Focus

Intelligenza artificiale e diritto: le sfide giuridiche in ambito pubblico

Fernanda Faini*

ARTIFICIAL INTELLIGENCE AND LAW: LEGAL CHALLENGES IN PUBLIC LAW

ABSTRACT: The contribution aims to examine the main legal challenges related to the use of artificial intelligence in the public sphere. In this context, the problems are peculiar as a consequence of the public nature of the subject involved, of the complex governance and of the significant ethical and social implications. Artificial intelligence solutions in the public sphere must comply with the relevant legislation and may lead to critical issues in the definition of ownership and in the identification of the related responsibilities; compliance with the data protection rules necessary to protect the person can be particularly problematic. The analysis aims to show that the technological approach alone is not enough, but it must be guided by the ability to direct the technique by means of law and by a solid ethical approach, based on accountability, transparency and openness.

KEYWORDS: artificial intelligence; public sector; data; algorithms; data protection

1. Intelligenza artificiale, dati e algoritmi

Nell'era tecnologica, gli ordinamenti giuridici sono chiamati a regolare l'"esistenza digitale" dell'uomo, parte integrante della vita, e gli strumenti che la caratterizzano.

Nella società attuale, attraversata da quella che viene definita come rivoluzione 4.0[1], un ruolo di estrema rilevanza ha assunto l'intelligenza artificiale, il cui impiego risulta potenzialmente particolarmente proficuo nel contesto pubblico, ambito preso in esame dal presente contributo.

* *Dottoressa di ricerca (PhD) in diritto e nuove tecnologie presso l'Università di Bologna, collabora nell'insegnamento di Informatica giuridica presso l'Università degli Studi di Firenze ed è docente del corso "Diritto e nuove tecnologie" presso l'Università Telematica Internazionale Uninettuno. Responsabile dell'assistenza giuridica in materia di amministrazione digitale, innovazione tecnologica e informatica giuridica presso la Regione Toscana. Mail: fernandafaini@gmail.com.* *Contributo sottoposto al referaggio del Comitato Scientifico.*

[1] Si usa il termine "Industria 4.0" o "Fabbrica 4.0" per indicare la quarta rivoluzione industriale idonea a rendere la produzione interamente digitale, interconnessa ed automatizzata.

ISSN 2284-4503

Focus

L'analisi delle sfide giuridiche poste dall'impiego dell'intelligenza artificiale in ambito pubblico necessita preventivamente dell'esame del fenomeno stesso, al fine di individuarne gli elementi caratterizzanti e poter valutare le problematiche poste al diritto.

L'Unione europea, in una comunicazione del 2018, individua con l'espressione intelligenza artificiale «sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi»; viene precisato che i software basati sull'intelligenza artificiale possono consistere «in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)»[2]. Per sviluppare soluzioni di intelligenza artificiale, come evidenzia la stessa Unione europea, sono necessari ingenti volumi di dati; quei dati sono elaborati da algoritmi, al fine di raggiungere il risultato cui le soluzioni di intelligenza artificiale sono rivolte.

Di conseguenza, l'anima delle soluzioni di intelligenza artificiale è formata da enormi quantità di dati, in specifico *big data*, e da algoritmi, capaci di "animare" i dati a disposizione e di estrarne il valore[3].

I *big data* consistono in enormi volumi di dati detenuti da grandi organizzazioni (poteri pubblici e multinazionali private), provenienti da diverse fonti e analizzati per mezzo di algoritmi, tecniche di *data mining*, *big data analytics*, *machine learning* e altre tecniche specifiche. Dalla definizione stessa emerge, accanto al volume, un'altra caratteristica fondamentale, ossia l'eterogeneità dei dati che compongono i *big data*.

Nella società contemporanea si tende a "datizzare" tutto ciò che ci circonda, convertendo i fenomeni in dati e inserendo sensori e rilevatori nella realtà al fine di produrre enormi quantità di dati analizzabili da potenti algoritmi: gli algoritmi costituiscono il "motore" capace generare valore grazie all'utilizzo e all'elaborazione di dati eterogenei[4]. Non a caso, la dimensione che caratterizza i *big data*, accanto alla varietà[5] e al volume[6], è proprio la velocità, che richiama la capacità degli algoritmi di analizzare i dati e che sottende la rilevanza della dinamicità[7].

---

[2] Comunicazione della Commissione europea «L'intelligenza artificiale per l'Europa» COM (2018) 238 final del 25 aprile 2018. Sotto tale profilo rileva, altresì, la Risoluzione del Parlamento europeo del 16 febbraio 2017 recante «raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica».

[3] L. AGRO', *Internet of Humans, Milano*, 2017, 73: rispetto all'intelligenza umana «l'intelligenza di una macchina, per quanto evoluta, parte da presupposti diversi e si basa su grandi quantità di dati e molteplici algoritmi che concorrono per ottenere un risultato sulla base di questi dati, o per generare nuovi algoritmi pur di raggiungere il risultato richiesto».

[4] Cfr. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, trad. it., Milano, 2013, 103 ss.

[5] La varietà riguarda l'eterogeneità della tipologia e dei formati dei dati, provenienti da fonti diverse (strutturate e non).

[6] Il volume si riferisce alla capacità di acquisire, memorizzare, accedere ed elaborare enormi quantità di dati.

[7] In dottrina sono considerate quali caratteristiche dei big data anche due dimensioni ulteriori: il valore, ossia il valore dei big data come insieme, e la veracità o veridicità, ossia la qualità e l'accuratezza dell'analisi. Da questi profili deriva il paradigma delle 3, 4 o 5 "V" dei big data (a seconda degli aspetti presi in considerazione): volume, velocità, varietà, valore e veracità; cfr. F. DI PORTO, *La rivoluzione Big Data. Un'introduzione*, in *Concorrenza e mercato*, 2016, 5 ss.

ISSN 2284-4503

Oggi è tecnicamente possibile analizzare tendenzialmente tutti i dati a disposizione: gli algoritmi portano a rinunciare alle ipotesi predeterminate e alla ricerca della causalità, affidandosi invece alle correlazioni e alle inferenze tra dati e poggiando sulla probabilità (e sulla correlata dose di "confusione"); in un percorso inverso rispetto al passato, si risale dai fenomeni alla valutazione delle probabili cause. In altri termini, gli algoritmi si basano sulle correlazioni che emergono dalle analisi sui dati e su metodologie deterministiche[8] e, in tal modo, sono capaci di strutturare le informazioni e automatizzare i processi[9]: con espressione efficace «codificano il mondo, lo classificano e predicono il nostro futuro»[10].

Il funzionamento degli algoritmi, su cui si basano le soluzioni di intelligenza artificiale, evidenzia sotto diversi profili il contrasto ontologico con il ragionamento giuridico alla base del diritto e con il modo di vedere la realtà da parte dei giuristi.

Gli algoritmi prediligono un metodo descrittivo che si differenzia dal carattere prescrittivo del diritto e si basano su fenomeni, numeri e calcoli, mentre il diritto è orientato ai valori della società di riferimento. L'algoritmo si nutre di dinamicità, mentre il diritto è "formale" e, in un certo senso, necessariamente "lento". Più ampiamente gli algoritmi sono fondati su metodologie deterministiche, che si basano su fenomeni, su circostanze oggettive e su probabilità e che rischiano, così, di inficiare le scelte individuali e la libera volontà, su cui poggiano i nostri ordinamenti giuridici[11].

Proprio in ciò che gli algoritmi permettono di fare emergono il valore e la conseguente attenzione rivolta all'intelligenza artificiale, capace di raggiungere diverse e significative finalità.

Innanzitutto le analisi compiute sui dati da parte degli algoritmi di intelligenza artificiale permettono di estrarre conoscenza, che si traduce nell'interpretazione dei bisogni, nell'ottimizzazione dei processi amministrativi, nella profilazione degli utenti, nel supporto alle decisioni. Gli algoritmi si atteggiano a moderni oracoli, dal momento che la conoscenza che consentono può consistere anche in una vera e propria capacità predittiva: ferme restando le connessioni false o apparenti, elevate correlazioni indicano alte probabilità, che permettono di fare previsioni sul futuro[12]. Di conseguenza, gli algoritmi consentono di effettuare predizioni sugli andamenti di mercato, di indicare preventivamente l'usura di infrastrutture, di migliorare diagnosi e cure, di prevenire disastri, di prendere decisioni politiche e, anche, di contribuire alla vittoria di elezioni[13].

La conoscenza del presente e la capacità di predizione del futuro si configurano come profili di particolare interesse in ambito pubblico.

Le amministrazioni pubbliche, infatti, hanno nella propria disponibilità enormi volumi di dati e relative banche dati, strumentali all'esercizio dei propri compiti. Le soluzioni di intelligenza artificiale pos-

[8] Cfr. A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, 2012, fasc. 1, 135-144; G. SARTOR, M. VIOLA DE AZEVEDO CUNHA, *Il caso Google e i rapporti regolatori USA/EU*, in *Il diritto dell'informazione e dell'informatica*, 2014, fasc. 4-5, 657-680.

[9] Cfr. M. OREFICE, *I big data. Regole e concorrenza*, in *Politica del diritto*, 2016, fasc. 4, 703.

[10] D. CARDON, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei* big data, Milano, 2016, 5.

[11] Cfr. V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten legal perspectives on the "Big data revolution"*, in *Concorrenza e mercato*, 2016, 49 ss.

[12] Cfr. V. MAYER-SCHÖNBERGER, K. CUKIER, *op. cit.*, 73 ss.

[13] Cfr., *inter alia*, D. DE PASQUALE, *La linea sottile tra manipolazione della rete e pubblicità*, in *Il Diritto industriale*, 2012, fasc. 6, 552 ss.; A. MANTELERO, *op. cit.*, 138-139.

sono usare quei dati per svariate funzioni e scopi che caratterizzano l'*agere* pubblico, quali le funzioni di controllo, come la rilevazione di irregolarità amministrative, ad esempio quelle fiscali, e le funzioni di regolazione, per conoscere i fenomeni, monitorarli e valutare l'impatto di eventuali scelte.
Pertanto, le soluzioni di intelligenza artificiale in ambito pubblico possono incidere significativamente sull'attività conoscitiva delle amministrazioni, permettendo di "oggettivarla", di rafforzare la capacità istruttoria e, di conseguenza, verosimilmente quella decisoria[14].
A tali funzioni, l'intelligenza artificiale affianca una finalità di particolare rilevanza nel contesto pubblico, ossia la possibilità di essere proficuamente impiegata nell'erogazione di servizi, garantendo maggiore efficacia ed efficienza, consentendo risparmi in termini finanziari e umani, sostituendo l'uomo in alcuni compiti e funzioni, e garantendo, altresì, maggiore tempestività all'azione pubblica.
In modo esemplificativo le soluzioni di intelligenza artificiale utilizzate dalle amministrazioni pubbliche possono contribuire a rendere *smart* i territori, migliorando la qualità di vita della collettività di riferimento.
Le tecnologie di intelligenza artificiale sono, pertanto, idonee a raggiungere in modo più efficiente gli obiettivi che guidano l'azione amministrativa, delineati come caratterizzanti anche dalla normativa di riferimento in materia di amministrazione digitale.
Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività sono, infatti, tenute a utilizzare le tecnologie informatiche e, quindi, anche l'intelligenza artificiale per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese[15]. L'art. 97 della Costituzione permette di leggere la digitalizzazione e l'impiego di soluzioni innovative da parte delle amministrazioni quale strumento per assicurare il buon andamento delle stesse, possibile solo nel perseguimento degli obiettivi tipici dell'azione pubblica.

2. Profili di *governance*

In considerazione del fatto che l'anima dell'intelligenza artificiale risiede nei dati, di conseguenza un profilo di significativo interesse attiene alla *governance* degli stessi: in ambito pubblico, infatti, diverse istituzioni si occupano di dati.

[14] Cfr. M. FALCONE, *Big data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Rivista Trimestrale di Diritto Pubblico*, fasc. 3, 2017, 601-639. In merito F. COSTANTINO, *Lampi. Nuove frontiere delle decisioni amministrative tra* open *e* big data, in *Diritto amministrativo*, fasc. 4, 2017, 799 ss. riporta la formula enfatica secondo cui «le tecnologie trasformano i dati in informazioni, e in tal modo attuano il passaggio dall'informazione alla "conoscenza dei fenomeni" e degli "andamenti", fino alle cd. nuove forme di governo abilitate dai dati (*government by data*). Così gli algoritmi utilizzati per elaborare i dati individuano relazioni utili per supportare le decisioni, in quanto basate su modelli previsionali. […] Si configura l'idea di un'amministrazione che prevede e anticipa, che adotta un *modus operandi* fondato non più sulla risposta a stimoli ma sull'anticipazione di bisogni e problemi, sulla pianificazione strategica, al fine di evitare perdite e gestire i rischi». L'Autore evidenzia l'impatto dei *big data* in ambito pubblico: seguire le predizioni esonererebbe da responsabilità l'amministrazione e, allo stesso modo, in caso di mancato adeguamento l'amministrazione andrebbe incontro a responsabilità.
[15] Art. 12, comma 1, d.lgs. 82/2005.

L'Agenzia per l'Italia Digitale (di seguito anche AgID) ontologicamente ha un ruolo centrale, dal momento che le sono attribuite funzioni strategiche e tecniche al fine di "traghettare" e accompagnare le amministrazioni verso la digitalizzazione, assicurando la corretta attuazione delle norme. Ad AgID, preposta alla realizzazione degli obiettivi dell'Agenda digitale italiana e alla promozione dell'innovazione digitale nel Paese, sono attribuite funzioni di programmazione, coordinamento e monitoraggio, l'emanazione di linee guida recanti regole e standard, la vigilanza e il controllo sull'attuazione e sul rispetto delle norme, la realizzazione di progetti e lo svolgimento di compiti di natura tecnica[16]. Risultano particolarmente rilevanti sotto il profilo dei dati, le strategie e le linee guida in materia[17].

In considerazione dei compiti attribuiti dalla normativa di riferimento, non a caso proprio AgID ha promosso con la Presidenza del Consiglio dei ministri una Task Force sull'intelligenza artificiale, formata da un coordinamento di 30 profili multidisciplinari e da una *community*, con il compito di analizzare le modalità di utilizzo dell'intelligenza artificiale nell'evoluzione dei servizi pubblici per migliorare il rapporto tra pubblica amministrazione e cittadini[18]. La Task Force, i cui lavori sono stati avviati nel settembre 2017, ha elaborato un Libro bianco sull'intelligenza artificiale al servizio del cittadino, pubblicato nel marzo 2018, dedicato ad esaminare gli ambiti di applicazione, le potenzialità e le opportunità dell'intelligenza artificiale nella pubblica amministrazione; il Libro bianco si compone di sfide e di raccomandazioni rivolte al Governo e alle amministrazioni pubbliche[19].

Nella *governance* relativa ai dati, agli algoritmi e all'intelligenza artificiale, accanto ad AgID rilevano anche due autorità amministrative.

Il Garante per la protezione dei dati personali, autorità di controllo italiana in materia di *data protection*, si occupa precipuamente di una tipologia di dati, i dati personali, ma, più ampiamente, ha altresì assunto significativo rilievo grazie a provvedimenti, linee guida, indicazioni nella gestione dei dati *tout court* parallelamente all'ampio raggio d'azione del regolamento europeo 2016/679, che si occupa non solo di *data protection*, ma anche di *data governance*.

E, ancora, ANAC ha un ruolo significativo in materia, perché quando si parla di trasparenza e accesso necessariamente si parla anche di dati. A tale proposito sono particolarmente significative le linee guida adottate da quest'ultima con delibera n. 1309 del 28 dicembre 2016, recanti indicazioni operative tese alla definizione delle esclusioni e dei limiti all'accesso civico.

La tematica quindi è trasversale a differenti tipologie di dati (la varietà, del resto, è caratteristica ontologica dei *big data*) e, parallelamente, a diversi enti indipendenti che entrano in gioco nella *governance* dei dati stessi: non è da escludere l'opportunità di costituire un coordinamento tra i diversi soggetti per un governo efficace dei dati, degli algoritmi e dell'intelligenza artificiale, per fornire le regole di una corretta gestione e monitorarne l'osservanza.

[16] Artt. 14, comma 2, e 14-bis, d.lgs. 82/2005.

[17] Si pensi alle linee guida per la valorizzazione del patrimonio informativo pubblico, prodotte da AgID.

[18] Cfr. *ia.italia.it.*

[19] Il Libro bianco è disponibile al link https://ia.italia.it/assets/librobianco.pdf ; la prima versione è stata messa in consultazione tra febbraio e marzo 2018; cfr. https://libro-bianco-ia.readthedocs.io/it/latest/.

Di conseguenza la gestione di soluzioni di intelligenza artificiale in ambito pubblico pone in primo luogo la necessità di rispettare la normativa di riferimento e, altresì, a livello di *governance*, le indicazioni delle diverse autorità coinvolte.

3. Le sfide giuridiche in ambito pubblico

In considerazione delle esaminate caratteristiche di dati e algoritmi, l'utilizzo di soluzioni di intelligenza artificiale in ambito pubblico deve essere attentamente valutato e deve fare i conti con gli elementi di incertezza e con la natura inferenziale e probabilistica delle elaborazioni compiute dagli algoritmi stessi, profili ancora più problematici nel contesto pubblico che ontologicamente deve garantire certezza del diritto e validità giuridica dell'attività amministrativa espletata nello svolgimento delle funzioni, oltre ad assicurare la trasparenza delle fasi del procedimento e la qualità dei dati.
La logica attenta alla quantità e alle correlazioni, infatti, rischia di mettere in crisi la disciplina sulla qualità dei dati pubblici, necessaria per garantire certezza e assicurare affidabilità e fiducia[20]. Le istituzioni devono valutare se le soluzioni di intelligenza artificiale conducano a una verità oggettiva e materiale, che rafforza la certezza dell'agire pubblico e rende ottimali le decisioni prese, o rischi di incrinarla in modo preoccupante[21].
Sicuramente i soggetti pubblici, in quanto retti dal principio di legalità amministrativa, devono attenersi scrupolosamente alla normativa in materia, composta da un insieme di norme afferenti al procedimento amministrativo, all'amministrazione digitale e alla normativa sulla trasparenza, alle quali si sommano le disposizioni da osservare a tutela dei diritti, in particolare in materia di proprietà intellettuale e di protezione dei dati personali.
Sotto tale profilo, il Codice dell'amministrazione digitale (d.lgs. 82/2005) e gli altri atti di riferimento contengono norme in materia di dati pubblici che riguardano i principi di disponibilità, fruibilità e di messa a disposizione dei dati e si spingono fino alle strategie di apertura che si sostanziano nella disciplina degli *open data*. Tali norme devono trovare rispetto anche laddove l'amministrazione decida di servirsi di tecnologie di intelligenza artificiale nello svolgimento delle funzioni e nell'erogazione dei servizi. Al riguardo, più ampiamente, come sarà precisato più avanti, le tecnologie di intelligenza artificiale devono basarsi sul principio di trasparenza e apertura non solo dei dati, ma anche della logica degli algoritmi che li "animano" e del processo di funzionamento del servizio.
Un aspetto cui porre particolare attenzione emerge proprio riguardo ai soggetti della relazione: da una parte ci sono amministrazioni pubbliche, dall'altra parte gli utenti di servizi pubblici. Ciò implica il rispetto della normativa inerente i procedimenti amministrativi e l'amministrazione digitale:

[20] Cfr. M. FALCONE, *op. cit.*, 601 ss.

[21] Cfr. M. FALCONE, *op. cit.*, 601 ss., che evidenzia come le amministrazioni abbiano ancora difficoltà a raccogliere e conservare i dati e utilizzarli in modo organizzato. Come rileva l'Autore, peraltro, il principio di verità materiale incontra limiti in alcuni principi del procedimento amministrativo, come il principio di economicità e non aggravamento e negli istituti di semplificazione o di certificazione. Al riguardo F. COSTANTINO, *op. cit.*, 799 ss. riporta i possibili vizi di un'attività "informatizzata", quali eccesso di potere per illogicità o irrazionalità manifesta (se la soluzione automatizzata non è ragionevole), illegittimità del provvedimento per malfunzionamento della macchina o difetto del software (illegittimità derivata), illegittimità per presupposti erronei (in caso di immissione errata di dati), illegittimità per vizi attinenti alla motivazione (che può essere difficile da fornire se la decisione deriva dall'elaborazione di *big data*).

l'implementazione di applicazioni di intelligenza artificiale deve rispettare, di conseguenza, da una parte, i diritti (anche digitali) dei cittadini e, dall'altra, gli obblighi propri delle amministrazioni e, pur con i necessari adattamenti, le garanzie procedimentali. Questo comporta che debba essere assicurato e regolato l'accesso ai dati, in considerazione della relativa normativa nazionale e tenendo conto delle peculiarità delle soluzioni concrete[22]. Sotto tali profili, come evidenziato dal Libro Bianco promosso da AgID, emerge l'esigenza di trovare metodi uniformi e compatibili con l'attuale ordinamento per consentire all'amministrazione pubblica di motivare i suoi provvedimenti anche nella parte elaborata dai sistemi di intelligenza artificiale.

Una gestione corretta dei dati, anima delle soluzioni di intelligenza artificiale, pertanto, deve rispettare i diversi diritti in gioco e, per farlo, deve osservare le prescrizioni normative di riferimento in materia di procedimento amministrativo, amministrazione digitale, trasparenza, proprietà intellettuale e protezione dei dati personali. A tali fini, il sistema deve essere necessariamente trasparente per l'utente, da garantire nel proprio diritto all'autodeterminazione informativa e da valorizzare nel proprio ruolo.

In tutto il processo, infatti, deve essere protagonista l'utente, il cui soddisfacimento è l'obiettivo da non perdere di vista quando si agisce in ambito pubblico. La qualità dei servizi online, che devono essere semplici e integrati, e la correlata misura della soddisfazione rientrano esplicitamente, del resto, tra i diritti che il Codice dell'amministrazione digitale riconosce e tutela (art. 7, d.lgs. 82/2005); di conseguenza anche i servizi basati su tecnologie di intelligenza artificiale devono essere integrati con un *feedback* costante da parte di chi ne fruisce.

Al fine di garantire il corretto rispetto delle norme di riferimento, di conseguenza è necessario assicurare l'*accountability* e la correlata definizione delle diverse responsabilità, anche per mantenere fiducia da parte della collettività nell'azione pubblica. A tali fini è essenziale la presenza di *policy* specifiche di accompagnamento da parte delle amministrazioni, cui le stesse devono attenersi, trasparenti per l'utente e per mezzo delle quali venga regolata e garantita non solo la qualità e la corretta gestione, ma anche l'aspetto di sicurezza a livello tecnologico, umano e organizzativo, con una definizione chiara delle responsabilità.

La regolazione presuppone delle valutazioni di ordine politico, strategico e giuridico. Bisogna partire dal presupposto, infatti, che raccogliere e gestire numerosi dati conferisce, necessariamente, un correlato enorme potere, ancora più evidente laddove si tratti di un soggetto pubblico. Proprio qui emerge un aspetto cruciale.

Il possesso dei dati relativi alle soluzioni di intelligenza artificiale, se non viene attentamente presidiato, può provocare una conseguente asimmetria di potere informativo e una forbice tra istituzioni e soggetti, cittadini o imprese, che può generare una conseguente perdita di fiducia. A tale profilo si somma un ulteriore e potenziale rischio collegato al controllo sociale: i soggetti pubblici potrebbero decidere di servirsi dei dati prodotti e gestiti dalle soluzioni di intelligenza artificiale per finalità ulteriori rispetto ai servizi per i quali sono impiegati; ciò permetterebbe fenomeni di monitoraggio della collettività, soprattutto laddove l'operazione avvenga in modo non trasparente per gli utenti. Tutto questo, naturalmente, rischierebbe di entrare in frizione con la normativa e di allontanare governanti

[22] Rilevano sotto tali profili le disposizioni contenute nella legge 241/1990, nel d.lgs. 82/2005 e nel d.lgs. 33/2013.

e governati in direzione opposta all'*open government* che anima le riforme più recenti e le strategie nazionali in materia di digitalizzazione[23].

Di conseguenza, emerge la necessità di bilanciare il valore e le opportunità offerte con le questioni etiche e sociali che si profilano.

Le soluzioni di intelligenza artificiale e la mole di dati gestiti per garantirne l'efficace funzionamento, infatti, producono una conseguente contrapposizione significativa tra i "signori dei dati"[24] e tutti gli altri. Gli Stati conoscono ingenti quantità di dati necessari per svolgere le funzioni pubbliche e, a loro volta, i colossi tecnologici come Google, Amazon, Facebook conoscono le nostre attività digitali, le nostre relazioni sociali, i nostri sentimenti.

Al fine di rendere maggiormente efficienti le soluzioni di intelligenza artificiale impiegate, i soggetti pubblici potrebbero decidere di avvalersi tramite rapporti negoziali, anche in connessione con i propri dati, delle grandi banche dati dei privati, che detengono informazioni acquisite su base contrattuale. In tal modo possono realizzarsi forme di sorveglianza e di controllo, influenzando la collettività e mettendo in pericolo le libertà.

Peraltro, in ambito pubblico, i dati sono forniti da soggetti interessati alla fruizione del servizio, per lo più inconsapevoli e, in ogni caso, imprigionati in una relazione sicuramente non simmetrica[25].

Il rischio è già diventato reale in materia di dati e potrebbe aggravarsi con un impiego esteso di soluzioni di intelligenza artificiale. Al riguardo merita ricordare il *Datagate*, che ha fatto emergere, grazie alle dichiarazioni di Edward Snowden, i rapporti tra le agenzie di *intelligence* statunitensi e i colossi tecnologici, che hanno dato vita a una sorveglianza di massa sui dati personali di cittadini di tutto il mondo[26] o il caso *Facebook - Cambridge Analytica*, che a seguito delle rivelazioni di Christopher Wylie, ha fatto emergere uno spregiudicato utilizzo di svariati dati personali per influenzare il voto e le elezioni negli Stati Uniti[27].

Nell'utilizzo di tali soluzioni si affaccia il rischio concreto che aziende e governi possano impiegare in vario modo la conoscenza del presente e le previsioni del futuro, anche per finalità diverse da quelle originarie con potenziali effetti discriminatori (es. ambito assicurativo, contesto lavorativo, prevenzione della criminalità).

Accanto a queste problematiche giuridiche collegate all'ambito pubblico e alle relative implicazioni etico-sociali degne di grande attenzione, sotto la lente giuridica sono svariati gli ulteriori profili critici.

---

[23] L'*open government* è il modello secondo cui le amministrazioni devono essere capaci di essere trasparenti a tutti i livelli e di rendere le proprie attività aperte e disponibili per favorire azioni maggiormente efficaci, rispondere alle istanze della società e garantire il controllo pubblico del proprio operato mediante le nuove tecnologie.

[24] A. MANTELERO, *op. cit.*, 135.

[25] M.F. DE TULLIO, *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Politica del diritto*, 2016, fasc. 4, 671 ss.

[26] Al riguardo cfr. G. GREENWALD, *Sotto controllo. Edward Snowden e la sorveglianza di massa*, trad. it., Milano, 2014.

[27] I dati personali sono stati forniti dagli utenti durante l'utilizzo di una *app* cui era possibile accedere tramite Facebook, che raccoglieva i dati dal *social* a fini di ricerca. L'azienda Cambridge Analytica ne è venuta in possesso per mezzo di accordi con il titolare e pare aver utilizzato i dati acquisiti con la finalità di influenzare e manipolare il voto nella campagna Brexit e nelle elezioni presidenziali che hanno portato alla vittoria di Trump, grazie alla conoscenza che i dati stessi consentivano dei soggetti inconsapevolmente coinvolti.

Un aspetto problematico si collega strettamente alle caratteristiche tecniche di funzionamento dell'intelligenza artificiale: l'analisi dei dati consiste in un processo di approssimazione, che genera il rischio di trarre conclusioni imprecise e discriminatorie. Affinché la quantità dei dati si traduca in conoscenza e sia funzionale allo scopo per cui la soluzione di intelligenza artificiale è predisposta, è necessario avvalersi di dati di qualità, tempestivi ed accurati, evitando errori, *bias* ed utilizzi impropri o manipolatori[28].

In merito alla possibilità di errori e *bias* involontari, si pensi al caso di Amazon: il colosso tecnologico ha scoperto che il sistema di intelligenza artificiale adottato per selezionare le candidature non si comportava in modo neutrale, ma escludeva le candidature delle donne; il sistema, infatti, aveva "imparato" dalle candidature passate, in larga parte di uomini, a "preferire" gli uomini alle donne[29]. I rischi in ambito pubblico sono intuitivamente peggiori e, per tale motivo, anche sotto tale profilo l'assenza di una regolamentazione esplicita dei fenomeni da parte della normativa implica la necessità della definizione degli obiettivi e dell'emanazione di *policy* di accompagnamento.

Un altro profilo di criticità dal punto di vista giuridico afferisce alla "proprietà" dei dati gestiti, soprattutto se si sceglie di avvalersi anche di soggetti esterni nell'implementazione e gestione di tali servizi. Anche da questo punto di vista interviene la normativa, in specifico quella sul diritto d'autore e sui diritti connessi, che protegge non solo le informazioni strutturate, ma anche le raccolte di dati, in genere ascritte, a seconda dei casi, a banche dati creative o non creative, facendo scattare parallelamente la tutela del diritto d'autore o del diritto *sui generis*: la filiera dei soggetti che intervengono in queste soluzioni è fondamentale per l'attribuzione dei correlati diritti e delle prerogative che li accompagnano.

In concreto, le raccolte di dati sui quali si basano queste soluzioni possono essere ricondotte a banche dati "non creative", attivando così la tutela del diritto *sui generis*, meno intensa del diritto d'autore e tale da far sopravvivere il diritto d'autore sulle informazioni strutturate e i *dataset* che compongono la banca dati stessa[30]. Talvolta, ritenendo che il valore economico non sia nei dati, ma nelle elaborazioni, nei calcoli e negli algoritmi, la tutela giuridica può essere spostata dalla proprietà dei dati al software, parimenti protetto dalla normativa sulla proprietà intellettuale, o al contratto di fornitura di servizi. Sotto tale profilo viene in gioco anche l'autonomia contrattuale cui si può ricorrere per tutelare più efficacemente tali soluzioni, per regolarne la cessione o la concessione di diritti, individuando i profili di responsabilità reciproca[31].

La questione è particolarmente complessa nel caso dell'intelligenza artificiale, dal momento che non sempre si tratta di un singolo bene immateriale, ma di un processo che spesso vede titolarità diverse (il titolare dello strumento può essere diverso dal titolare del servizio) e pone connessi problemi di

[28] A. MANTELERO, *op. cit.*, 135 ss.; G. COLANGELO, *Big data, piattaforme e antitrust*, in *Mercato Concorrenza Regole*, fasc. 3, 2016, 428 ss. Al riguardo C. ACCOTO, *Il mondo dato. Cinque brevi riflessioni di filosofia digitale*, Milano, 2017, 67 ss. sottolinea che *bias* algoritmici, capaci di dar luogo a discriminazioni, possono dipendere dalle banche dati utilizzate o dagli attributi scelti per le correlazioni, senza che ci sia uno scopo discriminatorio nelle intenzioni degli utilizzatori.

[29] Il team ha lavorato a tale progetto tra il 2014 e il 2017; il progetto è stato chiuso da Amazon nel 2017. Cfr. *www.corrierecomunicazioni.it/over-the-top/allintelligenza-artificiale-di-amazon-non-piacciono-le-donne-scartati-i-cv-femminili* (consultato il 10 gennaio 2018).

[30] M. FALCONE, *op*. cit., 601-639.

[31] V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *op. cit.*, 30 ss.

responsabilità. Sotto tale profilo le questioni di responsabilità giuridica diventano particolarmente ostiche, dal momento che, a seconda del caso concreto, può cambiare la partecipazione umana all'azione e alla decisione che conduce a eventuali danni ed è complessa la conseguente imputazione delle responsabilità. Si pongono, inoltre, inediti interrogativi relativi all'eventuale attribuzione di soggettività e relativa personalità giuridica alle applicazioni di intelligenza artificiale, che comporterebbe il potenziale riconoscimento di una serie di diritti e doveri, l'attribuzione di responsabilità e le connesse problematiche; si pensi in materia di diritto d'autore e brevetti alla qualificazione giuridica e alla disciplina delle creazioni autonome e delle invenzioni da parte di tali applicazioni[32].

Infine, profili particolarmente problematici sotto il profilo giuridico si individuano nella relazione con la normativa in materia di protezione dei dati personali, cui è dedicato il successivo paragrafo. Al riguardo, peraltro, è opportuno precisare che anche in presenza di dati non personali il problema non è completamente superato: il *data mining* e le analisi tecniche sono capaci di produrre fenomeni di re-identificazione e de-anonimizzazione, che consentono di rivelare l'identità di una persona o di piccoli gruppi e i comportamenti collegati, proponendo nuovamente le esigenze di tutela della normativa in materia di *data protection*[33].

4. *Data protection* e intelligenza artificiale

Il regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, è teso a rendere omogenea la tutela della persona nei diversi Stati e a rafforzarne l'effettività insieme alla correlata fiducia da parte della collettività.

L'approccio e gli strumenti che caratterizzano il regolamento (UE) 2016/679, pertanto, sono tesi ad una protezione effettiva ed efficace dell'individuo. Ma le caratteristiche che connotano l'intelligenza artificiale e i suoi elementi fondanti (dati e algoritmi) mostrano criticità ontologiche nel rispetto della disciplina in materia di *data protection*: in particolare, rischiano di scontrarsi apertamente con alcuni principi fondamentali della normativa, tesi a garantire il rispetto della persona e della sua libertà di autodeterminazione.

Come esaminato, l'intelligenza artificiale si basa su elaborazioni e inferenze capaci di condurre a risultati diversi e talvolta anche inaspettati, attraverso processi di natura deterministica distanti dal tipico ragionamento umano: soprattutto laddove impiegata per aumentare la conoscenza del presente e del futuro e supportare le decisioni, per dare risultati di particolare interesse l'intelligenza artificiale deve avere a disposizione un enorme mole di dati e basarsi su efficienti algoritmi che operano in modo distante dai processi basati su ipotesi determinate e nesso causale[34]. Di conseguenza può risultare complesso il rispetto del principio di limitazione della finalità, che prevede la raccolta dei dati personali per finalità determinate, esplicite e legittime e il successivo trattamento in modo che non sia in-

[32]Cfr. C. TREVISI, *La regolamentazione in materia di Intelligenza artificiale, robot, automazione: a che punto siamo*, in *Rivista di diritto dei media*, fasc. 2, 2018, pp. 447-458.

[33] V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *op. cit.*, 33 ss.; V. MAYER-SCHÖNBERGER, K. CUKIER, *op. cit.*, 73 ss.

[34] Cfr. A. MANTELERO, *op. cit.*, 135-144; V. MAYER-SCHÖNBERGER, K. CUKIER, *op. cit.*, 42; G. SARTOR, M. VIOLA DE AZEVEDO CUNHA, *op. cit.*, 657-680.

ISSN 2284-4503

compatibile con tali finalità[35]. Il volume dei dati, la varietà delle fonti e il modo di operare degli algoritmi rendono, inoltre, difficile il rispetto del criterio di minimizzazione dei dati e dei relativi principi di adeguatezza, pertinenza e limitazione dei dati personali a quanto necessario rispetto alle finalità del trattamento[36] e, allo stesso modo, rischiano di inficiare la qualità, l'esattezza e l'accuratezza dei dati[37].

I principi di limitazione della finalità, di esattezza e di minimizzazione dei dati rischiano quindi di essere depotenziati in un contesto dominato dagli algoritmi, a causa delle criticità esaminate.

Accanto al difficile rispetto di alcuni principi cardine del regolamento, nelle caratteristiche stesse di funzionamento dell'intelligenza artificiale emergono criticità profonde che rischiano di minare i fondamenti stessi della disciplina europea.

La rilevanza attribuita dalla normativa alle tecniche di anonimizzazione, che permettono di non applicare la disciplina, può risultare problematica, dal momento che il rischio si annida nelle inferenze che possono essere tratte su gruppi o individui da dati anonimi, grazie anche alla disponibilità di dati ausiliari riferibili alla persona: semplificando, ogni dato può finire per essere identificativo e quindi personale, esigendo come tale l'applicazione della relativa disciplina[38].

Del resto anche il concetto di "dato personale" può risultare insufficiente, dal momento che, oltre ai dati anonimi, che non è detto restino tali, ci possono essere dati afferenti a gruppi o comunità, che appartengono cioè a più persone, oltre ai metadati, estremamente significativi[39].

Il mondo degli algoritmi fa vacillare anche il paradigma basato sull'informativa e consenso; in specifico, è dubbio che in tale contesto le informazioni rese siano capaci davvero di informare in modo completo ed efficace e che il consenso possa considerarsi libero[40]. A tale proposito merita precisare che i soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, dal momento che in tal caso la liceità del trattamento deriva dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui all'art. 6, paragrafo 1, lett. e), reg. (UE) 2016/679 e, inoltre, in tale fattispecie esiste un evidente squilibrio tra le parti che inevitabilmente rischia di inficiare la necessaria libertà di espressione del consenso[41].

Ai fini di questa analisi rileva particolarmente la disposizione dedicata al «processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione», di cui all'art. 22 del regolamento (UE) 2016/679: «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»; la profilazione viene peraltro esplicitamente definita nell'art. 4, paragrafo 1, n. 4) del regolamento europeo. Il paragrafo 2 della disposizione riduce la portata della norma, che non si applica al verificarsi di alcune condizioni,

[35] Art. 5, paragrafo 1, lett. b), reg. (UE) 2016/679.
[36] Art. 5, paragrafo 1, lett. c), reg. (UE) 2016/679.
[37] Art. 5, paragrafo 1, lett. d), reg. (UE) 2016/679.
[38] Cfr. G. D'Acquisto, M. Naldi, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017, 34 ss.; V. Zeno-Zencovich, G. Giannone Codiglione, *op. cit.*, 33 ss.
[39] Cfr. C. Focarelli, *La privacy. Proteggere i dati personali oggi*, Bologna, 2015, 28 ss.
[40] Artt. 7, 12-14, reg. (UE) 2016/679. Cfr. F.H. Cate, V. Mayer-Schönberger, *Notice and consent in a world of Big Data*, in *International Data Privacy Law*, 2013, vol. 3, n. 2, 67-73.
[41] Al riguardo cfr. considerando 43 del reg. (UE) 2016/679.

in particolare «nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato».
Nel caso del consenso esplicito e in quello di necessità per la conclusione o l'esecuzione del contratto, il titolare del trattamento è comunque tenuto ad attuare «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» (art. 22, paragrafo 3, regolamento europeo 2016/679).

5. Principi e strumenti da valorizzare

A ben vedere, le criticità esaminate trovano condiviso fondamento nell'opacità e nella chiusura dei processi di gestione dei dati e degli algoritmi, nel significativo squilibrio tra le parti e nella conseguente inevitabile incapacità per il singolo di potersi tutelare.
In tale contesto è fondamentale il ruolo giocato dall'uomo e dal diritto per riuscire a governare l'intelligenza artificiale, proteggendo la dignità, lo sviluppo della persona e le sue libertà.
Pertanto, per affrontare le soluzioni di intelligenza artificiale in modo efficace in ambito pubblico, è opportuno valorizzare e dare applicazione ad alcuni principi che si pongono quale possibile rimedio a tali problematiche e che possono essere sintetizzati nei seguenti (oggetto di esame dei prossimi paragrafi): tecnica, etica, *accountability*, trasparenza e apertura.

5.1. Tecnica, etica e *accountability*

Seppur, come già esaminato, non manchino criticità nella normativa europea, alle soluzioni di intelligenza artificiale si attagliano alcuni principi innovativi della disciplina recata dal regolamento europeo 2016/679, che mirano a un approccio proattivo e a una ponderazione preventiva dell'impatto e dei rischi sulla *data protection*[42].
In particolare si tratta degli strumenti della *privacy by design* e *by default*, cui si affianca il *Data Protection Impact Assessment*, nei quali il diritto si avvale della tecnologia per assicurare il suo rispetto e garantire la tutela della dignità e dello sviluppo della persona: la tecnologia si pone quale "antidoto" preventivo a possibili violazioni delle norme, tutelando la persona fin dalla progettazione, per impostazione preventiva e per mezzo della valutazione d'impatto[43].
Il principio *privacy by design*, di cui all'art. 25, paragrafo 1 del regolamento (UE) 2016/679, prevede che, 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, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare debba mettere in

[42] Cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove leggi civili commentate*, 2017, fasc. 1, 1-18.
[43] Cfr. C. FOCARELLI, *op. cit.*, 63; A. MANTELERO, *op. cit.*, 159 ss.

ISSN 2284-4503

atto «*misure tecniche e organizzative adeguate, quali la pseudonimizzazione*» (di cui all'art. 4, comma 1, n. 5), «*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 soddisfare i requisiti del regolamento e tutelare i diritti degli interessati*».

A tale criterio si lega il principio *privacy by default*, posto nel secondo paragrafo dell'art. 25 del regolamento (UE) 2016/679: il titolare deve mettere in atto «misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento». L'individuo è tutelato in modo rafforzato dal momento che la disposizione impedisce l'accesso a un numero indefinito di persone fisiche da parte di macchine (senza l'intervento della persona fisica) e prevede che l'obbligo sia calibrato su aspetti quali la quantità di dati, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Interessante, altresì, l'art. 35 del reg. (UE) 2016/679, relativo al c.d. *Data Protection Impact Assessment*: quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare effettua, prima di procedere al trattamento, «una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali». Tale valutazione deve contenere almeno i requisiti prescritti dalla norma ed è prevista nelle ipotesi poste dalla normativa, quali trattamenti automatizzati, come le operazioni di profilazione degli utenti, che permettono una valutazione sistematica e globale di aspetti personali relativi a persone fisiche e fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; trattamenti su larga scala di particolari categorie di dati o di dati relativi a condanne penali e a reati; sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Sotto il profilo della gestione dei *big data* risultano interessanti anche altre novità del regolamento (UE) 2016/679, come la consultazione preventiva (art. 36)[44], la *data breach notification* (artt. 33-34)[45] e il *Data Protection Officer* (DPO) o Responsabile della protezione dei dati (RPD) (artt. 37-39); la nomina di questa figura è prevista con la funzione di garantire una corretta gestione dei dati in una serie di casi, tra i quali proprio l'ambito pubblico.

In linea con l'approccio proattivo e preventivo di tutela si pone la logica di *accountability* e responsabilizzazione dei soggetti che trattano i dati personali[46] e la contitolarità, accompagnata dalla definizione delle rispettive responsabilità[47], disposizioni coadiuvate sia dall'attenzione alla sicurezza[48], sia dall'effettività e dall'efficacia del sistema sanzionatorio correlato[49]. Nell'applicazione della disciplina e nella promozione della consapevolezza al riguardo, un ruolo strategico è svolto in concreto dalle au-

[44] Il titolare, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio.

[45] Le norme impongono al titolare l'obbligo di notificare eventuali violazioni dei dati personali all'autorità nazionale nei tempi e nelle modalità previste. Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare comunica la violazione all'interessato senza ingiustificato ritardo.

[46] Art. 24, reg. (UE) 2016/679.

[47] Art. 26, reg. (UE) 2016/679.

[48] Art. 32, reg. (UE) 2016/679.

[49] Artt. 82-84, reg. (UE) 2016/679.

torità di controllo indipendenti (nel caso italiano il Garante per la protezione dei dati personali)[50]. Nelle attività e nei poteri conferiti, come già rilevato, infatti, l'autorità di controllo assume una strategica e incisiva funzione che dalla *data protection* più ampiamente si estende a una vera e propria *data governance*.

5.2. Trasparenza algoritmica

In ambito pubblico tra i valori che guidano l'azione amministrativa si pone indubbiamente il principio di trasparenza, che ha vissuto un'espansione negli ultimi anni grazie alla riforma del d.lgs. 33/2013 da parte del d.lgs. 97/2016, che ha dato forma e sostanza alla libertà di informazione nei confronti delle istituzioni. Il principio di trasparenza, insieme a partecipazione e collaborazione, è uno dei pilastri fondanti di un'amministrazione pubblica digitale e aperta, come emerge dalla normativa di riferimento.

Alla luce di tali principi che informano l'azione pubblica e per contrastare l'opacità che rischia di caratterizzare le soluzioni di intelligenza artificiale, le amministrazioni pubbliche che decidano di avvalersi di tali soluzioni devono affidarsi a una trasparenza sostanziale nei confronti degli interessati e, parallelamente, consentire la conoscenza da parte dell'interessato della logica degli algoritmi, accompagnata dalla consapevolezza in merito alle conseguenze e all'impatto sulla persona.

Ciò è necessario anche ai fini di una consapevole autodeterminazione degli individui, dando vita a una sorta di "dovere di lealtà" nei confronti degli utenti, capace di superare l'opacità di potenziali *black box* e diminuire la congenita "asimmetria algoritmica" che le caratterizza[51].

Sotto tale profilo risulta significativo quanto previsto dagli art. 13, paragrafo 2, lett. f) e art. 14, paragrafo 2, lett. g) del regolamento (UE) 2016/679. Il titolare del trattamento è tenuto, infatti, a fornire all'interessato, tra le informazioni necessarie per garantire un trattamento corretto e trasparente, «l'esistenza di un processo decisionale automatizzato, compresa la profilazione […] e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato».

Le soluzioni di intelligenza artificiale si avvalgono di processi decisionali automatizzati; in tale contesto, pertanto, la norma si traduce nella necessità di fornire informazioni sulla logica utilizzata dagli algoritmi, ma anche sull'impatto e sulle conseguenze per l'interessato. In tal modo è possibile riequilibrare l'asimmetria tra le parti, imponendo maggiore trasparenza in merito alla logica utilizzata dagli algoritmi stessi, al fine di garantire la consapevole autodeterminazione e la correlata libertà degli individui, valori protetti dalla disciplina e, più ampiamente, dagli ordinamenti democratici.

[50] Artt. 51-59, reg. (UE) 2016/679.

[51] C. ACCOTO, *op. cit.*, 66 ss.: «Codice e algoritmo sono accomunati da una peculiarità. Come per il software anche per gli algoritmi torna rilevante la questione dell'invisibilità (si parla esplicitamente di *black box society*). Invisibilità che impedirebbe la comprensione della loro natura e, in caso di discriminazione o manipolazione, una loro eventuale rimozione o mitigazione». Secondo l'Autore «si va verso la presa di consapevolezza della necessità di un'accountability e di un auditing degli algoritmi (cioè di una conoscenza responsabile, condivisa e più trasparente)» (p. 67). L. BOLOGNINI, *Follia artificiale. Riflessioni per la resistenza dell'intelligenza umana*, Soveria Mannelli, 2018, 47 sottolinea l'importanza di avere «regole chiare che impongano trasparenza e contestabilità degli algoritmi utilizzati in ambito pubblico per trattare dati personali e/o per prendere decisioni con impatti significativi sulle persone». D. CARDON, *op. cit.*, 68 ss. parla di «nuova rivendicazione di un *dovere di lealtà* delle piattaforme nei confronti dei loro utenti» (p. 69).

In merito, anche la 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» evidenzia l'importanza della responsabilità e della trasparenza a livello degli algoritmi, che «dovrebbero riflettere l'applicazione di misure tecniche e operative che assicurino la trasparenza, la non discriminazione del processo decisionale automatizzato e il calcolo delle probabilità del singolo comportamento»[52].

Pertanto, al fine di tutelare i diritti e le libertà della persona, i soggetti pubblici devono coniugare la *data governance* con il governo degli algoritmi, capaci di dare vita e rendere dinamici i dati stessi, estraendone conoscenza e valore, per rispondere alle legittime istanze di conoscenza e di protezione dei diritti da parte degli utenti, garantendo la consapevole autodeterminazione e il controllo, assicurando un'autentica libertà degli individui[53]. Si tratta, di conseguenza, di garantire una «trasparenza algoritmica», che impone al titolare il dovere di governare l'algoritmo e le strutture logiche del suo funzionamento per far fronte alle richieste avanzate dagli utenti in forza del diritto di conoscere l'esistenza di un processo decisionale automatizzato, compresa la profilazione, di ricevere informazioni significative sulla logica utilizzata e di conoscere, altresì, l'importanza e le conseguenze previste di tale trattamento per l'interessato, come previsto dagli esaminati artt. 13 e 14 del regolamento (UE) 2016/679.

5.3. Apertura e riutilizzo

Con il concetto di "trasparenza algoritmica" si sposano l'istanza di apertura e il rilascio dei dati in *open data*, esigenze che emergono in modo evidente nella normativa relativa ai dati pubblici[54]. Sono *open data* i dati resi disponibili con le caratteristiche tecniche e legali necessarie per essere liberamente utilizzati, riutilizzati e ridistribuiti da chiunque, in qualsiasi momento e ovunque[55].

L'apertura dei dati, dei quali l'intelligenza artificiale si nutre per svolgere le funzioni e i compiti cui è destinata, potrebbe contribuire a sanare, insieme alla trasparenza, le asimmetrie informative e i correlati rischi etico-sociali, mettendo a disposizione della collettività i dati; inevitabilmente tale operazione provocherebbe una perdita di potere per i titolari degli stessi[56].

[52] Nella risoluzione si pone «enfasi sulla necessità di una responsabilità e una trasparenza ancora maggiori a livello di algoritmo per quanto concerne il trattamento e l'analisi dei dati da parte del settore pubblico, di quello privato e di qualsiasi altro attore che ricorre all'analisi dei dati, quale strumento essenziale per garantire che l'interessato sia debitamente informato del trattamento dei propri dati personali». Al riguardo F. COSTANTINO, *op. cit.*, 799 ss. evidenzia che i modelli utilizzati attualmente sono opachi, non regolati e incontestabili e, peraltro, possono essere errati, dando luogo a gravi lesioni dei diritti nella direzione della cosiddetta dittatura delle probabilità: le decisioni, infatti, sono adottate in base ad un numero talmente elevato di dati «da rendere praticamente impossibile la ricostruzione a posteriori dell'*iter* logico, e quindi della motivazione, con ovvi riflessi sul diritto di difesa di chi si ritenesse pregiudicato»; in merito l'Autore riporta gli esempi di risultati poco convincenti nell'uso dei *big data* in ambito di *screening* dell'occupazione, recidivismo criminale, polizia predittiva.

[53] S. LEUCCI, *Diritto all'oblio, verità, design tecnologico: una prospettiva di ricerca*, in *Rivista di diritto dei media*, fasc. 1, 2017, 123 ss.

[54] In particolare artt. 1 e 50 ss., d.lgs. 82/2005.

[55] In tal senso l'*International Open Data Charter*; cfr. https://opendatacharter.net.

[56] Cfr. A. MANTELERO, *op. cit.*, 140 ss.

Il significativo squilibrio tra le parti in gioco si traduce, infatti, anche nel rischio di "solitudine" del singolo, incapace di potersi tutelare in modo efficace. I "beni" che caratterizzano la società contemporanea sono dati, informazioni e conoscenza, beni collettivi e a titolarità diffusa, che permettono di realizzare interessi generali come trasparenza, partecipazione, democrazia, sviluppo economico, culturale e sociale: in conformità alla loro natura ontologica necessitano di una capacità di disposizione da parte della comunità; di conseguenza, i dati possono essere considerati beni collettivi, che per mezzo dell'apertura possono tornare al legittimo titolare costituito dalla collettività stessa. Aprendoli, i *big data* vengono restituiti e destinati a beneficio dell'intera comunità, al fine di godere dei diritti ed esercitare la sovranità popolare: a tali scopi la regola dovrebbe consistere nell'apertura accompagnata da eccezioni finalizzate sempre al perseguimento di interessi generali, come la tutela di diritti inviolabili o la sicurezza[57].

L'apertura dei dati è capace di realizzare una sanatoria al momento della diffusione, capace di riequilibrare le asimmetrie e garantire libertà e diritti della persona, in linea con la natura non escludibile e non rivale del bene costituito dai dati.

Peraltro l'apertura è in linea con le politiche, le strategie e le normative in materia orientate agli *open data*, trovando fondamento negli artt. 3, 97 e 118 della Costituzione[58].

6. Conclusioni e prospettive future

Le soluzioni ipotizzate che fanno leva su tecnica, etica e *accountability* e favoriscono trasparenza e apertura tracciano alcune direttrici sulle quali basare la *governance* etica e giuridica in materia di intelligenza artificiale.

Sotto tale aspetto, i recenti atti che a livello europeo e nazionale si sono occupati di intelligenza artificiale valorizzano questi profili.

In particolare la Comunicazione della Commissione europea «*L'intelligenza artificiale per l'Europa*» del 25 aprile 2018 evidenzia l'esigenza di rendere disponibili per il riutilizzo volumi maggiori di dati, «materia prima dell'IA», nei quali in particolare sono fatti rientrare i dati del settore pubblico; l'apprendimento automatico opera grazie ai dati disponibili e, di conseguenza, maggiori dati rendono maggiormente accurate le relazioni tra gli stessi su cui le soluzioni di intelligenza artificiale si basano. Con l'apertura si sposa l'esigenza, messa in evidenza dall'Unione europea, di trasparenza sulla logica degli algoritmi, necessaria a garantire efficace protezione alla persona e ad assicurare fiducia nella tecnologia; l'Unione europea reputa di particolare importanza la spiegabilità dei sistemi di intelligenza artificiale, idonea a far comprendere agli uomini le azioni e la logica sottostante, aumentando così la trasparenza e minimizzando il rischio di condizionamenti e errori. I principi di trasparenza e apertura sono idonei a ridurre i rischi in tema di sicurezza, discriminazioni e responsabilità.

[57] M.F. DE TULLIO, *op. cit.*, 678 ss.

[58] Secondo F. COSTANTINO, *op. cit.*, 799 ss. «la maggior parte dei dati di cui dispongono i pubblici poteri può essere ritenuta in ultima analisi di titolarità della comunità e non dell'amministrazione come apparato. […] L'uso di *open data* accresce l'efficacia e l'efficienza dell'attività autoritativa dell'amministrazione e della prestazione dei servizi, promuove il principio di trasparenza, e la partecipazione che essa consente costituisce uno strumento di legittimazione delle istituzioni».

A tali esigenze di trasparenza e apertura, l'Unione europea accompagna la necessità che l'approccio sia basato sui valori e sui diritti fondamentali, in modo da essere sostenibile e da apportare benefici all'intera comunità. A tal fine è necessario assicurare un quadro etico e giuridico adeguato, coerente con la Carta dei diritti fondamentali dell'Unione europea. In specifico gli orientamenti etici dovranno affrontare temi come il futuro del lavoro, l'equità, la sicurezza, l'inclusione sociale e la trasparenza degli algoritmi, esaminando l'impatto sui diritti fondamentali, quali vita privata, dignità, tutela dei consumatori e non discriminazione.

L'Unione europea si concentra altresì sui temi della sicurezza e della responsabilità, che possono esigere anche modifiche alle norme esistenti, laddove insufficienti a regolare questo fenomeno.

Anche la Risoluzione del Parlamento europeo del 16 febbraio 2017 recante «*raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*» evidenzia l'esigenza di norme che disciplinino in particolare la responsabilità, la trasparenza e l'assunzione di responsabilità e che riflettano i valori intrinsecamente europei, universali e umanistici; tali regole non devono influenzare il processo di ricerca, innovazione e sviluppo nel settore della robotica. Il Parlamento europeo pone l'accento sul principio della trasparenza, «nello specifico sul fatto che dovrebbe sempre essere possibile indicare la logica alla base di ogni decisione presa con l'ausilio dell'intelligenza artificiale che possa avere un impatto rilevante sulla vita di una o più persone»; a questo si accompagna la necessità di ricondurre i calcoli tipici di un sistema di intelligenza artificiale a una forma comprensibile per l'uomo. Di conseguenza, il quadro etico di orientamento dovrebbe essere basato sui principi sanciti negli atti dell'Unione europea, quali la dignità umana, l'uguaglianza, la giustizia e l'equità, la non discriminazione, il consenso informato, la vita privata e familiare e la protezione dei dati, la non stigmatizzazione, la trasparenza, l'autonomia, la responsabilità individuale e sociale[59].

In materia di dati, sono interessanti, altresì, le considerazioni delle «*Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*», adottate il 23 gennaio 2017 dal Comitato previsto dalla Convenzione 108, che evidenziano la centralità della persona e del suo diritto di controllo sui dati nell'era degli algoritmi. Le linee guida suggeriscono la considerazione dell'impatto giuridico, sociale ed etico dell'utilizzo dei *big data* sia a livello individuale che collettivo, al fine di prevenire i potenziali effetti negativi sulla dignità umana, sulle libertà e sui diritti fondamentali e indicano la necessità di un uso etico, consapevole e socialmente responsabile dei dati, che comporta al momento dell'analisi del rischio la valutazione circa la possibilità di conflitto con altri diritti e valori, soprattutto laddove le informazioni siano impiegate per scopi predittivi nei processi decisionali.

Anche il Libro Bianco sull'intelligenza artificiale al servizio del cittadino, promosso da AgID, curato dalla Task Force costituita a tal fine e pubblicato nel marzo 2018, prevede tra le sfide dell'intelligenza artificiale al servizio del cittadino l'etica, gli aspetti legali e il ruolo dei dati.

Il Libro Bianco evidenzia la necessità di qualità e neutralità dei dati, accompagnata da *accountability* e responsabilità, tutela della persona e dei suoi dati, trasparenza e apertura. Sotto tale profilo la pubblica amministrazione deve ottemperare a precisi obblighi nei confronti dei cittadini, nel momento in cui stabilisce di fornire loro dei servizi o di prendere decisioni che li riguardano, servendosi di so-

[59] Per un'analisi della risoluzione cfr. O. RUSSO, *Io, persona robot. Il nuovo diritto pubblico della robotica*, in *Amministrativ@mente*, 2018, fasc. 3-4, 1-10.

luzioni di intelligenza artificiale; in particolare il funzionamento di queste ultime deve rispondere a criteri di trasparenza e apertura. La trasparenza si trasforma in un prerequisito fondamentale per evitare discriminazioni e risolvere il problema dell'asimmetria informativa, garantendo al cittadino il diritto alla comprensione delle decisioni pubbliche. A tal fine, le basi di dati devono essere costituite in maniera corretta, garantendo consistenza, qualità, interoperabilità e intelligibilità e trasformando i dati in conoscenza diffusa e condivisa, tale da rendere trasparente l'amministrazione verso i cittadini e verso se stessa; in tal modo l'amministrazione pubblica è capace di assicurare a cittadini e amministratori non solo l'accesso semantico alle informazioni e l'interoperabilità dei processi, ma una migliore comprensione del rapporto tra Stato e cittadino.

In conclusione, alla luce dell'analisi compiuta e in considerazione degli atti esaminati, nel difficile rapporto tra intelligenza artificiale e diritto in ambito pubblico la tecnologia deve essere guidata dalla mano dell'uomo, deve essere orientata ai valori e ai principi giuridici per mezzo della scienza giuridica e deve essere accompagnata da un solido approccio etico, basato su *accountability*, trasparenza e apertura.

ISSN 2284-4503