma anche la stessa Amministrazione, che non conserva margini di discrezionalità nella loro concreta attuazione e non può disapplicarle, neppure quando alcune di queste regole risultino inopportune o incongrue o comunque superate, fatta salva la sola possibilità di procedere all'annullamento delle regole di gara nell'esercizio del potere di autotutela “. Consiglio di Stato, Sez. V, 23/11/2020, n.7257 si esprime nel senso che “Ferma restando la possibilità di annullare il bando (anche in parte, ossia nella sola parte ritenuta illegittima) nell'esercizio dei poteri di autotutela, la sola eventualità che può consentire la non applicazione del bando si ricollega all'ipotesi di clausole nulle, inidonee a produrre effetti giuridici, come nel caso della disposizione del bando che introduca una causa di esclusione dalla procedura non prevista dalla legge, nulla per la violazione del principio di tassatività delle cause di esclusione, ai sensi dell'art. 83, comma 8, del Codice dei contratti pubblici”. Sul valore della *lex specialis*, cfr. E. Boscolo, *Il divieto di eterointegrazione del bando: certezza e stabilità della “lex specialis”*. Nota a TAR LA - Roma sez. II bis 26 settembre 2017, n. 9921, in *Giurisprudenza italiana* n. 1/ 2018, pp. 173-178. Cfr. anche sent. Tar Puglia – Lecce, sez. II , sentenza 22 gennaio 2021 n. 113.

non implica la mera soccombenza dei diritti dell'autore, ma al contrario – in positivo – evidenzia i principi che la pubblica amministrazione è tenuta a rispettare.

In particolare, l'amministrazione dovrebbe prestare accorta attenzione alla fase contrattuale, assicurandosi l'acquisizione della titolarità del software per evitare, sul fronte privatistico, conseguenti azioni rimediale – anche a carattere risarcitorio – dell'operatore economico – *software house*²⁹, volte all'accertamento della condotta contraria ai doveri di leale collaborazione e buona fede (previsti dal novellato articolo 1, comma 2-bis della l.241/1990)³⁰, nonché al ristoro del pregiudizio subito.

Sono ravvisabili, pertanto, due differenti regimi che governano i rapporti instaurati dall'amministrazione, rispettivamente, con l'autore del software ed i partecipanti al procedimento amministrativo. Nel primo caso, infatti, l'amministrazione è tenuta all'applicazione e rispetto dei principi di leale collaborazione e buona fede di cui all'articolo 1, comma 2-bis; nel secondo caso, invece, l'amministrazione dovrà garantire la trasparenza e ponderare la richiesta di accesso procedimentale dell'interessato.

In ossequio ai principi individuati dalla norma, l'amministrazione non potrebbe procedere all'ostensione del codice sorgente in assenza di esplicita pattuizione: al contrario, la condotta risulterebbe pregiudizievole, giacché l'autore del *software* fornisce il programma all'amministrazione secondo le condizioni contrattuali (ivi compresa l'attribuzione del corrispettivo) prestabilite in sede di gara, che non contemplano la cessione del listato e che, se conosciute in anticipo dall'aggiudicatario, avrebbero costituito motivo deterrente di partecipazione alla gara.

Al contrario, l'attuale indirizzo giurisprudenziale sembra non cogliere adeguatamente tali aspetti³¹, limitandosi ad imporre aprioristicamente l'ostensione del codice sorgente, adottando così una soluzione drastica per l'effettivo titolare dei diritti di proprietà intellettuale³², motivando che “non può assumere rilievo l'invocata riser-

²⁹ F. Sciarretta, *La dimensione relazionale della responsabilità per violazione delle regole di comportamento dell'Amministrazione che contratta*, in *federalismi.it* n. 10/2020, pp. 419-461. Si v. anche C. Scognamiglio, *Tutela dell'affidamento, violazione dell'obbligo di buona fede e natura della responsabilità precontrattuale*, in *Resp. civ. e prev.*, 2012, p. 1949 ss. Per approfondimenti sul concetto di affidamento, cfr. F. Merusi, *L'affidamento del cittadino*, Milano, 1970.

³⁰ L'articolo 1 (Principi generali dell'attività amministrativa) della L. 241/1990 stabilisce al comma 2-bis che “2-bis. I rapporti tra il cittadino e la pubblica amministrazione sono improntati ai principi della collaborazione e della buona fede”. Per approfondimenti e prime applicazioni del principio, si v. P. Cucumile Pietro, *La tutela del legittimo affidamento del privato secondo l'orientamento della Corte di Cassazione Nota a ordinanza Corte suprema di Cassazione civile sezioni unite 28 aprile 2020, n. 8236 (Comune di Lignano Sabbiadoro vs De Candido Costruzioni S.r.l.)*, in *Disciplina del commercio e dei servizi*, n.3/2020, pp. 9-28.

³¹ Peraltro, come osservato da F. Bravo, “La maggior parte delle pronunce in tema di accesso al codice sorgente di software utilizzati dalla p.a. omette ogni considerazione sulle modalità di acquisizione”: F. Bravo, *Trasparenza del codice sorgente e decisioni automatizzate*, in *Diritto dell'Informazione e dell'Informatica* n. 1/2020, p. 693.

³² Ex plurimis, a titolo esemplificativo, si osserva in Tar Lazio, sentenza n. 7370 del 30 giugno 2020 che “la circostanza che, poi, l'algoritmo sia stato realizzato non direttamente da parte del M.I.U.R. per mezzo dei propri funzionari o personale dipendente ma a opera della società di cui sopra cui la creazione dello stesso è stata commissionata da parte dell'amministrazione a seguito di

vatezza delle imprese produttrici dei meccanismi informatici utilizzati le quali, ponendo al servizio del potere autoritativo tali strumenti, all'evidenza ne accettano le relative conseguenze in termini di necessaria trasparenza³³.

Pertanto, anche gli arresti giurisprudenziali sull'ostensione del codice sorgente di software proprietari *iussu iudici* confliggono con i principi di buona fede e del legittimo affidamento, che costituiscono ulteriore declinazione dell'*accountability* amministrativa. Si rischia, in altri termini, di discriminare l'operatore economico, sul quale gravano ulteriori previsioni normative che ne limitano l'operatività, quali ad esempio in relazione al principio di rotazione degli affidamenti. Questo orientamento, peraltro, risulta incoerente rispetto agli indirizzi giurisprudenziali recenti, protesi al riconoscimento e alla tutela del legittimo affidamento incolpevole³⁴.

4. Considerazioni conclusive

L'intelligenza artificiale si propone come utile strumento per l'amministrazione pubblica, al fine di coadiuvare i processi decisionali e favorire l'efficienza.

Al contempo, l'impiego delle nuove tecnologie impone una rinnovata responsabilizzazione della pubblica amministrazione.

L'amministrazione algoritmica deve dunque essere "*accountable*", maturando piena consapevolezza sugli strumenti in uso e sulle implicazioni giuridiche connesse, per evitare illegittime ed inconsapevoli discriminazioni.

Il caso della tutela del software offre l'occasione per riflettere sulla dimensione dell'*accountability* amministrativa, e del duplice ruolo dell'amministrazione algoritmica. Sulla scorta delle pronunce giurisprudenziali sino ad ora affermatesi, molteplici criticità risultano ravvisabili. In effetti, le esigenze di trasparenza, in più occasioni ribadite dalla giurisprudenza, confermano l'esigenza di una maggiore consapevolezza dell'amministrazione nella scelta delle modalità di acquisizione del software, ma

aggiudicazione di procedura di appalto e che costituisca, quindi, l'oggetto di una contrattazione di tipo privatistico, non è di per se ostativa proprio in quanto, indipendentemente dalla natura pubblicistica o privatistica della disciplina sostanziale, l'algoritmo è diretta espressione dell'attività svolta dalla pubblica amministrazione che è indubbiamente attività di pubblico interesse in quanto interessante l'organizzazione del servizio pubblico rappresentato dalla pubblica istruzione e, infatti, il predetto algoritmo è entrato nella procedura quale elemento decisivo e lo stesso è, comunque, stabilmente detenuto dalla stessa amministrazione ministeriale che lo ha commissionato e, quindi, utilizzato per le proprie finalità".

³³ Cfr. Cons. Stato, sent. n. 881 del 4 febbraio 2020.

³⁴ Sul punto, cfr. l'Adunanza Plenaria del Consiglio di Stato, sentenza n. 19 del 29.11.2021. La sentenza ribadisce che "l'affidamento nella legittimità dei provvedimenti dell'amministrazione e, più in generale, sulla correttezza del suo operato è riconosciuto dalla risalente giurisprudenza del Supremo Collegio dei giudici amministrativi come situazione giuridica soggettiva tutelabile attraverso il rimedio del risarcimento del danno". Precisa, inoltre, che l'affidamento "è un principio generale dell'azione amministrativa che opera in presenza di una attività della pubblica amministrazione che fa sorgere nel destinatario l'aspettativa al mantenimento nel tempo del rapporto giuridico sorto a seguito di tale attività" (Cons. Stato, VI, 13 agosto 2020, n. 5011).

soprattutto nella puntuale definizione, in sede di gara, delle modalità di acquisto della titolarità dello stesso.

Alla luce delle riflessioni fino ad ora condotte, dunque, è possibile concludere auspicando che nell'ambito dell'amministrazione algoritmica la tutela del software viaggi al crinale tra trasparenza e legittimo affidamento, per ponderare le esigenze degli interessati e la pubblica commessa.

AI E NUOVE FORME DI DISCRIMINAZIONE

Guido Scorza

Abstract [IT]: L'intervento mira a tratteggiare il momento storico attuale in materia di intelligenza artificiale con le opportunità e i rischi che si possono delineare, passando in rassegna i principali provvedimenti che l'Autorità per la protezione dei dati personali ha adottato nei confronti di soggetti pubblici e privati.

Abstract [EN]: The intervention aims to outline the current historical moment in the field of artificial intelligence with the opportunities and risks that can be outlined, by reviewing the main measures that the Authority for the protection of personal data has adopted against public and private subjects.

Keywords [IT]: intelligenza artificiale – algoritmo – Autorità Garante per la protezione dei dati personali – GDPR – riconoscimento facciale.

Keywords [EN]: artificial intelligence – algorithm – Guarantor Authority for the protection of personal data – GDPR – facial recognition.

Inizierei, forse sono già state evocate, ma credo siano un po' la sintesi almeno nella dimensione giuridica e democratica della questione al centro di questo di questo nostro incontro, con le parole di Michelle Bachelet, la *Special rapporteur* delle Nazioni Unite sui diritti umani che ha scritto nella sua relazione di qualche mese fa: l'intelligenza artificiale può essere una forza positiva aiutando la società a superare alcune delle grandi sfide dei nostri tempi, ma le tecnologie di intelligenza artificiale possono avere effetti negativi, persino catastrofici, se vengono utilizzate senza tenere in sufficiente considerazione in modo in cui influiscono sui diritti umani delle persone. Ecco questo invito sostanzialmente alla neutralità nell'approccio alla intelligenza artificiale, a non bollare le applicazioni dell'Intelligenza artificiale né in termini apocalittici, né in termini di panacea dei mali del mondo, è un po' in realtà l'anima dell'attività o dell'approccio all'attività che qui all'Autorità per la protezione dei dati personali abbiamo in relazione alle cose dell'intelligenza artificiale, utilizzando nella avvicinarci ad esse - per ora - lo strumento essenzialmente del GDPR, della disciplina europea sulla protezione dei dati, in attesa di poter disporre, eventualmente anche, delle nuove disposizioni di cui immagino avrete largamente parlato, della proposta di Regolamento in materia di intelligenza artificiale della Commissione europea. Prima di arrivare a proporvi, in estrema sintesi, alcune delle occasioni nelle quali ci siamo occupati di intelligenza artificiale in questi ultimi mesi qui in Autorità, credo che al centro del tavolo - ma lo avrete fatto con molti dei colleghi e amici che hanno preso la parola prima di me - credo che sia importante mettere a fuoco il momento nel quale ci troviamo, un momento in cui di fatto abbiamo davanti uno scenario

straordinariamente liquido, quello del progressivo ingresso degli algoritmi, delle soluzioni di intelligenza artificiale nella società, ne parliamo spesso al futuro, ma in realtà il tempo giusto per parlarne è il presente, perché l'intelligenza artificiale è già fra noi, quindi non una dimensione prospettica, ma una dimensione attuale e presente.

E quindi, in questo contesto, la sfida che abbiamo noi naturalmente come Autorità e che hanno più di noi il decisore pubblico nazionale e quello europeo, è identificare e dettare i principi e le regole, forse i principi più che le regole, per governare l'impatto dell'intelligenza artificiale in tutte le sue dimensioni sulla nostra società.

Perché, se questo non accade, il rischio che osserviamo, e di qui a poco ve ne darò conto, dall'Autorità è un rischio neppure troppo nuovo per chi si occupa di nuove tecnologie: cioè se le regole e i principi non vengono identificati dall'Autorità, quelle regole e quei principi vengono identificati dai mercati perché è il mercato che fissa la regola.

È quello che è accaduto tutto sommato negli ultimi 25-30 anni nella dimensione di Internet e del Web, in cui prima l'entusiasmo per il Web, piazza pubblica, Agorà pubblica, la più grande della storia dell'Umanità, poi la difficoltà di maneggiare strumenti straordinariamente nuovi hanno determinato, è fuori di dubbio, che Governi, decisori pubblici, le Autorità si siano ritrovati a giocare in ricorsa nella partita al governo dei nuovi scenari, è quello che è accaduto in particolare con i gestori delle Big Tech che si sono sostituiti a Parlamenti, Governi, Autorità. Il rischio è che questo scenario possa avvenire anche nelle cose dell'intelligenza artificiale. Perché lo chiamo rischio? Qualcuno potrebbe dire si tratta di opportunità, il mercato tutto sommato produce anche effetti benefici. Lo chiamo rischio perché nella dimensione del mercato, nelle cose dell'intelligenza artificiale in particolare, almeno per come le abbiamo osservate sin qui, quello che accade è che il mercato come principio ispiratore della sua azione sceglie di dire: tutto quello che è tecnologicamente possibile, tutto quello che è algoritmicamente possibile, può considerarsi anche giuridicamente legittimo e democraticamente sostenibile, non è così!

L'esempio chiave, l'aspetto principale nel quale questo principio si riscopre democraticamente fragile, fragile sotto la lente dei diritti fondamentali, è esattamente quello del titolo di questo incontro: *"IA & nuove forme di discriminazione"*.

Non è così, tra l'altro perché, cedere alla nuova declinazione del principio del fine che giustifica i mezzi caro a Machiavelli nella chiave di ciò che tecnologicamente possibile è anche giuridicamente legittimo e democraticamente sostenibile, significa correre il rischio che perseguendo fini certamente utili come la maggiore efficienza dell'amministrazione, la maggiore economicità di talune azioni di business, il più veloce raggiungimento del profitto, il supporto anche a soluzioni di carattere diagnostica medica, si possano creare discriminazioni importanti.

Arrivo davvero al cuore delle questioni, rasserenando chi è davanti al PC ormai da qualche ora sul fatto che resterò in silenzio di qui a poco, l'Autorità ha incrociato diverse volte negli ultimi mesi questi problemi tanto nei confronti di soggetti pubblici quanto nei confronti di soggetti privati.

Probabilmente il più celebre, diciamo, tra i provvedimenti adottati dall'Autorità nei confronti di soggetti pubblici aventi l'intenzione di utilizzare soluzioni di intelligenza artificiale è il parere reso al Ministero dell'Interno nel caso cosiddetto "*Sari Real Time*", cioè il software di riconoscimento facciale intelligente, con il quale Ministro dell'Interno si proponeva per l'appunto di procedere all'identificazione di massa di soggetti in luoghi pubblici.

In quell'occasione, di fronte alla quale, come dire, il fine perseguito dal Ministero dell'Interno era innegabilmente nobile cioè la tutela dell'ordine pubblico, la repressione del crimine e l'identificazione del criminale, ciò che nella sostanza ha detto l'Autorità per la protezione dei dati personali: non si può imboccare quella strada, perché se la si imboccasse in assenza di una legge che identifica all'esito di un processo ampio e condiviso il punto di bilanciamento tra il fine perseguito e la compressione della privacy delle persone, si produrrebbero effetti incompatibili con la democrazia.

Perché di fatto il riconoscimento facciale di massa gestito da un soggetto pubblico ha come conseguenza, la dico in termini approssimativi, sperando di far prima ma di essere di essere capito, è quella di fare del mondo intero che sfila davanti alle telecamere di riconoscimento facciale un esercito di potenziali sospettati.

Tutti diventiamo sospettati, tutti veniamo osservati e l'immagine, o meglio l'impronta biometrica, di ciascuno di noi viene matchata con quella di un elenco di sospettati, che è cosa molto diversa anche dall'utilizzo delle stesse tecnologie per riconoscimenti puntuali di soggetti, autori di condotte illecite poste o che si sospettano essere illecite.

Cambiando completamente scenario, l'Autorità si è ritrovata a pronunciarsi in materia di intelligenza artificiale, di dati e di algoritmi in due precedenti molto simili l'uno all'altro.

L'uno nei confronti di Foodinho, società che gestisce Glovo, l'altra nei confronti di Deliveroo, quindi due società per la gestione di piattaforme di rider, di consegne a domicilio, due società che hanno scelto di scommettere in maniera significativa proprio sugli algoritmi di intelligenza artificiale.

Algoritmi di intelligenza artificiale per far cosa? Algoritmi di intelligenza artificiale in entrambi i casi essenzialmente per gestire in maniera più efficiente, più efficiente possibile dal punto di vista dei gestori della piattaforma, l'assegnazione delle corse ai diversi rider, quindi il parco rider, il parco corse, il parco lavoratori. Perché questi algoritmi hanno destato dapprima l'attenzione e poi hanno determinato provvedimenti sanzionatori da parte di quest'Autorità.

Per tante ragioni, ne metto in fila due per non impegnare più tempo del necessario. La prima è una ragione con la quale credo ci troveremo a confrontarci decine o centinaia di volte nei prossimi mesi: l'assenza di trasparenza della logica algoritmica verso il lavoratore. Un lavoratore ha il diritto di sapere, come qualsiasi altro interessato, non solo che il titolare del trattamento tratterà i suoi dati utilizzando anche sistemi algoritmici, ma sapere qual è la logica che sta dietro il trattamento, quando cioè l'algoritmo lo riterrà, la dico male per intenderci, un rider meritevole di una

corsia preferenziale nell'assegnazione corsa e quando, viceversa, quell'algoritmo lo riterrà un rider destinato a perdere posizioni nell'assegnazione delle corse. Se manca questa trasparenza, quel trattamento è un trattamento illecito, non ci servono norme nuove, quelle che arriveranno con il Regolamento, è sufficiente il GDPR e gli obblighi di informativa, con gli articoli 12, 13, 14 per arrivare a questa conclusione. Ma vengo al tema della discriminazione più da vicino. In quei provvedimenti si è detto "Attenzione": anche ammesso e non concesso che sia sostenibile il ricorso all'algoritmo nell'universo lavorativo, quel che è certo è che l'algoritmo, in quel e in altro contesto, deve trattare in maniera diversa soluzioni diverse. Quel che facevano gli algoritmi è assumere che la puntualità e tempestività con la quale un rider si loggava alla piattaforma per iniziare il turno di lavoro era un fattore scriminante per distinguere i più buoni dai meno buoni, i più capaci dai meno capaci. Ma nel gestire algoritmicamente questo tipo di valutazione in realtà azzerava il rilievo della ragione che eventualmente avesse indotto un rider che si fosse prenotato per il turno delle 18.00 di fronte al McDonald's di via Giulio Cesare e che poi non si fosse presentato. Che quel rider non si fosse presentato perché aveva avuto un incidente, per ragioni di malattia, perché aveva partecipato ad una manifestazione o ad uno sciopero, che invece non si fosse presentato perché, nonostante la prenotazione, aveva preferito non presentarsi perché aveva accettato un lavoretto diverso in quella stessa fascia oraria, quel rider, nella dimensione algoritmica, subiva un pregiudizio, cioè veniva pretermesso da altri nell'assegnazione delle corse e delle cose future e non gli veniva dato modo, almeno in maniera semplice, agevole e immediata di rettificare la valutazione algoritmica del proprio profilo. L'Autorità è intervenuta su algoritmi non più utilizzati, ma il ricorso a soluzioni algoritmiche palesemente discriminatorie è da considerarsi illegittimo tra l'altro in una dimensione di protezione dei dati personali. Di discriminazione in discriminazione, ma non voglio abusare del vostro tempo, l'ultimo provvedimento dell'Autorità è relativo a Clearview, società di riconoscimento facciale, che nella sostanza ha rastrellato, ha pescato a strascico nella dimensione digitale, in particolare in quella dei social network 10 miliardi di immagini di miliardi di persone, tra le quali decine di milioni di italiani presenti online e ha poi fornito e fornisce dei servizi in particolare alle forze di polizia - sostiene la società non in Italia almeno non in Italia in questo in questo momento - per il riconoscimento facciale.

Anche lì qual è il rischio elevato, a prescindere dalla illegittimità di un trattamento che nasce pescando a strascico dati personali senza nulla dire a queste persone? Il rischio è elevato anche qui non solo in termini discriminatori, perché il sistema si basa sull'associazione dell'immagine di una persona presente sui social al nome e cognome di quella persona e ad altre informazioni che Clearview assume come buone e che propone come tali alla forza di polizia di turno. Questa, ad esempio, carica in piattaforma l'immagine di un sospettato e utilizza il sistema per cercare la corrispondenza di quell'immagine, o meglio dell'impronta biometrica di quell'immagine, alla quale però nel database di Clearview potrebbe corrispondere anche il

nome di una persona diversa.

Ciascuno di noi crea profili on-line per motivi e nell'ambito di logiche completamente diverse, tra le quali mai vi è quella che quelle immagini potranno essere un giorno utilizzate ai fini di identificazione con rilevanza nell'universo investigativo. Se online si realizza, perché la realizza l'interessato o la realizzano terzi, una associazione non reale tra un'immagine, un nome e un cognome, il risultato è che qualcuno di noi si ritroverà sospettato nel database di qualche forza di polizia in giro per il mondo, senza aver fatto nulla di male.

Questo è sicuramente un altro profilo di illegittimità del trattamento dei dati a mezzo algoritmo con cui l'Autorità si è confrontata di recente sanzionando Clearview AI con una sanzione da venti milioni di euro, ordinando di cancellare dal database le immagini raccolte in Italia e di non erogare il suo servizio almeno in relazione alle immagini di cui stiamo discutendo.

Sono molteplici gli ambiti nel pubblico e nel privato in cui già oggi sulla base semplicemente del GDPR, in particolare degli obblighi di informazione e di quelli relativi alle decisioni automatizzate, l'Autorità ha incrociato il tema dei trattamenti di dati personali attraverso algoritmi e naturalmente si tratta di un filone, inesorabilmente, destinato a crescere, Io non vorrei aggiungere neppure una parola di più salvo non ci siano curiosità, cui rispondo ben volentieri.

