amministrativ@mente

Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com



Rivista scientifica trimestrale di diritto amministrativo

Pubblicata in internet all'indirizzo www.amministrativamente.com

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Marco Cardilli

Redazione
Giuseppe Egidio Iacovino, Carlo Rizzo

FASCICOLO N. 2/2019

estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

Comitato scientifico

Annamaria Angiuli, Antonio Calonge Velázquez, Vincenzo Caputi Jambrenghi, Enrico Carloni, Guido Clemente di San Luca, Andry Matilla Correa, Gianfranco D'Alessio, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Luca Raffaello Perfetti, Alessandra Pioggia, Helene Puliat, Francesco Rota, Leonardo J. Sánchez-Mesa Martínez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Salvatore Bonfiglio, Vinicio Brigante, Ambrogio De Siano, Manuel Delgado Iribarren, Giuseppe Doria, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Giovanni Martini, Gaetano Natullo, Marcin Princ, Giuliano Taglianetti, Ramón Terol Gómez, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

L'Intelligenza Artificiale nell'utilizzo e nel rispetto dei dati personali

di Filippo Lorè

(Dottore in Giurisprudenza)

Sommario

1. . Il Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino (Agenzia per l'Italia Digitale). – 2. Le Linee Guida Etiche sull'Intelligenza Artificiale del Gruppo di Esperti della Commissione europea. – 3. La Convenzione 108+

Abstract

The paper deals with the topic of Artificial Intelligence (IA). In particular, the main contents of the White Paper on Artificial Intelligence at the service of the citizen are analyzed, presented by the Agency for digital Italy on 21 March 2018, with reflections on the challenges, problems and principles that must guide the State , the PA, businesses and citizens in the use of AI.

Subsequently the Ethical Guidelines on Artificial Intelligence of the Group of Experts of the European Commission are examined, with reflections on the necessary requirements for a reliable AI, with a focus on those of security, confidentiality and data governance. Finally, the European Council Convention 108+ is analyzed.

1. Il Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino

Il Libro Bianco sull'Intelligenza Artificiale (IA) al servizio del cittadino, a cura dell'Agenzia Italiana per il Digitale (AGID)[1], nasce per fare una ricognizione dei servizi digitali in Italia e per analizzare l'impatto dell'IA sulla società e in particolare sulla Pubblica Amministrazione (PA). Lo Stato può adottare queste tecnologie per migliorare i servizi ai cittadini e alle imprese, dando un impulso decisivo all'innovazione e all'economia. Sundar Pichai, CEO di Google, ha affermato[2] che "*l'IA sarà più grande dell'elettricità o del fuoco*". L'IA è in effetti una delle tecnologie più promettenti del presente ma, allo stesso tempo, una delle più pericolose. Essa oggi permette di salvare vite umane, elaborare le previsioni degli acquisti, aumentare la produttività in agricoltura, supportare i medici nell'identificare malattie, rilevare le frodi nelle transazioni, guidare al posto nostro, prendersi cura delle persone anziane o ammalate, svolgere lavori pericolosi o usuranti, aiutarci a prendere decisioni ponderate, comunicare in lingue che non conosciamo[3]. Questo vale ovviamente anche per i Governi e le PA, l'IA, infatti, può essere utilizzata nel sistema sanitario, scolastico, giudiziario, nel pubblico impiego, nella sicurezza. Le stesse relazioni della PA con i cittadini possono essere rese più semplici, efficaci, veloci ed efficienti, nell'ottica dello sviluppo dell'*e-government* e digitalizzazione dei servizi pubblici, perseguito dalla Commissione Europea[4]. L'Italia, nel 2014, era uno degli ultimi Paesi Ue nella classifica degli individui che avevano utilizzato internet per interagire con le PA[5]. Il Libro Bianco infatti fornisce anche spunti di riflessione su come migliorare la vita dei cittadini sfruttando in modo positivo l'IA, con un'attenzione particolare verso strumenti come, a titolo esemplificativo, le *chatbot*[6], i robot che si prendono cura dei malati, gli algoritmi che leggono i risultati degli esami medici, quelli che seguono il percorso scolastico degli studenti e li aiutano a migliorare la loro preparazione, i

[1] L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica. AgID ha il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese. AgID sostiene l'innovazione digitale e promuove la diffusione delle competenze digitali anche in collaborazione con le istituzioni e gli organismi internazionali, nazionali e locali.

[2] Agenzia Italiana per il Digitale, Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino, Versione 1.0, Marzo 2018, p. 52

[3] Agenzia Italiana per il Digitale, Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino, Versione 1.0, Marzo 2018, p. 9

[4] AgID partecipa a molti tavoli consultivi avviati presso le istituzioni europee (v. https://www.agid.gov.it/it/agenzia/attivita-internazionali/politiche-digitali-europee)

[5] Dati OCSE, in https://www.assolombarda.it/centro-studi/l2019e-government-in-italia-situazione-attuale-problemi-e-prospettive

[6] Le *chatbot*, già usate nelle grandi aziende private per i rapporti con la propria clientela, sono state introdotte anche nella PA. Si pensi alle procedure di assistenza di recupero credenziali per i servizi on-line, alla raccolta differenziata, al trasporto pubblico locale.

mezzi per il monitoraggio e la gestione delle carriere, quelli per la sorveglianza dei luoghi pubblici o per il riconoscimento di minacce in rete, gli strumenti per la gestione razionale dei problemi generati dalle catastrofi naturali. Tuttavia, secondo la *task force* del Libro Bianco, per avere un'IA efficace e utile, all'implementazione di tecnologie basate su sistemi di IA, dovrebbe essere propedeutica la valutazione dei problemi e delle sfide generate dall'uso dell'IA. La parte centrale del Libro Bianco è dedicata all'individuazione di queste sfide che sono: "Etica", "Tecnologia", "Competenze", "Ruolo dei dati", "Contesto legale", "Accompagnare la trasformazione", "Prevenire le disuguaglianze", "Misurare l'impatto", "L'essere umano". Il primo problema è quello etico, da risolvere mediante l'affermazione del principio antropocentrico: l'IA deve essere sempre messa al servizio delle persone e non viceversa. È opportuno formulare alcuni principi generali di equità per soddisfare il rispetto delle libertà e dei principali diritti individuali e collettivi. Più in particolare il documento cita la qualità e la neutralità dei dati, la responsabilità di chi utilizza gli algoritmi, la trasparenza e l'apertura di questi ultimi, la tutela della privacy. Bisogna far capire come l'uso scorretto delle tecnologie e la non consapevolezza dei rischi potrebbero essere nocivi alla società. La seconda sfida affrontata dal Libro Bianco è quella tecnologica: l'IA non è ancora in grado di riprodurre il funzionamento complesso della mente umana (solo alcune sue capacita circoscritte), ma per avere in futuro riscontri pratici nella nostra vita quotidiana, bisogna vincere questa sfida. La terza è invece quella delle competenze da sviluppare sia tra i cittadini, promuovendo l'alfabetizzazione digitale, sia tra gli attori della PA, i quali devono sapere come funzionano gli algoritmi e le basi di dati su cui questi operano. Il sistema scolastico e universitario deve essere al passo coi tempi ma, per arrivare a questo, prima di tutto i docenti necessitano di formazione ed è necessaria una preparazione interdisciplinare, anche per chi opera nel settore dell'IA. Vi è attualmente una sproporzione tra la domanda di figure specialistiche nei settori delle tecnologie avanzate e disponibilità di competenze adeguate, sicché il settore privato è disposto a pagare stipendi altissimi per poter competere nel mercato dell'innovazione con il contributo dei migliori talenti[7]. La quarta sfida è riferita al ruolo dei dati su cui operano gli algoritmi. Dati di qualità e senza pregiudizi (*bias*) portano a risultati di qualità. Un terreno di confronto è rappresentato dalla gestione e ricerca dei dati pubblicati in rete sotto forma *di linked open data*. Inoltre i sistemi di IA beneficiano dell'enorme mole di dati personali e ambientali quotidianamente registrata dai sistemi informatici. Determinante sarà allora garantire qualità e

[7] Agenzia Italiana per il Digitale, *Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino*, Versione 1.0, Marzo 2018, p. 50, al cui interno si elencano alcune professioni che non esistevano 10 anni fa: sviluppatore di app, admissions consultant, user experience designer, chief listening officer, esperto di sostenibilità, esperto di assistenza agli anziani, esperto generazione millennials, esperto servizi cloud computing, social media manager, market research, data miner, data scientist, data architect, data visualizer, data engineer/operator.

interoperabilità. Un'operazione necessaria in tal senso, ma molto onerosa, è quella che consente ai dati di essere "annotati" dagli esseri umani che "insegnano" alle macchine come interpretarli (*supervised learning*). La discrezionalità degli annotatori, però, potrebbe generare dati simili annotati in maniera diversa, depotenziando il funzionamento delle macchine e propagando errori e pregiudizi. Il Libro Bianco ci mette in guardia proprio da questo problema, per il quale a suggerire un metodo efficace è Mantelero[8]. I comitati di esperti di vari settori (scienze sociali, diritto, etica, ecc.) possono rappresentare la migliore impostazione per discutere e affrontare le questioni relative all'impatto dell'IA sulle persone e sulla società, compensando il punto di vista limitato degli sviluppatori di IA. I comitati multidisciplinari potrebbero anche essere in grado di rilevare potenziali pregiudizi che dipendono dall'identità degli sviluppatori di intelligenza artificiale: ad esempio, pregiudizi di genere, pregiudizi ideologici o sotto rappresentanza delle minoranze. Un altro modo per ridurre le possibilitàà di *bias* delle applicazioni AI, è rappresentato da forme partecipative di valutazione del rischio, focalizzate non solo sulla sicurezza dei dati e sulla qualità dei dati, ma anche sull'impegno attivo dei gruppi potenzialmente colpiti da applicazioni di IA, e che possono contribuire alla rilevazione e rimozione di pregiudizi esistenti. La quinta sfida del Libro Bianco di AgID è quella legale, vale a dire il bilanciamento tra gli interessi sociali e gli interessi individuali, ad esempio tra il principio di trasparenza degli atti amministrativi e la protezione dei dati personali oppure le questioni riguardanti la tutela del diritto d'autore di chi ha creato gli algoritmi o, ancora, il problema della responsabilità giuridica a monte. È opportuno soffermarsi brevemente su questi temi. L'articolo 5 del GDPR[9] afferma che i dati devono essere processati in modo lecito, trasparente e giusto (principio di legalità, equità e trasparenza); raccolti ed utilizzati per un motivo specifico ed esplicitamente dichiarato (principio della limitazione delle finalità); adeguati e limitati alle finalità per cui vengono processati (principio della minimizzazione dei dati); corretti e aggiornati (principio di accuratezza); non archiviati in modo identificabile per più del necessario (principio connesso al periodo di conservazione dei dati); trattati in modo da garantire adeguata tutela dei dati personali (principio di integrità e confidenzialità). Gli algoritmi di IA possono incidere direttamente sulle valutazioni e sulle decisioni pubbliche, nonché sui procedimenti amministrativi. Questo pone un problema di *accountability*[10] e di verifica dell'effettiva responsabilità giuridica a monte

[8] Intelligenza artificiale e protezione dei dati: sfide e possibili rimedi, Relazione di Alessandro Mantelero al Rapporto sull'intelligenza artificiale del Comitato consultivo della Convenzione per la protezione dei singoli per quanto riguarda l'elaborazione automatica dei dati personali, Strasburgo, 25 gennaio 2019, p. 9

[9] Regolamento UE 2016/679, *Principi applicabili al trattamento*.

[10] Il principio di *accountability* ha avuto un definitivo riconoscimento nel Regolamento UE 2016/679 sulla protezione dei dati personali. Questo termine anglosassone non è facilmente traducibile ma fa capo al concetto di "rendicontazione", del titolare del trattamento, delle azioni volte a tutelare i dati personali e la riservatezza. In particolare il Regolamento 2016/679 recepisce tale principio all'art. 24 dove prevede che, tenuto conto della

di determinate decisioni o risultati. La PA deve trovare metodi uniformi e compatibili con l'ordinamento per arrivare a motivare i suoi provvedimenti anche nella parte elaborata dai sistemi di IA. Deve altresì indicare le sorgenti dei dati che alimentano l'IA ed attraverso i quali essa ha compiuto le proprie valutazioni. La PA deve infine porre i responsabili dei procedimenti amministrativi a conoscenza delle modalità di elaborazione utilizzate dai sistemi IA. Il cittadino, d'altra parte, dovrà essere messo in condizione di comprendere attraverso quale percorso il sistema IA è pervenuto a un determinato risultato, in modo sufficientemente chiaro da poter eventualmente riconoscere un errore di calcolo ed intervenire per ottenerne la correzione[11]. Senza dimenticare che l'uso di dati particolari da parte della PA può incidere fortemente sulla *privacy* del cittadino. La sesta sfida del Libro Bianco di AgID è per la PA e consiste nel capire quali sono le azioni necessarie per accompagnare la trasformazione del Paese verso l'adozione dell'IA tenendo presente che essa dovrebbe non sostituire le persone ma affiancarle ed aiutarle a svolgere le loro attività. La settima sfida è quella di ridurre le disuguaglianze sociali esistenti, si pensi alle applicazioni dell'IA nell'istruzione, nella sanità, nella disabilità. Viceversa si avranno più disuguaglianze e nuove disuguaglianze. L'IA deve essere accessibile a tutti, dunque semplice e di uso immediato. L'ottava sfida riguarda la misurazione dell'impatto dell'IA sulla PA attraverso l'ottimizzazione dei processi organizzativi, in termini di efficienza ed efficacia, e la verifica dell'impatto che le soluzioni di IA avranno sulle politiche pubbliche. L'ultima sfida prevede la necessità di "accompagnare" le persone verso una corretta comprensione dell'IA e delle sue implicazioni sulla loro vita, anche a livello psicologico. Tutti devono essere consapevoli del significato profondo che può assumere l'utilizzo di questi strumenti. L'IA può trasformare radicalmente il nostro mondo nel bene e nel male, bisogna, quindi, fare molta attenzione e governarla nel modo più appropriato. Il documento si conclude con un insieme di raccomandazioni al fine di creare un dibattito sui temi esposti. AgID si propone di promuovere una piattaforma nazionale sullo sviluppo di sistemi di IA; di istituire un Centro di competenza nazionale come punto di riferimento per le PA; di favorire l'istituzione e la certificazione di figure professionali nell'ambito dell'IA con la previsione di percorsi di formazione specifici; di implementare un Piano 4.0 per attrarre investimenti privati e pubblici; di istituire un Centro transdisciplinare sull'IA. Analizzate le nove sfide, merita un cenno il fatto

natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente al Regolamento. L'*accountability* involge dunque sia l'affidabilità del titolare e del responsabile del trattamento verso l'esterno (gli interessati) sia le competenze tecniche necessarie all'interno dell'azienda per essere *compliant*.

[11] Agenzia Italiana per il Digitale, Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino, Versione 1.0, Marzo 2018, p. 55

che, se dal punto di vista legislativo il dibattito sull'IA è ancora allo stadio embrionale, si può dire che tecnicamente il Libro Bianco è riconducibile alle forme di *soft law*, in particolare di *pre-law*[12]. Per la dottrina anglosassone il *soft law* prevede regole di condotta cui non è attribuito dall'ordinamento carattere vincolante ma che comunque producono effetti giuridici ovvero sono adottate con lo scopo di raggiungere gli stessi effetti giuridici formalmente collegati ad atti vincolanti[13]. Il Libro Bianco sull'IA si caratterizza per la sua non percettività, riferendosi peraltro ad un ambito nuovo e poco esplorato, in special modo nell'attività della PA. Quanto invece alle ricadute sul piano giuridico che avrà l'uso di sistemi di IA nella PA è difficile fare previsioni, però appare chiaro quanto sia cruciale la questione della protezione dei dati personali, a garanzia dei diritti e delle libertà dei "cittadini digitali" nei rapporti con lo Stato. Sta nascendo in tal senso, una letteratura tuttavia una grande spinta è stata data dall'entrata in vigore del Regolamento UE 2016/679, nel quale si ravvisano disposizioni importanti, seppur non riferite espressamente all'IA, anzitutto, oltre a quelli già enucleati, il principio della *privacy by design*[14] ovvero la protezione dei dati personali fin dalla progettazione. Connesso a tale principio è il *data protection impact assessment* (DPIA o valutazione di impatto sulla *privacy*) da mettere in atto prima che il trattamento venga effettuato, allo scopo di valutare se il trattamento è necessario e quali rischi comporta per i diritti e le libertà delle persone fisiche[15]. Si tratta di un approccio *risk - based*. Il Considerando 15 del Regolamento stabilisce inoltre che "*al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i*

[12] R. Bin, *Soft law, no law*, in A. Somma (a cura di), Soft law e hard law nelle società postmoderne, Torino, 2009, 31 ss., per il quale rientrerebbero nel *pre-law* libri bianchi, libri verdi, programmi di azioni, comunicazioni istituzionali, mentre nel *post-law* linee guida, direttive interpretative, circolari ecc.

[13] Annamaria Poggi, *Soft law nell'ordinamento comunitario*, Relazione tenuta al convegno annuale dell'Associazione italiana dei costituzionalisti, L'integrazione dei sistemi costituzionali europeo e nazionali, Catania, 14-15 ottobre 2005. Ciò che realmente descrive il *soft law*, secondo queste ricostruzioni, è l'intenzione di produrre un atto astrattamente non vincolante, ma volutamente alternativo ad un atto vincolante, nella certezza che esso comunque produrrà effetti giuridici. Perciò, tra le tre funzioni in cui vengono classificati gli atti ascrivibili tale fenomeno e cioè *pre-law* (strumenti preparatori di atti giuridici vincolanti quali Libri bianchi, Libri verdi), *post-law* (strumenti di interpretazione di atti vincolanti quali linee guida, codici di condotta, comunicazioni interpretative) e *para-law* (strumenti alternativi ad atti vincolanti quali raccomandazioni, pareri comunicazioni non interpretative), solo quest'ultima viene ritenuta funzione di "vero" *soft law*, poiché essa renderebbe assolutamente evidente lo scopo che si vuole raggiungere: dar vita ad un atto alternativo alla legislazione.

[14] Art. 25, paragrafo 1 del Regolamento UE 2016/679, "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di tutelare i diritti degli interessati*".

[15] Art. 35 del Regolamento UE 2016/679, *Valutazione di impatto privacy*, quando un determinato trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

dati personali sono contenuti o destinati a essere contenuti in un archivio [...]". Per quanto riguarda le operazioni "automatizzate" di trattamento dei dati personali, il Regolamento riconosce all'interessato il diritto di opposizione[16]. Infine, il Regolamento disciplina anche le misure "*tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*"[17]. Anche il Parlamento europeo è intervenuto sul ricorso a processi decisionali automatizzati nella PA, affermando[18] che la possibilità di verifica e controllo umani devono essere integrati nei processi decisionali automatizzati e algoritmici, in modo che sia sempre possibile indicare la logica alla base di ogni decisione presa con l'ausilio dell'intelligenza artificiale, specialmente se essa può avere un impatto rilevante sulla vita della persona. Non è più solo fantascienza ormai il timore che l'uomo possa un giorno non essere più in grado di gestire le dinamiche legate ai sistemi di IA[19]. Illuminante in tal senso è la Carta dei Diritti e dei Doveri dei robot[20], contenente le Linee guida per la regolamentazione della robotica. L'art. 13 stabilisce che gli esseri umani non potranno mai tramutarsi in robot, né totalmente né in parte, mentre l'art. 16 asserisce che gli esseri umani non dovranno mai essere impiegati al servizio dei robot. A livello nazionale il Codice dell'Amministrazione Digitale[21] completa il quadro

[16] Art. 22 del Regolamento, che stabilisce peraltro che anche qualora un tale trattamento si basi sul consenso esplicito dell'interessato, il titolare del trattamento deve tutelare i diritti, le libertà e i legittimi interessi dell'interessato, riconoscendo allo stesso almeno il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione.

[17] Art. 32 del Regolamento UE 2016/679. Queste misure comprendono, tra le altre, se del caso, la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Risulta chiara la scelta del legislatore europeo in materia di protezione dei dati personali di non fornire, alla luce dell'importante progresso tecnologico al quale la Società assiste, misure specifiche che potrebbero risultare, nel breve periodo, obsolete.

[18] Risoluzione 16 febbraio 2017, la quale riconosce "*che i robot potrebbero svolgere compiti di assistenza automatizzati e agevolare il lavoro degli assistenti sanitari, migliorando, nel contempo, le cure fornite dal personale sanitario e rendendo il percorso di riabilitazione più mirato, consentendo così al personale medico e agli assistenti di dedicare più tempo alla diagnosi e a una migliore pianificazione delle opzioni terapeutiche», tuttavia bisogna «rispettare il principio dell'autonomia supervisionata dei robot, in base al quale la programmazione iniziale di cura e la scelta finale sull'esecuzione spetteranno sempre a un chirurgo umano*".

[19] V. su questi temi Simone Pieranni, *Il giudice e l'algoritmo: in Cina l'intelligenza artificiale arriva nei tribunali*, 8 febbraio 2019, https://ilmanifesto.it/il-giudice-e-lalgoritmo-in-cina-lintelligenza-artificiale-arriva-nei-tribunali/ in cui si dà conto di come in Cina l'intelligenza artificiale viene ormai applicata anche nel mondo giudiziario, per raccogliere prove, per uniformare le sentenze, senza alcun dibattito in merito. V. anche Dario Acquaro, Gli studi legali esplorano l'esito delle sentenze con l'intelligenza artificiale, 15 novembre 2018, https://www.ilsole24ore.com/art/norme-e-tributi/2018-11-14/intelligenza-artificiale-studi-legali-esplorano-l-esito-sentenze-195032.shtml?uuid=AE2TmsbG in cui si osserva come il mercato dei grandi studi americani e inglesi sia florido di investitori e veda oltre cento applicazioni di Ai già attive. E anche in Italia già da un pò di tempo alcuni studi legali esplorano l'esito delle sentenze con l'intelligenza artificiale.

[20] Con il contributo, peraltro, della Scuola Superiore Sant'Anna di Pisa.

[21] D. Lgs. 82/2005, come modificato dal D.Lgs. 26 agosto 2016, n. 179.

normativo, con i principi di fruibilità, disponibilità, accesso e riutilizzo dei dati pubblici. Sarà certamente necessario tuttavia che l'Autorità Garante per la protezione dei dati personali, AGID e ANAC agiscano in maniera coordinata nell'ottica della *governance*. Nel nostro ordinamento è centrale il rispetto del principio di trasparenza, pertanto dovrà essere applicato eventualmente ai sistemi di IA utilizzati nella PA nei procedimenti amministrativi (algoritmi, logiche di costruzione dei database, processo di funzionamento dei servizi). In special modo, alla luce dei recenti interventi del legislatore sugli obblighi di pubblicazione della PA e sull'accesso civico generalizzato[22]. Ci si chiede, infatti, come potrà la PA formulare criteri che le consentano di motivare i provvedimenti parzialmente elaborati da sistemi di IA e, più in generale, come tali provvedimenti possano avere un fondamento giuridico. Infine, è opportuno focalizzare l'attenzione sulla tutela giurisdizionale nei confronti di atti amministrativi adottati da sistemi di IA. Nel merito si è espresso nel 2017 il TAR del Lazio[23] che, esaminando un caso riguardante il diniego da parte del M.I.U.R. di accogliere un'istanza di accesso agli atti avente ad oggetto l'algoritmo relativo al *software* usato per gestire i trasferimenti in mobilità del personale docente, ha riconosciuto ai ricorrenti il diritto a conoscere l'algoritmo. Il MIUR aveva motivato il suo diniego alla luce della specifica tutela del software quale opera dell'ingegno e della non assimilabilità del codice sorgente alla categoria di documento amministrativo. Secondo il MIUR questo «atto» non rientra nella nozione di "documento amministrativo" ex art. 22, lett. d), L. 241/1990. Il TAR del Lazio ha invece sconfessato questa tesi stabilendo che la disciplina in materia di diritto d'autore protegge l'opera dell'ingegno da una riproduzione volta ad un eventuale sfruttamento economico da parte di terzi, senza precludere la riproduzione ai fini dell'esercizio del diritto di accesso, come in questo caso. Il Tar del Lazio ha ritenuto[24] inoltre che il programma informatico in questione rientri nella nozione di atto amministrativo c.d. informatico dunque il diritto di accesso, ex artt. 22 e ss. della l. 241/1990, al linguaggio informatico sorgente, deve essere riconosciuto ai ricorrenti, non essendo sufficiente la semplice descrizione dell'algoritmo e del suo funzionamento. In conclusione, i giudici amministrativi hanno affermato la non

[22] D. Lgs. 33/2013 e D. Lgs. 97/2016.

[23] Tar Lazio, sez. III bis, 14 febbraio 2017, n. 3769

[24] Con l'occasione il TAR si è soffermato sulla distinzione tra "atto amministrativo informatico", che viene creato mediante un programma di videoscrittura, e atto ad elaborazione elettronica, il software, il cui contenuto deriva da un procedimento automatizzato, per cui la sua determinazione è affidata completamente allo strumento informatico. Per il TAR "*l'ammissibilità dell'elaborazione elettronica dell'atto amministrativo non è legata alla natura discrezionale o vincolata dell'atto quanto invece essenzialmente alla possibilità, che tuttavia è scientifica e non invece giuridica, di ricostruzione dell'iter logico sulla base del quale l'atto stesso possa essere emanato per mezzo di procedure automatizzate quanto al relativo contenuto dispositivo*". Le modifiche ad opera della L. 15/2005, tuttavia, hanno allargato il raggio d'azione della nozione di "documento amministrativo" di cui all'art. 22, lett. d), l. 241/1990. Ciò che rileva è la valenza amministrativa del provvedimento e non la sua provenienza.

superabilità del diritto di accesso con le motivazioni esposte dal MIUR, tanto più perché nella formazione della graduatoria è stato decisivo il criterio decisionale insito nel *software*. Come era prevedibile, insomma, il diffondersi di tecnologie legate all'IA pone sempre più spesso questioni giuridiche di non poco conto, in particolare nell'ottica della responsabilità delle azioni dei sistemi di IA. A tal riguardo il Parlamento Europeo, nella Risoluzione del 16 febbraio 2017, invita il legislatore "*a definire una tassonomia dei robot in relazione al grado di autonomia della macchina e anche alla loro interazione con l'uomo e con l'ambiente […] Una volta individuati i soggetti responsabili in ultima istanza, la loro responsabilità dovrebbe essere proporzionale all'effettivo livello* di istruzioni *impartite al robot e al grado di autonomia di quest'ultimo*[25]*, di modo che quanto maggiore è la capacità di apprendimento o l'autonomia di un robot e quanto maggiore è la durata della formazione di un robot, tanto maggiore dovrebbe essere la responsabilità del suo formatore*". In futuro si avranno sempre più robot capaci di auto, apprendere ed auto-programmarsi, e tanto più, l'IA sarà autonoma tanto più a livello giuridico, ci si porrà il problema di sganciarla dal soggetto umano. Qualche anno fa, ad esempio, in un allenamento di *machine learning* nel laboratorio Facebook Artificial Intelligence Research (Fair), i ricercatori, al lavoro su *chatbot* che replicano conversazioni di negoziazione, si sono trovati davanti a risultati inaspettati in quanto le *chatbot* non solo hanno sviluppato strategie proprie di trattativa, ma anche utilizzato un linguaggio unico e non assimilabile a quello umano[26]. Ci si chiede allora quale natura giuridica assumeranno i robot e se la nostra società (il nostro ordinamento) sarà pronta ad attribuir loro soggettività giuridica. Per dirla con Iaselli, "*se cioè devono essere considerati soggetti o oggetti di diritto*"[27]. Alla luce di quanto esposto, è opportuno dunque riflettere sui rischi che si corrono nello standardizzare eccessivamente l'azione della PA, comprimendo gli spazi di discrezionalità dell'amministrazione e di partecipazione del cittadino[28]. Si ha la sensazione, infatti, che, attraverso l'uso sempre maggiore di sistemi di IA nell'attività della PA, sia il legislatore sia le Corti

[25] A seconda del grado di autonomia esistono vari tipi di robot. Alcuni sono comandati a distanza dall'uomo dunque non hanno alcuna autonomia; altri sono robot "ad autonomia debole", in cui l'uomo «si limita a fornire un input iniziale e un programma fornisce tutte le regole di comportamento del robot» che, quindi, è in grado di auto-guidarsi; infine esistono macchine molto sofisticate capaci di auto-programmarsi e, in alcuni casi, di apprendere dalla propria esperienza. Si tratta del *deep learning* (apprendimento profondo), vale a dire un esteso insieme di algoritmi basato su Reti Neurali Artificiali che rappresentano modelli di calcolo, valutazione ed elaborazione elettronica ispirati ai meccanismi di funzionamento del cervello umano. A tal proposito v. Taddei Elmi G., Romano F., Il robot tra *ius condendum* e *ius conditum*, Informatica e diritto, vol. XXV, 2016

[26] Diletta Perlangeli, I chatbot di Facebook hanno inventato un linguaggio tutto loro, 21 giugno 2017, https://www.wired.it/internet/web/2017/06/21/chatbot-facebook-linguaggio/?refresh_ce=

[27] Iaselli M., Robot con intelligenza artificiale, verso una soggettività giuridica?, 21 febbraio 2017, http://www.altalex.com. Riflessioni più approfondite su questi aspetti sono in Giuseppe Morano, Robotizzazione, intelligenza artificiale e p.a., http://www.neldiritto.it/appdottrina.asp?id=15772#.XNfhDI5KjIV

[28] Michela Tresca, I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale, III Colloquio italo-francese sul Diritto del Web, Università LUISS Guido Carli, 21 giugno 2018, Medialaws - Rivista di diritto dei media n. 3/2018

interverranno sempre di più su questioni giuridiche legate al bilanciamento tra diversi diritti quali diritto di accesso agli atti amministrativi, trasparenza, riservatezza, diritto d'autore ed altri ancora. Soprattutto per non delegare totalmente alle macchine compiti importanti che deve svolgere l'uomo. Lo stesso Garante per la protezione dei dati personali ha affermato che "*gli algoritmi non sono matematica pura, infallibile e neutra, ma piuttosto opinioni umane strutturate in forma matematica e riflettono quindi spesso, in misura più o meno rilevante, le precomprensioni di chi li progetta o le serie storiche assunte a riferimento. Con il rischio, dunque, non soltanto di cristallizzare il futuro nel passato, leggendo sempre il primo con gli schemi del secondo, ma anche di assumere le correlazioni (quasi sempre contingenti) delle serie storiche considerate, come relazioni necessariamente causali*"[29].

2. Le Linee Guida Etiche sull'Intelligenza Artificiale del Gruppo di Esperti della Commissione europea[30].

Un altro esempio di *soft-law* è rappresentato dalle Linee Guida Etiche sull'Intelligenza Artificiale predisposte dal Gruppo di Esperti della Commissione europea. Questa ha come obiettivo la promozione di una IA "etica, sicura e all'avanguardia in Europa", comprendendo in questo obiettivo non solo i sistemi di intelligenza artificiale realizzati in Europa, ma anche quelli sviluppati altrove e utilizzati in Europa. Alla base della visione della Commissione si pongono tre pilastri. Il primo è la volontà di aumentare gli investimenti pubblici e privati nell'IA per aumentarne la diffusione. Il secondo pilastro è quello di preparare i cambiamenti socioeconomici. Il terzo è quello di assicurare un quadro etico e giuridico appropriato rafforzando i valori europei. A tale scopo la Commissione ha istituito un Gruppo di Esperti di alto livello sull'IA[31], incaricato della stesura di due documenti: le Linee guida sull'etica dell'IA e le Raccomandazioni politiche e di investimento[32]. Tali Linee Guida articolano un quadro per il raggiungimento di una IA affidabile, basato sui diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea e dalle norme internazionali sui diritti umani[33]. Il Gruppo sostiene che l'IA abbia il potenziale per trasformare significativamente la nostra società, essendo un mezzo

[29] Antonello Soro, Uomini e macchine, Atti del convegno "*Protezione dati per un'etica del digitale*", p. 7, ove il Garante cita anche l'algoritmo utilizzato negli Usa per il calcolo del rischio di recidiva penale, che si è dimostrato incline ad assegnare, in assenza di ragioni criminologiche, un tasso maggiore ai neri rispetto ai bianchi, solo sulla base delle correlazioni desunte da una determinata serie storica assunta a riferimento.

[30] European Commission, *High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/futurium/en/ai-alliance-consultation, 8 April 2019

[31] AI HLEG, d'ora in avanti "Gruppo".

[32] I prossimi *step* prevedono una "fase "pilota" dall'estate al dicembre del 2019 alla quale tutte le parti interessate potranno partecipare, nonché una revisione delle Linee Guida entro il 2020 da parte del Gruppo.

[33] V. anche *Intelligenza artificiale e protezione dei dati*: sfide e possibili rimedi, Relazione di Alessandro Mantelero al Rapporto sull'intelligenza artificiale del Comitato consultivo della Convenzione per la protezione dei singoli per quanto riguarda l'elaborazione automatica dei dati personali, Strasburgo, 25 gennaio 2019, p. 3

per aumentare la prosperità umana, migliorando così il benessere individuale e sociale e il bene comune, oltre a portare progresso e innovazione. In particolare, i sistemi di IA possono contribuire a facilitare il raggiungimento degli Obiettivi di Sviluppo Sostenibile delle Nazioni Unite[34]. Secondo il Gruppo, tuttavia, i sistemi di IA, che devono essere incentrati sull'uomo, portano con sé alcuni rischi che devono essere gestiti in modo appropriato e questa fase di sviluppo è il momento giusto per farlo. Si possono così massimizzare i benefici dei sistemi di IA e allo stesso tempo prevenire e ridurre al minimo i rischi. Gli esseri umani e le comunità avranno fiducia nello sviluppo della tecnologia e nelle sue applicazioni se sarà chiaro il modo per raggiungere la loro affidabilità. L'affidabilità è dunque il prerequisito fondamentale per sviluppare, distribuire e utilizzare i sistemi di IA. Per affidabilità si intende non solo l'affidabilità del sistema dell'IA, ma anche di tutti gli attori e dei processi che fanno parte del contesto socio-tecnico del sistema. Questa affidabilità passa, per il momento, per tre componenti, tutti indispensabili, che devono essere soddisfatti durante l'intero ciclo di vita del sistema, il quale deve essere lecito, rispettando tutte le leggi e i regolamenti applicabili; etico, garantendo l'aderenza ai principi e ai valori etici; robusto, sia dal punto di vista tecnico che sociale, poiché, anche con buone intenzioni, i sistemi di IA possono causare conseguenze indesiderate. Bisogna lavorare per garantire che non ci siano tensioni tra questi tre elementi, anche in ottica legislativa. In definitiva, le Linee Guida hanno lo scopo di promuovere un'innovazione responsabile e sostenibile in Europa, dunque sono rivolte a tutti coloro che progettano, sviluppano, implementano, utilizzano, o sono influenzate dall'IA (società, organizzazioni, ricercatori, servizi pubblici, agenzie governative, istituzioni, organizzazioni della società civile, individui, lavoratori e consumatori). I sistemi di IA sono già regolamentati a livello europeo[35] e internazionale[36] nonché dalle legislazioni degli Stati membri dell'UE, infatti, le Linee Guida non forniscono consigli su come garantire la conformità legale dell'IA né creano diritti legali o impongono obblighi legali a terzi. Le Linee Guida mirano a offrire una guida sulla promozione e la messa in sicurezza del secondo e terzo requisito (IA etica e IA robusta) in quanto la realizzazione di questi può andare oltre gli obblighi legali esistenti. Affinché i sistemi di IA siano affidabili, dovrebbero anche essere etici, tanto più perché le leggi non sono sempre al passo con gli sviluppi tecnologici e a volte

[34] Ovvero promuovere l'equilibrio di genere e affrontare il cambiamento climatico, razionalizzare il nostro uso delle risorse naturali, migliorare i nostri processi di salute, mobilità e produzione e sostenere il modo in cui si monitorano i progressi contro gli indicatori di sostenibilità e di coesione sociale.

[35] Oltre ai Trattati dell'Unione europea e alla Carta dei diritti fondamentali, rilevano in tal senso il regolamento generale sulla protezione dei dati, la direttiva sulla responsabilità da prodotto, il regolamento sul Flusso di dati non personali, le direttive antidiscriminazione, il diritto dei consumatori e le direttive sulla sicurezza e la salute sul lavoro.

[36] V. i Trattati sui diritti umani delle Nazioni Unite e le Convenzioni del Consiglio d'Europa (come la Convenzione europea sui diritti umani).

possono essere in contrasto con le norme etiche o semplicemente non essere adatte ad affrontare determinati problemi. I sistemi di IA non devono causare danni non intenzionali, dunque, dovrebbero essere previste misure di sicurezza. La solidità dei sistemi di IA sia dal punto di vista tecnico che sociale poiché, anche con buone intenzioni, i sistemi di IA possono causare danni non intenzionali. Le Linee Guida, che non intendono sostituire alcuna forma di regolamentazione attuale o futura, né mirano a scoraggiare la sua introduzione, ma sono soltanto un punto di partenza per la discussione sull'IA, sono strutturate in tre livelli di astrazione, dal più astratto (Capitolo I) al più concreto (Capitolo III), e terminano con esempi di opportunità e criticità sollevate dai sistemi di IA. Il Primo Capitolo è basato su un approccio fondato sui diritti fondamentali ed identifica e descrive i principi etici e i valori ad essi correlati che devono essere rispettati nello sviluppo, nella distribuzione e nell'uso dei sistemi di IA: questo ricorso ai diritti fondamentali contribuisce anche a limitare l'incertezza normativa. I quattro principi etici, radicati nei diritti fondamentali, che devono essere rispettati al fine di garantire che i sistemi di IA siano sviluppati, distribuiti e utilizzati in maniera affidabile, sono specificati come imperativi etici per gli "addetti ai lavori". Questi principi sono: il rispetto dell'autonomia umana, fortemente associato al diritto alla dignità e alla libertà umana (artt.1 e 6 della Carta); la prevenzione del danno, strettamente legata alla protezione dell'integrità fisica o mentale (riflessa nell'articolo 3); l'equità; l'esplicabilità. Molti di questi principi sono già stati in larga misura ispiratori delle normative esistenti[37]. Nell'ambito di questi principi rientrano le situazioni che coinvolgono gruppi più vulnerabili come bambini, persone con disabilità e altri che sono storicamente stati svantaggiati o sono a rischio di esclusione, e a situazioni che sono caratterizzate da asimmetrie di potere o informazione, come tra datori di lavoro e lavoratori o tra imprese e consumatori. A tal proposito il Gruppo si è ispirato alla Carta dei diritti fondamentali dell'UE[38]. Inoltre, i sistemi di IA possono avere impatti negativi difficili da prevedere, identificare o misurare, ad esempio sulla democrazia, lo stato di diritto e la giustizia distributiva, o sulla stessa mente umana. Fondamentale sarà allora adottare misure adeguate per attenuare questi rischi appropriate e proporzionali all'entità del rischio. Il secondo capitolo fornisce indicazioni su come realizzare un'IA affidabile, traducendo i principi etici in sette requisiti chiave che i sistemi di IA dovrebbero implementare e soddisfare durante l'intero ciclo di vita. Sia i metodi tecnici che quelli non tecnici possono essere utilizzati per la loro implementazione. Diversi gruppi di parti interessate hanno ruoli diversi da svolgere nel garantire che i requisiti siano soddisfatti: gli sviluppatori

[37] Si pensi ad esempio al Regolamento UE 2016/679 sulla protezione dei dati personali (GDPR) o ai Regolamenti UE sulla tutela dei consumatori.

[38] Questa, agli articoli da 24 a 27, si occupa dei diritti dei minori e degli anziani, dell'integrazione delle persone con disabilità e dei diritti dei lavoratori e, all'articolo 38, della protezione dei consumatori.

nell'ambito della progettazione e dello sviluppo; i responsabili della distribuzione assicurandosi che i sistemi che utilizzano e i prodotti e i servizi che offrono soddisfino i requisiti; gli utenti finali dovrebbero conoscere i requisiti che possono pretendere dai sistemi IA. I requisiti, che non sono esaustivi, sono: l'agenzia e la supervisione umana (i diritti fondamentali, l'agenzia umana e la supervisione umana); la solidità tecnica e sicurezza (resilienza agli attacchi e alla sicurezza, piano di riserva e sicurezza generale, accuratezza, affidabilità e riproducibilità), la *privacy* e la *governance* dei dati (il rispetto per la privacy, la qualità e l'integrità dei dati e l'accesso ai dati); la trasparenza; la diversità, la non discriminazione e l'equità (divieto di pregiudizi sleali, accessibilità e design universale e partecipazione dei soggetti interessati); il benessere sociale e ambientale (sostenibilità e compatibilità ambientale, impatto sociale, società e democrazia); la responsabilità (auditabilità, minimizzazione e comunicazione dell'impatto negativo, dei compromessi e dei mezzi di ricorso). Potendo nascere tensioni tra diversi principi e requisiti, sarà opportuno identificare, valutare, documentare e comunicare continuamente queste situazioni e le relative soluzioni; oltre alla promozione della ricerca nell'ambito dell'IA, infatti, hanno un ruolo rilevante la comunicazione e l'interazione tra le parti interessate[39]. Il terzo capitolo fornisce agli operatori di IA una guida pratica, con una lista di valutazione dell'IA affidabile, finalizzata a rendere operativi i sette requisiti chiave. Questo dovrà essere adattato al caso d'uso specifico del sistema di IA. Le Linee Guida, opportunamente, segnalano che tale elenco di valutazione, o *assessment*, non sarà mai esaustivo: garantire un'IA affidabile non si riassume in cose da fare o "caselle da spuntare", ma nell'identificazione e nell'implementazione continua dei requisiti, nella valutazione delle soluzioni, nella garanzia di migliori risultati nell'intero ciclo di vita del sistema di IA con il coinvolgimento degli *stakeholders* in questo. Una sezione finale delle Linee Guida, infine, offre alcuni importanti esempi di opportunità vantaggiose e criticità generate dai sistemi di IA, che dovrebbero servire a stimolare ulteriori dibattiti. Tra i sette requisiti figurano quelli della solidità tecnica e della sicurezza. La presenza attiva di altri agenti (umani e artificiali) nei sistemi di IA potrebbe infatti minacciare l'integrità fisica e mentale degli esseri umani, che deve essere sempre garantita. I sistemi IA, come tutti i sistemi software, dovrebbero essere protetti contro le vulnerabilità che possono consentire loro di essere sfruttati dagli "hackers". Gli attacchi possono riguardare i dati (avvelenamento dei dati), il modello (fuga di modelli) o l'infrastruttura sottostante, software e/o hardware. Il livello delle misure di sicurezza richieste,

[39] con attività quali la diffusione dei risultati e l'apertura di pubbliche consultazioni; la formazione sistematica di una nuova generazione di esperti in etica dell'intelligenza artificiale; la comunicazione, in modo chiaro e proattivo, delle informazioni alle parti interessate in merito alle capacità e ai limiti del sistema di intelligenza artificiale; la promozione della tracciabilità e dell'auditabilità dei sistemi di IA, in particolare in contesti o situazioni critici; il coinvolgimento delle parti interessate in tutto il ciclo di vita del sistema IA

allora, dipende dall'entità del rischio rappresentato da un sistema di IA, che a sua volta dipende dalle capacità del sistema. Precisione, affidabilità e riproducibilità sono fondamentali, così come il rispetto dell'art. 22 GDPR. Allo stesso modo importante è certamente il diritto alla riservatezza, strettamente legato al principio di prevenzione del danno. I sistemi IA devono garantire la *privacy* e la protezione dei dati nell'intero ciclo di vita di un sistema e per far ciò è sufficiente il rispetto del GDPR e della Direttiva *ePrivacy*[40]. In questo ambito sono incluse le informazioni inizialmente fornite dall'utente, così come le informazioni generate sull'utente nel corso della loro interazione con il sistema. Le registrazioni digitali del comportamento umano possono consentire ai sistemi di IA di interferire non solo con le preferenze delle persone, ma anche con l'orientamento sessuale, età, sesso, opinioni religiose o politiche delle persone. Per far si che le persone si fidino del processo di raccolta dei dati, è necessario garantire che i dati raccolti su di esse non vengano utilizzati per discriminare illegalmente o ingiustamente. Per quanto riguarda l'accesso ai dati, in ogni organizzazione che gestisce i dati personali, devono essere messi in atto protocolli che regolino l'accesso ai dati, che indichino i profili di autorizzazione all'accesso dei dati e in quali circostanze. Solo il personale debitamente qualificato con la competenza e la necessità di accedere ai dati individuali dovrebbe essere autorizzato a farlo. Infine, la prevenzione del danno alla privacy richiede un'adeguata *governance* dei dati che deve riguardare anzitutto la qualità dei dati utilizzati. Quando i dati vengono raccolti possono contenere pregiudizi sociali ed inesattezze e questo problema deve essere affrontato prima del *training* con un insieme di dati. La qualità dei set di dati utilizzati è fondamentale per le prestazioni dei sistemi di IA. In secondo luogo deve riguardare l'integrità dei dati utilizzati: l'alimentazione di dati dannosi in un sistema di IA può cambiare il suo comportamento, in particolare con i sistemi di autoapprendimento. I processi e i set di dati utilizzati devono essere testati e documentati in ogni fase, come pianificazione, formazione, test e implementazione. Questo dovrebbe valere anche per i sistemi di IA che non sono stati sviluppati internamente, ma acquisiti all'esterno. La *governance* dei dati deve, altresì, riguardare anche la rilevanza dei dati nell'ambito in cui verranno implementati i sistemi IA, nonché i protocolli di accesso e la capacità di elaborare i dati in modo tale da proteggere la *privacy*. In chiusura è opportuno un chiarimento sulle relazioni intercorrenti tra il Regolamento UE 2016/679 e la Direttiva *ePrivacy* citata pocanzi, e su questo è intervenuto di recente il Comitato Europeo per la protezione dei dati (EPDB)[41]. Si tratta di un organo

[40] Direttiva 2002/58/CE del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), modificata dalle Direttive 2009/136/CE e 2009/140/CE.

[41] Di esso fanno parte i rappresentanti delle autorità nazionali per la protezione dei dati e il Garante europeo (GEPD)

indipendente che contribuisce all'applicazione uniforme delle norme sulla protezione dei dati in tutta l'Unione Europea, promuovendo la cooperazione tra le autorità di controllo dei Paesi membri. Il Comitato ha chiarito[42] che l'esistenza di una sovrapposizione tra la Direttiva e il Regolamento non necessariamente implica un conflitto tra norme. È lo stesso art. 1 par. 2 della Direttiva *ePrivacy* ad affermare che le disposizioni della Direttiva precisano ed integrano quelle del GDPR con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche. Pertanto, in ossequio al principio di specialità, dovrà essere fatto un raffronto in concreto tra le norme e, ove una disposizione della Direttiva renda più specifica una regola del GDPR, la prima prevarrà sulla seconda. Sono ad esempio norme speciali rispetto al GDPR gli articoli 5, 6, 9 e 13 della direttiva *ePrivacy* che riguardano, rispettivamente, le informazioni archiviate sui *device* dei cittadini, i dati sul traffico, i dati sull'ubicazione, le comunicazioni indesiderate, i cookies. È opportune segnalare, però, che il 13 marzo scorso l'EDPB ha invitato[43] i Paesi membri ad accelerare nell'adozione del nuovo Regolamento ePrivacy, che sostituirà la Direttiva *ePrivacy*.

3. La Convenzione 108.

Il Consiglio d'Europa nel 1981 adottò la Convenzione n. 108[44] allo scopo di "*garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano (protezione dei dati)*". La Convenzione sancì che il trattamento e la raccolta dei dati devono avvenire rispettando alcuni principi: qualità dei dati, correttezza, liceità e finalità del trattamento. I dati devono essere raccolti e trattati solo in base a specifiche norme che ne autorizzano il trattamento automatizzato, devono essere trattati per scopi specifici legittimi e non devono essere destinati a un uso incompatibile con la finalità di trattamento originaria. Infine, non devono essere conservati oltre il tempo necessario per raggiungere lo scopo prefissato. I dati devono essere corretti, pertinenti allo scopo e non eccessivi rispetto alla finalità perseguita. Sono i principi fondamentali che reggono l'intera normativa in materia di protezione dei dati personali. La Convenzione vietò, altresì, di trattare

[42] Opinione n. 5 del 2019

[43] *Statement 3/2019 on the future ePrivacy Regulation*, 13 marzo 2019, con cui il Comitato Europeo per la Protezione dei Dati (EDPB) sollecita nuovamente l'adozione del Regolamento ePrivacy che dovrà sostituire la Direttiva ePrivacy 2002/58/CE in tema di protezione dati nelle comunicazioni elettroniche. Il Comitato invita i legislatori nazionali ad intensificare gli sforzi verso l'adozione di una regolamentazione che è essenziale al completamento del rinnovato quadro normativo europeo sulla protezione dei dati personali. Il Regolamento ePrivacy non dovrà in alcun caso abbassare il livello di tutela garantito dalla Direttiva e dovrà integrare il GDPR disponendo ulteriori forti garanzie per tutti i tipi di comunicazione elettronica.

[44] Convenzione n. 108/1981, per la protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale, al fine di regolamentare i flussi transnazionali dei dati e assecondare l'esigenza di tutela dei diritti degli individui dai pericoli e dagli abusi nell'ambito dei nuovi mezzi di comunicazione.

dati sensibili, quali la razza, le opinioni politiche e la salute, in assenza di adeguate garanzie giuridiche, stabilendo anche il diritto del cittadino ad ottenere informazioni sui suoi dati e la loro eventuale rettifica. L'importanza della Convenzione è data dal fatto che essa è l'unico strumento giuridicamente vincolante a livello internazionale in tale materia, potendo ad essa aderire anche Stati non membri del Consiglio d'Europa[45]. Allo scopo di rafforzare la protezione dei dati personali a livello mondiale il 18 maggio del 2018 il Consiglio d'Europa, che oggi conta 47 Stati aderenti, ha adottato un protocollo di modifica (detto anche Convenzione 108+) del testo della Convenzione, teso a modernizzarla[46]. Il protocollo contiene diverse novità e fornisce un quadro giuridico robusto e flessibile per facilitare il flusso dei dati attraverso le frontiere avendo al contempo garanzie efficaci. Esso introduce innovazioni rilevanti rafforzando gli obblighi di trasparenza a carico dei titolari del trattamento, come l'obbligo di comunicare le violazioni dei dati (*data breach*) e di assicurare un approccio di *privacy by design*. I diritti degli interessati, che ora racchiudono anche il diritto a non essere soggetto a decisioni puramente automatizzate e a conoscere la logica del trattamento, vengono ampliati. Il Protocollo rafforza infine i compiti delle Autorità di protezione dati e del Comitato della Convenzione, chiamato a svolgere un ruolo nella valutazione dell'effettivo rispetto dei principi della Convenzione che deve essere assicurato dai Paesi che ne faranno parte. Il Protocollo istituisce un quadro giuridico multilaterale solido e flessibile, destinato a prevenire gli abusi e a facilitare il flusso transfrontaliero di dati, fornendo al contempo efficaci garanzie in caso di utilizzo di dati personali. L'Italia è il ventiseiesimo Paese ad aver ratificato[47] la Convenzione 108+, un provvedimento che, combinato con il Regolamento UE 2016/679, garantirà una doppia tutela ai cittadini in materia di protezione dei dati personali. Il Protocollo è importante anche per l'Intelligenza artificiale, dato che esso si applicherà nell'ambito di ricerca e sviluppo di sistemi di IA. Infatti, come ribadito dal Comitato Convenzione 108 nelle sue Linee guida[48] in materia di intelligenza artificiale e protezione dei dati, tutti i progetti basati sull'IA dovrebbero rispettare i contenuti della Convenzione, vigilando sugli algoritmi ed attuando valutazioni d'impatto circa le possibili conseguenze sui diritti fondamentali, al fine di minimizzare i rischi. Mantelero[49] ha affermato che per

[45] Ad esempio, nel 2013 vi ha aderito l'Uruguay.

[46] Convenzione modernizzata per la protezione delle persone con riguardo al trattamento dei dati personali, 128.ma sessione del Comitato dei Ministri (Elsinore, Danimarca 17-18 maggio 2018), v. https://www.coe.int/en/web/data-protection/convention108/modernised

[47] Il 5 marzo 2019 l'ambasciatore **Michele Giacomelli**, rappresentante permanente d'Italia presso il Consiglio d'Europa, ha sottoscritto l'Accordo.

[48] Comitato Convenzione 108, Linee Guida in materia di intelligenza artificiale e protezione dei dati, 25 gennaio 2019

[49] *Intelligenza artificiale e protezione dei dati: sfide e possibili rimedi*, Relazione di Alessandro Mantelero al Rapporto sull'intelligenza artificiale del Comitato consultivo della Convenzione per la protezione dei singoli per quanto riguarda l'elaborazione automatica dei dati personali, Strasburgo, 25 gennaio 2019, p. 5

scongiurare una futura "dittatura dei dati", imposti da potenziali *data scientist* insensibili alle problematiche sociali, è necessario basarsi sui principi della Convenzione 108 come fondamento di una fiorente società digitale e mettere in campo un piano d'azione basato su tre direttive fondamentali: un approccio basato sui valori (comprendente valori sociali ed etici), una valutazione e gestione dei rischi, nonchè la partecipazione dei cittadini. Bisogna sottolineare la centralità dell'essere umano nello sviluppo tecnologico e, dunque, nello sviluppo di sistemi AI. Ciò significa riaffermare i diritti fondamentali in questo campo. In questo senso, il diritto alla protezione dei dati personali può diventare una pietra miliare verso la progettazione di una società dei dati diversa, in cui lo sviluppo dell'IA non è guidato dal puro interesse economico o da una disumanizzante efficienza algoritmica. La Convenzione 108+ è formata da trentuno articoli in otto capitoli più un'Appendice. All'art. 1 della Convenzione è esplicato il suo scopo, vale a dire quello di proteggere ogni individuo, indipendentemente dalla sua nazionalità o residenza, in relazione al trattamento dei suoi dati personali, contribuendo in tal modo al rispetto dei suoi diritti umani e delle sue libertà fondamentali, e in particolare del diritto alla *privacy*. Il secondo Capitolo della Convenzione è dedicato ai principi di base per la protezione dei dati personali: legittimità dell'elaborazione dei dati (art. 5) e qualità dei dati, sicurezza dei dati (art. 7) e trasparenza del trattamento (art. 8). Quanto alla tutela dei diritti degli interessati, l'art. 9 par. 1, stabilisce che ogni individuo ha diritto a non essere soggetto a una decisione che lo riguardi in modo significativo esclusivamente sulla base di un trattamento automatizzato di dati senza che le sue opinioni vengano prese in considerazione. Seguendo, la Convenzione stabilisce che tutti hanno diritto ad ottenere, a richiesta, a intervalli ragionevoli e senza eccessivo ritardo o spesa, la conferma del trattamento dei dati personali che li riguardano, la comunicazione in forma intelligibile dei dati trattati, tutte le informazioni disponibili sulla loro origine, sulla conservazione, così come ogni altra informazione che il responsabile del trattamento è tenuto a fornire al fine di garantire la trasparenza del trattamento. Ancora, tutti hanno diritto ad ottenere, su richiesta, conoscenza del ragionamento alla base dell'elaborazione dei dati in cui gli vengono applicati i risultati di tale trattamento e di opporsi in qualsiasi momento, per motivi relativi alla loro situazione, al trattamento di dati personali che li riguardano a meno che il responsabile del trattamento non dimostri motivi legittimi per il trattamento che prevalga sui suoi interessi o diritti e sulle libertà fondamentali. Infine, tutti hanno diritto ad ottenere, su richiesta, gratuitamente e senza eccessivo ritardo, rettifica o cancellazione, a seconda dei casi, di tali dati se questi sono, o sono stati, trattati in violazione delle disposizioni della Convenzione, ad avere un rimedio e a beneficiare, a prescindere dalla nazionalità o residenza, all'assistenza di un'autorità di controllo. Il Capitolo III è dedicato ai flussi transfrontalieri di dati personali. L'art. 14 stabilisce che una Parte, al solo scopo di proteggere i dati personali, non può vietare, o

subordinatamente all'autorizzazione speciale, il trasferimento di tali dati a un destinatario soggetto alla giurisdizione di un'altra Parte della Convenzione. Tuttavia, una tale Parte può farlo se sussiste un rischio reale e grave che il trasferimento a un'altra Parte o all'altra Parte di una non Parte porti a eludere le disposizioni della Convenzione. Una Parte può anche farlo, se vincolato da norme di protezione armonizzate condivise da Stati appartenenti a un'organizzazione internazionale regionale. Quando il destinatario è soggetto alla giurisdizione di uno Stato o di un'organizzazione internazionale che non è Parte della Convenzione, il trasferimento di dati personali può avvenire soltanto laddove sia garantito un livello adeguato di protezione basato sulle disposizioni della presente Convenzione. Un livello adeguato di protezione può essere garantito dalla legge di tale Stato o organizzazione internazionale, inclusi i trattati e gli accordi internazionali applicabili; oppure da garanzie standardizzate ad hoc o approvate, fornite da strumenti giuridicamente vincolanti e esecutivi, adottati e attuati dalle persone coinvolte nel trasferimento e nell'ulteriore trattamento. Fatte salve queste disposizioni, ciascuna Parte può prevedere che il trasferimento di dati personali possa aver luogo se l'interessato ha espresso un consenso esplicito, specifico e libero, dopo essere stato informato dei rischi insorti in assenza di adeguate garanzie; se gli interessi specifici dell'interessato lo richiedono nel caso specifico; se gli interessi legittimi prevalenti, in particolare gli interessi pubblici importanti, sono previsti dalla legge e tale trasferimento costituisce una misura necessaria e proporzionata in una società democratica; infine se costituisce una misura necessaria e proporzionata in una società democratica per la libertà di espressione. Altri Capitoli sono dedicati alle Autorità di controllo, alla cooperazione e assistenza reciproca, all'assistenza agli interessati, al Comitato della Convenzione.