Il sapere e la professionalità dell'amministrazione pubblica nell'era dei big data e dell'intelligenza artificiale.

Angelo Lalli

Sommario. Premessa. 1.Lo Stato e l'amministrazione all'epoca dei big data. Le nuove dimensioni e le nuove fragilità del potere: una rinnovata legittimazione dell'intervento diretto dello Stato e nuovi modelli di regolazione. 2. L'intelligenza artificiale e le sue applicazioni nell'ambito dell'attività amministrativa tra cautele e aperture: il condizionamento delle tradizioni culturali. 3.Alcune conclusioni: necessità di dialogo interdisciplinare e ripensamento del metodo giuridico.

Premessa. Klaus Schwab, fondatore e presidente del *World Economic Forum* (2016), descriveva l'epoca che stiamo vivendo come "quarta rivoluzione industriale". Con tale espressione si allude allo sviluppo e alla contestuale estesa applicazione a tutti gli ambiti della vita sociale ed economica di alcune nuove tecnologie quali le varie modalità di comunicazioni digitali, la elaborazione dei dati e l'interconnessione della popolazione mondiale sempre più estesa attraverso la rete internet. Secondo la prospettiva di Schwab, mentre le precedenti rivoluzioni industriali avevano liberato l'umanità dal condizionamento della forza animale, con l'invenzione delle macchine a vapore; reso possibile la produzione di massa, con la realizzazione della catena di montaggio, e portato una prima generazione di capacità digitali a miliardi di persone, con l'avvento e lo sviluppo esponenziale delle comunicazioni digitali, della telefonia mobile e della rete internet, l'attuale c.d. quarta rivoluzione industriale avrebbe una natura fondamentalmente diversa. È caratterizzata da tecnologie che fondono il mondo fisico, digitale e biologico e che incideranno, in breve tempo, in modo radicale su tutti i settori economici e industriali. Ciò metterà in discussione la stessa idea di essere umano cui siamo abituati: si pensi, a mero titolo di esempio, alle nuove possibilità che sono consentite dall'ingegneria genetica, dalla bioingegneria e dallo sviluppo delle nanotecnologie.

I fattori trainanti sono lo sviluppo sempre più rapido dell'intelligenza artificiale (nella più evoluta declinazione del c.d. *machine learning*), la robotizzazione delle economie e della vita quotidiana, l'uso della stampa 3D, il dominio dei *big data* e della rete delle cose "*internet of things*". Questi sviluppi potranno portare benefici all'umanità, ma data la radicalità, pervasività e rapidità dei cambiamenti - che già sono

in corso - rispetto a inveterati modelli di produzione, di organizzazione del lavoro e, in ultima istanza, di vita quotidiana - sono intuibili anche i possibili rischi di effetti negativi. Si pensi, solo per fare qualche esempio, allo strapotere dei detentori, soggetti privati e pubblici, dei *big data* che, ad oggi, non risulta efficacemente contenuto dalle varie forme di controllo sociale pure istituite, con la conseguenza che quei soggetti hanno la possibilità, un tempo impensabile, di configurare – a nostra insaputa - una schedatura dettagliata di ogni nostra azione della vita, che resta nei loro archivi e può essere usata per i più disparati fini. Si pensi alla c.d profilazione dei consumatori e ma anche degli elettori, e dunque con impatti condizionanti sia le scelte economiche, sia addirittura le scelte politiche dei singoli[1]. Si pensi, ancora, all'inevitabile progressiva eliminazione dell'intervento umano per lo svolgimento di un novero sempre più ampio di lavori anche caratterizzati da un contenuto eminentemente intellettuale e non manuale, con la conseguente formazione di una massa sempre più estesa di persone che non potranno trovare un'occupazione perché semplicemente non ci sarà più bisogno di loro. Si pensi poi ai computer dotati di algoritmi "intelligenti" che funzionano secondo il modello delle reti neurali[2] e che, dunque, riescono a sviluppare risultati imprevedibili al momento dell'elaborazione dell'algoritmo di base: in sostanza riescono a imparare dal contesto fattuale con cui entrano in contatto, potendo adottare scelte non del tutto prevedibili da chi ha impostato l'algoritmo originario.

Un simile scenario pone sfide veramente nuove al diritto e alla capacità dei governi e delle amministrazioni di regolare la società se si vuole – come pare si debba – tutelare in questo nuovo contesto quel complesso dei diritti di libertà e diritti sociali, individuali e collettivi, che sono alla base della nostra cultura giuridica.

Si tratta di sfide che potranno essere affrontate solo a patto che gli Stati e le amministrazioni si adeguino anche in termini di capacità professionali idonee a gestire l'attuale inusitata complessità.

---

[1] Si può ricordare lo scandalo di Cambridge Analytica, una società di consulenza britannica che gestiva i dati delle persone acquisite da Facebook a loro insaputa per influenzare le campagne elettorali. Il metodo utilizzato combinava il *data mining*, l'intermediazione dei dati e l'analisi dei dati con la comunicazione strategica per la campagna elettorale. Il 2 maggio 2018 la società ha dichiarato la bancarotta a causa dello scandalo in cui era stata travolta con Facebook che a sua volta è stata da ICO, il Garante Privacy UK, multata per 500 mila sterline.
Si può dubitare che simili meccanismi sanzionatori siano realmente efficaci per prevenire l'uso distorto dei dati personali carpiti abusivamente dalle gigantesche imprese di servizi che operano sul web. Su tali aspetti si veda il rapporto dell'ICO "*Investigation into the use of data analytics in political campaigns, A report to Parliament, 6 November 2018*, reperibile su https://ico.org.uk.

[2] Introduction to Computational Neurobiology & Clustering, B. Tirozzi, D. Bianchi, E. Ferraro, World Scientific, Singapore 2007; Schmidhuber, J., Deep Learning in Neural Networks: An Overview, (Submitted on 30 Apr 2014 (v1), last revised 8 Oct 2014) in Neural Networks, 2015.

I saperi necessari all'amministrazione, infatti, devono essere in grado di poter rispondere alle nuove esigenze poste dalla "quarta rivoluzione industriale". Le nuove esigenze richiedono nuovi modelli di intervento pubblico e, dunque, anche nuove modalità di regolazione.

Occorre descrivere, almeno in linee generali, queste nuove modalità di intervento e di regolazione per poter poi conseguentemente trarre conclusioni in merito alle tipologie dei saperi di cui l'amministrazione ha bisogno e ai rapporti che dovranno instaurarsi tra i diversi saperi nell'esercizio delle competenze amministrative nel nuovo contesto.

Occorre anticipare, infatti, che non sarebbe sufficiente una risposta che si limiti a rilevare l'esigenza di assumere tecnici esperti nei vari settori dell'economia digitale, dell'*information technology* e dell'intelligenza artificiale in grado di comprendere le nuove tecnologie. Questo sarà senz'altro utile: ma occorre che l'amministrazione acquisisca anche una più matura consapevolezza sui cambiamenti qualitativi che dovranno caratterizzare i propri processi decisionali e i propri interventi per essere adeguati alle nuove sfide che la società di oggi presenta.

La "quarta rivoluzione industriale" pone allo Stato e all'amministrazione pubblica problemi indubbiamente complessi che esigono una modifica degli stessi processi di regolazione e, in genere, anche il potenziamento degli interventi diretto dello Stato proprio allo scopo di sostenere ricerche teoriche e applicative nel settore.

Da ciò discende, come cercheremo di evidenziare, la sempre più sentita necessità di poter poggiare le varie attività amministrative su conoscenze specialistiche, tecniche e giuridiche, che devono operare secondo un approccio interdisciplinare che promuova il dialogo tra i vari ambiti disciplinari e sia in constante rapporto con le competenze che si formano nel settore privato: l'amministrazione risulta, infatti, spesso tributaria di conoscenze che il settore privato pare in grado di sviluppare meglio e più rapidamente.

In tale contesto, la cultura giuridica dovrà non solo interagire con gli altri saperi tecnici, ma dovrà anche tentare di rinnovarsi e riformulare i propri criteri operativi in modo da renderli più oggettivi possibili al fine di poter offrire un sostegno efficace alle scelte dell'amministrazione in un mondo ormai cambiato.

Ai fini espositivi si ritiene opportuno selezionare, in via esemplificativa, solo alcuni dei problemi posti dall'attuale stato dell'evoluzione tecnologica, per poi discuterne le possibili implicazioni, anche alla luce di prime concrete esperienze; da

queste considerazioni, come premesso, si potranno trarre orientamenti circa il ruolo che le competenze professionali e i diversi saperi dovrebbero avere in un'amministrazione pubblica che voglia essere al passo con i tempi.

Si ritiene di soffermare l'analisi su due problematiche che, sebbene siano il frutto delle medesime innovazioni tecnologiche, esprimono esiti ambivalenti. Ci si riferisce, da un lato, alla tematica del potere derivante dal possesso e dalla gestione dei *big data,* realizzata con i più sofisticati processi di *data mining* e, dall'altro, alla accresciuta vulnerabilità – dovuta alle medesime tecnologie - delle stesse strutture, pubbliche o private, che presiedono alla gestione dei propri dati e tramite essa all'esercizio delle proprie funzioni o attività. In quest'ultimo ambito, si analizzeranno solo gli aspetti significativi ai fini del discorso che ci proponiamo di svolgere della disciplina posta dalla direttiva UE 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, cd. NIS, recante misure per un livello comune di sicurezza delle reti e dei sistemi informativi dell'Unione che è stata attuata con il Dlgs. 18 maggio 2018, n.65.

Si passerà poi a considerare le prospettive dischiuse dall'intelligenza artificiale sia per quanto concerne la sua applicazione nell'attività amministrativa che giurisdizionale.

Si trarranno, infine, alcune conclusioni.

1.**Lo Stato e l'amministrazione all'epoca dei *big data*. Le nuove dimensioni e le nuove fragilità del potere: una rinnovata legittimazione dell'intervento diretto dello Stato e nuovi modelli di regolazione.**

Le tecnologie dell'informazione, internet e i software operativi che consentono di processare l'enorme quantità di dati prodotti nel settore pubblico e privato stanno cambiando le modalità di affermazione dei rapporti di forza tra gli Stati a livello internazionale e le relazioni tra gli Stati e i privati cittadini.

D'altro canto, l'interconnessione attraverso la rete *internet* - che è caratteristica tipica degli attuali sistemi di elaborazione dati gestititi da enti pubblici e da privati - espone i gestori a possibili ingerenze abusive di parti terze: i c.d. attacchi informatici o *hakeraggi* che possono mettere in crisi la prestazione di importanti servizi pubblici e carpire informazioni e dati che dovrebbero rimanere riservati.

In sintesi, Stato e amministrazione pubblica all'epoca dei *big data*, da un lato, acquisiscono nuove e particolarmente incisive forme di potere, ma contestualmente, dall'altro, sono esposti a ingerenze che possono provenire da altri Stati o anche da

privati che siano in grado di penetrare le difese dei loro sistemi informatici, carpire le informazioni più delicate e alterarne il funzionamento.

Dunque, una nuova dimensione del potere e nuove fragilità vanno di pari passo: da questa realtà derivano conseguenze che occorre valutare partitamente.

Sul fronte delle nuove dimensioni del potere si può osservare che da sempre l'acquisizione delle informazioni ha costituito un'attività utile, se non necessaria, per garantire stabilità al potere e per accrescerne l'influenza, ma solo oggi la tecnologia consente non soltanto di acquisire informazioni su un numero indefinito ed elevatissimo di persone e situazioni - attingendo alle fonti più disparate (dall'attività di navigazione su *internet*, all'utilizzo dei social network, dall'uso della posta elettronica, alla mappatura dei movimenti attraverso la geolocalizzazione fornita oggi da qualunque *smartphone*, solo per fare gli esempi più immediati che provengono dalla comune realtà quotidiana) - ma anche di processare questa enorme messe di dati, rilevando concordanze, *trend* di comportamento dei consumatori, prospettive di andamento dei mercati e linee di orientamento in genere di persone e imprese. Va sottolineato che le informazioni oggetto di trattamento non attengono solo alla dimensione meramente economica e consumistica della vita delle persone e delle imprese, ma possono riguardare ogni aspetto della vita umana. Si pensi ai momenti di vita privata che, attraverso le nostre volontarie[3] comunicazioni sui *social network*, sono consegnati a uno spazio cibernetico, a-territoriale che li memorizza, li rende visibili quantomeno al c.d. amministratore di sistema, ma potenzialmente anche a una serie indeterminata di soggetti. In questo contesto, chi detiene gli strumenti che consentono di raccogliere i dati, di incrociarli e processarli non solo è informato, ma spesso lo è in anticipo grazie anche alla capacità predittiva, sempre più attendibile, di alcuni *software*; egli quindi non solo sa, ma sa prima degli altri ed è in grado quindi anche di orientare il proprio e l'altrui comportamento.

L'informazione nell'era del digitale è, quindi, sempre più strumento di potere in quanto oggi è possibile l'analisi dei grandi flussi di dati aggregati e anche l'indagine disaggregata di quei medesimi flussi; si tratta di operazioni che possono consentire di cogliere, documentare e condizionare l'attività di singoli individui o singole imprese.

In considerazione di questo rilevante accrescimento del potere di controllo e di condizionamento su persone e imprese, l'attività volta ad accrescere e migliorare i

[3] Anche se, occorre osservare, che spesso la volontarietà si basa su consensi rilasciati senza un'adeguata informazione e con il condizionamento derivante dal fatto di non poter accedere al servizio offerto ove si scegliesse di non consentire il richiesto trattamento dei dati personali

sistemi informatici che questo potere sorreggono è considerata dagli Stati di primaria rilevanza.

La lotta per il controllo dei dati e per l'elaborazione delle informazioni costituisce oggi una delle linee di trincea più importanti lungo la quale si contendono il potere e la capacità di influenza i grandi Stati nazionali nell'arena internazionale. A questo livello il conflitto, non è cruento, ma non per questo è meno acceso. Attori principali, come detto, sono gli Stati, anzi i grandi Stati nazionali che sono i protagonisti della scena internazionale. Essi mobilitano ingenti risorse pubbliche per la ricerca e la elaborazione di sistemi sempre più sofisticati di acquisizione e gestione dell'informazione. Gli obiettivi possono essere la sicurezza dello Stato da attacchi esterni o il sostegno della propria economia e delle proprie imprese al fine di penetrare i mercati esteri.

Va rilevato un altro elemento importante. Assieme agli Stati nazionali, in tale scenario, giocano un ruolo importante alcune grandi imprese che operano sulla rete *internet* fornendo servizi e perciò gestendo la miriade di dati dei propri clienti: si pensi ai gestori dei social network, ma anche ai motori di ricerca e alle piattaforme di vendita di beni e servizi. Tali soggetti, di fatto, hanno un accesso privilegiato ai dati in virtù dei rapporti che intrattengono con milioni di utenti e la forza economica per sviluppare applicativi in grado di sempre meglio profilare i comportamenti dei singoli individui con cui sono in contatto.

In queste attività spesso tali soggetti cooperano con gli Stati nazionali per la gestione e il controllo sui dati, secondo modalità di volta in volta di fatto negoziate e che interrogano il modo tradizionale di intendere le garanzie del diritto costituzionale riguardo ai rapporti tra poteri pubblici e poteri privati.

Se, ad esempio, Facebook[4] continuerà a promuovere il progetto di attivare una sua criptovaluta, è da ritenere che le autorità statunitensi interverranno, ma difficilmente avranno il potere reale di impedire la realizzazione di un business che dovesse incontrare il favore – come è probabile – di un'amplissima platea di soggetti. Piuttosto, è credibile che le autorità si accordino con l'operatore privato per una gestione concordata dei dati e dei nuovi servizi [5].

[4] Si legga il Wall Street Journal che sin dall'inizio della vicenda ha dedicato ampio spazio alla questione reperibile su https://www.wsj.com/; in particolare nell'edizione del 23 settembre 2019 si veda *The Coming Currency War: Digital Money vs. the Dollar.*

[5] La stessa Banca d'Italia, pur con cautele, dimostra disponibilità a valutare l'adeguata vigilanza da porre per questi fenomeni senza però ostacolarli cfr. L'intervento del vice direttore generale della Banca d'Italia a un convegno del settembre 2019 reperibile su https://cryptonomist.ch › 2019/09/25.

Si pensi ancora alla profilatura di massa che si sta realizzando in Cina attraverso la creazione del c.d. Sistema di Credito Sociale[6]. Si tratta di un'iniziativa del Governo cinese attivata al fine di sviluppare un sistema nazionale per classificare la reputazione dei propri cittadini, sulla base del rilevamento delle loro abitudini e dei comportamenti, cui segue un meccanismo di attribuzione di un punteggio: positivo per i comportamenti ritenuti socialmente apprezzabili e negativo per quelli che saranno considerati antisociali. Il punteggio sarà il presupposto per realizzare un apparato premiale, ma anche sanzionatorio. Il sistema per il momento nasce su base volontaria, ma entro il 2020 sarà obbligatorio in tutta la Cina continentale. Il Sistema di Credito Sociale viene presentato dal Governo cinese come uno strumento per perfezionare l'economia di un mercato socialista e per rafforzare e innovare il modo di dirigere la società. Dato interessante è che al progetto partecipano attivamente non solo enti pubblici, ma anche grandi imprese di servizi che operano sulla rete come Alibaba Group e lo sviluppatore di software Tencent.

Con queste osservazioni, si conferma uno degli aspetti tipici delle nuove tecnologie digitali connesse ai *big data*: esse consentono la concentrazione di un potere inusitato in capo a pochi soggetti pubblici – i grandi Stati - o i grandi operatori privati.

Nell'arena internazionale si assiste, come avvertito, a una guerra incruenta che può dare luogo a occasionali e transitorie negoziazioni tra grandi Stati e tra questi e le grandi imprese.

In questo ambito l'interesse degli stati è orientato a potenziare gli investimenti in ricerca e sviluppo: lo Stato che meglio e prima degli altri riesce ad attingere alle informazioni e alle più sofisticate modalità di elaborazione delle stesse sarà in grado di esprimere una forza politica maggiore sul piano internazionale. E ciò vale per tutti gli Stati, non solo quelli considerati autoritari, ma anche quelli di tradizione democratica.

Sul piano pratico, va anche considerato che piccole nazioni, come la nostra, non potranno mai esprimere una capacità di investimento pubblico paragonabile a quella manifestata dai grandi Stati o dalle grandi imprese citati. L'amministrazione italiana potrà senz'altro potenziare i propri apparati di ricerca e gestione dei dati, ma

[6] Si veda la descrizione dell'iniziativa contenuta nella *State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014-2020*) e tradotta da Rogier Creemers, ricercatore di Oxford; il documento è reperibile sul sito https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/

nella consapevolezza che, in assenza di una più intensa e leale cooperazione a livello europeo, non sarà possibile attingere ai medesimi risultati applicativi che rendono i grandi Stati nazionali tali sulla scena internazionale.

Di fronte a questi scenari, in ogni caso, si pongono però anche rilevanti problemi per gli ordinamenti ispirati alla tradizione dello stato di diritto: riemerge con forza l'eterna preoccupazione del controllo sociale sul potere dello Stato.

Occorre domandarsi se i meccanismi noti e consolidati siano sufficienti per impedire derive quali quella segnalata nel caso della Cina e che in misura meno penetrante, ma sempre lesiva dei diritti delle persone, si potrebbero realizzare anche negli stati democratici.

Hanno oggi i parlamenti mezzi conoscitivi adeguati e professionalità idonee per capire e valutare l'impatto effettivo del potere di alcune amministrazioni di raccogliere e processare i dati dei cittadini? Sono sufficienti le cautele poste a presidio del diritto alla riservatezza?

Se si osservano le attuali strutture e procedure conoscitive e ispettive dei parlamenti, come il nostro, pare lecito dubitare che siano in grado di valutare in autonomia l'impatto e l'effettiva incidenza degli strumenti di gestione delle informazioni utilizzati da alcune peculiari strutture tecniche amministrative: si pensi alle banche dati delle agenzie fiscali, del Ministero dell'interno, delle Agenzie per la sicurezza interna e internazionale.

Concludendo sul punto, si può affermare che il potere dello Stato e dei grandi privati nell'epoca dei *big data* ha indubbiamente acquistato nuovi spazi di affermazione.

La battaglia per il dominio sui dati e sulle informazioni si combatte a colpi di investimenti in ricerca e sviluppo di dimensioni ingenti e attraverso forme di intervento diretto dello Stato che, per le ragioni dette, sono nella disponibilità delle amministrazioni, sotto la direzione dei Governi e senza subire adeguati controlli da parte dei Parlamenti.

I *big data* esigono una presenza forte degli Stati che vogliano mantenere un potere reale nell'agone internazionale. A questo livello, si deve inoltre constatare che i singoli Stati dell'Unione europea, tra loro divisi ancora su queste politiche, mostrano un'evidente debolezza rispetto ai grandi Stati nazionali, come appunto la Cina, gli Stati Uniti o la Russia.

L'epoca dei *big data* poi, come notato, fa riemergere il problema dell'efficacia dei controlli sociali su queste nuove forme di potere pervasive.

Una via per riequilibrare il sistema di *checks and balances* potrebbe passare proprio attraverso politiche di sviluppo di strutture tecniche di controllo pubbliche, soggette ai Parlamenti e in grado di dialogare con le strutture tecniche dell'amministrazione che detengono il controllo sui dati.

L'approntamento di strutture pubbliche dotate di sapere tecnico e il frazionamento delle stesse tra i poteri supremi dello Stato pare oggi una via efficace per ristabilire un controllo effettivo dei Parlamenti sulle amministrazioni che non può certo essere soddisfatto dalla mera soggezione formale del Governo al potere di sindacato ispettivo del Parlamento che, in mancanza di adeguate professionalità, non è all'evidenza in grado di esplicarsi efficacemente.

Venendo alle nuove fragilità che pur connotano le strutture pubbliche – e private - all'epoca dei *big data* a causa dell'interconnessione dei sistemi di gestione delle informazioni attraverso la rete internet, occorre indagare alcune peculiari caratteristiche della regolazione predisposta allo scopo di garantire appunto la sicurezza dei sistemi informatici (c.d. *cyber security*). Nell'economia del presente lavoro, il *focus* su questa normativa è funzionale a illustrare alcune nuove peculiari modalità regolatorie che caratterizzano l'età presente. Esse differiscono dai tradizionali approcci dello schema *comand and control* e presuppongono specifici saperi in grado di gestire le competenze amministrative da esercitare sui nuovi problemi.

Come noto, l'esigenza di varare la direttiva UE 2016/1148, c.d. NIS, è scaturita dalla constatazione che le reti e i sistemi informativi svolgono un ruolo centrale nella vita economica e sociale. Una serie di servizi, oggi essenziali, dal credito, all'energia elettrica, dai trasporti, alla sanità, alla fornitura di acqua potabile funzionano sulla base di sistemi informatizzati. Questi sistemi, in quanto interconnessi alla rete internet, possono essere vulnerati per i più diversi fini dall'esterno: per lo più si tratta di fini illeciti, non ultimi sono da considerare gli scopi terroristici; inoltre, i sistemi informatici possono subire pregiudizi al loro funzionamento a causa di guasti interni o errori degli stessi gestori. Il malfunzionamento di questi sistemi, indotto intenzionalmente o anche originatosi per difetto intrinseco del sistema stesso, può determinare ingenti danni a cittadini a imprese e alla stessa pubblica amministrazione; si tratta di danni di rilievo non solo patrimoniale, atteso che alcuni dei servizi potenzialmente aggredibili sono diretti proteggere interessi primari della persona come la salute e attengono alla

sicurezza dei cittadini intesa in generale. Di qui l'esigenza di una regolazione comune stabilita dall'Unione europea.

Il sistema di protezione della sicurezza informatica delineato dalla direttiva individua, in primo luogo, i soggetti su cui gravano gli obblighi strumentali a garantire la sicurezza delle reti. Si tratta degli operatori nei servizi essenziali e dei fornitori dei servizi digitali. È demandata agli Stati l'individuazione puntuale dei soggetti tenuti a rispettare gli obblighi imposti dalla normativa.

Su tali soggetti grava in particolare l'obbligo di adottare "*misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguati al rischio esistente*". Gli operatori dei servizi essenziali e i fornitori dei servizi digitali devono, inoltre, attuare "*misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi*". (art.14 e 16 della direttiva).

Gli operatori sono tenuti poi a notificare all'Autorità competente, che ogni Stato deve individuare, gli incidenti aventi impatto rilevante sulla continuità dei servizi prestati.

Il sistema di controllo pubblicistico è, quindi, affidato a un'Autorità competente a controllare il rispetto della direttiva. Questa Autorità deve essere dotata di risorse anche umane e, dunque, professionali adeguate per svolgere in modo efficiente ed efficace i propri compiti (art.8). Essa ha il potere di richiedere agli operatori le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, ha il potere di esigere dai soggetti obbligati la prova che hanno effettivamente attuato adeguate politiche di sicurezza. L'Autorità può emanare istruzioni vincolanti per rimediare alle carenze eventualmente riscontrate. Affianca l'Autorità competente, il Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT), che si attiva appunto in caso di incidente; anch'esso deve essere "*dotato di risorse adeguate*" e in particolare deve avere accesso *"a una infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale*" (art.9).

L'Autorità competente svolge, come accennato, un controllo preventivo e costante sugli operatori e il CSIRT si attiva in caso di incidente.

Le Autorità possono anche imporre sanzioni sugli operatori che violino gli obblighi imposti dalla direttiva (art. 21).

Sono quindi previsti meccanismi di cooperazione tra le autorità competenti dei vari Stati membri, nella consapevolezza che gli incidenti di funzionamento delle reti e dei sistemi informativi possono avere un carattere diffusivo che si estende ad aree geografiche molto ampie.

L'aspetto che più interessa in questa sede è quello connesso all'individuazione del contenuto puntuale degli obblighi che gravano sugli operatori e alle modalità di elaborazione e di verifica degli stessi.

Gli articoli 14 e 16 della direttiva sopra richiamati non delineano comportamenti specifici da tenere, ma fissano obblighi di risultato. Gli operatori sono tenuti a svolgere un'autovalutazione dei rischi che possono colpire la propria rete o il proprio sistema e ad approntare i rimedi più adeguati al loro caso specifico. Il parametro normativo di riferimento è, in ultima analisi, costituito dalle "*conoscenze più aggiornate in materia".*

Ad evidenza, si tratta di indicazioni tutt'altro che puntuali e che in ogni caso rinviano a un dato extra normativo che inevitabilmente sarà il frutto della elaborazione di saperi tecnici. A ragionare sulla base del tradizionale principio di legalità, si dovrebbe concludere che la norma in questo caso non individua – come dovrebbe - un parametro di comportamento sufficientemente definito e, pertanto, l'obbligo di conformazione dell'operatore è difficile da valutare nel concreto e ancora più critica sarebbe l'eventuale applicazione di una sanzione – pur prevista – per non essersi attenuti a un comportamento dovuto che non è previamente definito nei contenuti.

Il fenomeno è già presente nella regolazione dell'economia: si pensi al tema dei concetti giuridici indeterminati che si applicano ad esempio nella disciplina *antitrust* (i termini di mercato rilevante, posizione dominante, abuso, intesa anticoncorrenziale). Tuttavia, in questo caso il concetto giuridico indeterminato risulta in realtà integrato e definito dal riferimento a nozioni economiche che conoscono un adeguato grado di stabilità. La giurisprudenza dell'Unione e nazionale hanno contribuito a definire con elevato grado di precisione i parametri di riferimento: il momento di dubbio può sorgere nella fase di valutazione del fatto concreto e nella sua sussunzione nell'astratto paradigma dell'illecito concorrenziale, ma quest'ultimo conosce una compiuta identificazione.

Ad analoghe conclusioni può pervenirsi con riguardo alla regolazione posta in essere dalle autorità dei vari settori: dalle comunicazioni, alle energia, ai mercati

finanziari. In questi casi, i concetti giuridici indeterminati con cui la legge delinea il presupposto applicativo del potere delle Autorità è da queste ultime puntualmente definito a seguito di un processo regolatorio partecipato che giunge a individuare un quadro di regole predeterminare su cui gli operatori possono fare affidamento.

Non è così riguardo la richiamata disciplina della *cyber security*: in tale caso, come si è cercato di illustrare, il parametro di comportamento obbligatorio è continuamente cangiante.

Costituiscono ulteriore dimostrazione della realtà che si sta descrivendo le previsioni (artt.15 e 17 della direttiva citata) secondo cui le Autorità competenti possono adottare provvedimenti, se "*necessario mediante misure di vigilanza ex post*", quando ottengono la prova che un operatore di servizi essenziali o un fornitore di servizi digitali non rispetta gli obblighi di risultato ora richiamati. In sostanza, il controllo pubblico può intervenire *ex post*, ovvero alla luce del verificarsi di un incidente informatico, per valutare - con il senno di poi - se il sistema di prevenzione della sicurezza adottato era adeguato. Ma il verificarsi dell'evento ne dimostra di per sé l'inadeguatezza e ciò legittima l'autorità competente a imporre misure e forse anche sanzioni.

L'assenza di puntuali e relativamente stabili parametri che integrino il contenuto del dovere di conformazione dell'operatore è poi ulteriormente ed esplicitamente dimostrato dall'art. 19 della direttiva che, al fine di promuovere l'applicazione di *standard* di sicurezza convergenti, stabilisce che gli Stati membri "*senza fare imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, incoraggino l'uso di norme e specifiche europee o accettate a livello internazionale relative alla sicurezza delle reti e dei sistemi informativi".* L'Ente europeo (ENISA), in collaborazione con gli Stati membri, redige pareri e linee guida allo scopo di supportare l'auspicabile processo di convergenza che però per sua natura non potrà esitare in un decalogo di prescrizioni puntuali, ma indicherà protocolli e prassi soggetti a costante aggiornamento.

Queste disposizioni che, come detto, a prima vista delineano un modello di regolazione estraneo alle nostre tradizioni culturali – il comportamento imposto all'operatore non è definito, l'Autorità può intervenire *ex post* e imporre misure e sanzioni in assenza dell'accertamento della violazione di una precisa prescrizione che non è predeterminata, ma per il sol fatto che il sistema si è dimostrato vulnerabile – si può comprendere e giustificare solo se si mette in luce il particolare fenomeno regolato.

La sicurezza dei sistemi informatici esige un costante adeguamento dei protocolli e delle metodologie per scongiurare gli incidenti: uno *standard* considerato oggi adeguato può rivelarsi, nel torno di pochi mesi, assolutamente insufficiente. In questa situazione la regolamentazione deve operare necessariamente per clausole generali, limitandosi a indicare le finalità delle dovute azioni di protezione. Ma, soprattutto, un simile impianto di vigilanza si deve basare necessariamente sulla collaborazione costante tra operatori soggetti agli obblighi di regolamentazione e le autorità di controllo.

In assenza di questo essenziale e continuo confronto tecnico tra Autorità di controllo e operatori cade l'effettività stessa del sistema di protezione della sicurezza degli apparati che l'Unione ha correttamente voluto affermare.

Occorre prendere atto, in altri termini, che la peculiarità del fenomeno da regolare impatta sulla modalità stessa di regolazione. Questa, per essere efficace, deve essere sufficientemente elastica poter comprendere tutte le evenienze pericolose. Ma ciò comporta una radicale trasformazione del modello di regolazione.

Non più, dunque, il modello classico del *command and control*, ma una continua interazione tra autorità di controllo e operatore controllato allo scopo di individuare, in modo cooperativo, non oppositivo, né conflittuale, le soluzioni migliori. In questo quadro lo strumento sanzionatorio, non solo resta *extrema ratio,* ma per risultare compatibile con il principio di legalità ovvero con la *rule of law* nel senso più ampio dell'espressione potrà essere utilizzato solo per stigmatizzare comportamenti deliberatamente posti in essere in violazione di quei pochi obblighi di comportamento sufficientemente dettagliati in anticipo. Non potrà certo essere utilizzato per stigmatizzare la mancata previsione di un sistema di protezione che sarebbe stato impossibile ipotizzare prima della realizzazione dell'incidente.

Nella disciplina di questi aspetti l'Amministrazione competente non ha un proprio sapere da imporre – anzi esplicitamente la norma, come visto, richiama il principio della neutralità tecnologica, lasciando con ciò all'evoluzione spontanea del mercato elaborare gli *standard* migliori – ma dovrà essere promotrice di un sapere che si integra necessariamente con i saperi sviluppati dagli stessi operatori nel mercato, nella logica della collaborazione più volte evidenziata. Gli *standard* di protezione quindi non potranno che emergere a seguito dell'apporto congiunto dei saperi espressi dall'amministrazione e di quelli elaborati dagli operatori regolati. Questa realtà esigerà certamente da parte dell'amministrazione e degli operatori l'individuazione di

professionalità tecniche adeguate, ma presupporrà anche un cambio di mentalità degli operatori del diritto chiamati a valutare la conformità dei comportamenti alla legge. La cultura giuridica avrà bisogno di essere integrata dalla cultura tecnica per poter efficacemente operare in questi settori.

2. L'intelligenza artificiale e le sue applicazioni nell'ambito dell'attività amministrativa tra cautele e aperture: il condizionamento delle tradizioni culturali.

Tra gli sviluppi più significativi che connotano la c.d. "quarta rivoluzione industriale" c'è l'evoluzione, imprevista solo fino a qualche anno fa, delle potenzialità applicative della c.d. intelligenza artificiale (più semplicemente in seguito I.A).

In via di estrema sintesi, e cercando di cogliere l'aspetto in questa sede rilevante, con intelligenza artificiale si può intendere l'insieme di quei processi, realizzati artificialmente mediante l'uso di computer e consistenti nella raccolta e organizzazione di grandi masse di dati (i *big data* di cui si è discorso sopra) e nella individuazione, sulla base della predetta elaborazione, di concordanze e connessioni che fanno emergere apporti conoscitivi nuovi, non esistenti al momento dell'inizio dell'elaborazione. Si tratta di processi conoscitivi non meramente computazionali (ovvero ripetitivi di uno schema di elaborazione sempre uguale a se stesso) che si realizzano attraverso un procedimento di calcolo – appunto l'algoritmo – che è in grado di elaborare schemi interpretativi nuovi della realtà, sulla base di inferenze probabilistiche che poggiano sui dati acquisiti; l'algoritmo, inoltre, è in grado di elaborare attendibili predizioni sugli eventi futuri. L'aspetto di maggiore interesse è rappresentato dalla possibilità - oggi concreta - che tali 'macchine' riescano a imparare da sole e, sulla base di queste cognizioni auto-acquisite, procedere a scelte successive non predeterminate, perché non presenti come tali nell'iniziale istruzione di funzionamento iscritta nell'elaboratore da parte dell'ideatore umano (il c.d codice sorgente).

Il fenomeno viene definito "*machine learning*" e indica appunto quelle metodologie che consentono all'elaboratore il riconoscimento di *pattern* e il miglioramento progressivo della *performance* di un algoritmo nell'identificare schemi nuovi attraverso la lettura di dati in applicazione di varie tecnologie quali le reti neurali artificiali, il filtraggio adattivo, la teoria dei sistemi dinamici, l'elaborazione delle immagini, il c.d. *data mining*. L'evoluzione in esame è strettamente connessa al data

mining[7] (cioè l'estrazione di informazioni da grandi quantità di dati grezzi di per sé insignificanti) e all'applicazione delle sofisticate tecniche statistiche bayesiane che consentono di produrre modelli realistici dei probabili sviluppi della realtà, basandosi sull'osservazione della stessa. Queste tecniche sono solo oggi divenute possibili in virtù dell'aumento della potenza di calcolo dei computer e della maggiore disponibilità di dati facilmente reperibili attraverso la rete *internet*.

Le applicazioni concrete dell'IA divengono sempre più numerose nella vita economica.

Si pensi, ad esempio, ai consigli che operatori come NETFLIX o Amazon rivolgono ai clienti, attuali o potenziali, elaborati sulla base delle loro preferenze dedotte dai comportamenti che i medesimi manifestano navigando sul web. Si pensi alle applicazioni quali Siri, Alexia o Google Assistant, ovvero piattaforme interattive con cui è persino possibile avere scambi vocali di domande e risposte. Esistono e sono omologate vetture che, individuata un'area di parcheggio adeguata, possono eseguire una perfetta operazione di manovra senza che il guidatore (che diventa quindi passeggero-spettatore) sfiori pedali o volante. La IBM ha realizzato il sistema Watson che è in grado di rispondere a domande espresse in un linguaggio naturale e di elaborare soluzioni concrete a problemi complessi che presuppongono conoscenze specialistiche. La prima applicazione è stata realizzata in campo medico con particolare riferimento alle diagnosi. È questa un'attività complessa che presuppone l'elaborazione da parte del medico umano di una sterminata quantità di dati in relazione al caso concreto che gli si presenta. Il sistema Watson è in grado di processare una quantità di dati tali che nessun essere umano singolo e gruppo di essere umani sarebbero in grado di vagliare. Sulla base di una simile analisi, il sistema è poi in grado di selezionare i dati rilevanti, astraendoli dalla massa sterminata di quelli disponibili, e adattando la ricerca alle peculiarità del caso sottoposto all'esame. In tal modo il sistema migliora la diagnosi, migliorano le possibilità di cura, fa diminuire i falsi positivi.

Tra le molte capacità di Watson vi è anche quella di saper leggere i flussi di tutti i post di Facebook e tutti i tweet che vengono pubblicati; tale capacità è usata dalle aziende per anticipare le tendenze del mercato.

[7] Testi di riferimento scientificamente riconosciuti sono, tra i molti: Christopher D. Manning, Prabhakar Raghavan, Henrich Schueze Introduction to Information Retrieval, Cambridge University Press, 2008; J. Kleinberg and E. Tardos. Algorithm Design. Pearson Education (Paperback), 2013.

Nei mercati finanziari, già da tempo gli intermediari offrono consulenze e attività di acquisito di prodotti finanziari basati sull'attività esclusiva di un procedimento informatico, senza l'assistenza o la mediazione di un operatore umano[8].

Il successo di queste applicazioni già in essere è decretato dagli stessi utenti consumatori o operatori interessati. Ciò dimostra pragmaticamente che i risultati cui perviene l'applicazione dell'IA trovano riscontro nel crescente consenso sociale che i servizi sopra richiamati conseguono.

Dunque, ferma l'esigenza che l'ordinamento garantisca quelle cautele, essenzialmente riferite alla protezione dei dati personali, in occasione delle attività di trattamento dei dati che l'applicazione di tali tecnologie comportano, queste paiono nondimeno destinate a un sempre maggior successo.

Il successo è governato e trainato dai saperi tecnici ed è sostenuto dai risultati empiricamente verificati. I procedimenti di decisione algoritmica sono usati dal mercato e anzi per il loro miglioramento le imprese investono risorse immani, semplicemente perché si constata che funzionano, ovvero ottengono i risultati che ci si è prefisso di realizzare.

Anche le pubbliche amministrazioni si stanno progressivamente aprendo alle applicazioni dell'I.A soprattutto riguardo ai servizi accessori all'esercizio delle proprie competenze.

Si va, ad esempio, dalla gestione di dati raccolti mediante un apparato di sensori presenti sulle autostrade al fine di anticipare e gestire i flussi di traffico, alla gestione delle domande di sussidi e aiuti di carattere sociale; alla elaborazione di portali dialoganti in lingua umana per rispondere ai quesiti più frequenti in relazione alle diverse competenze amministrative; ancora, si possono ricordare sistemi di prevenzione degli incendi negli edifici; i sistemi di valutazione predittiva della sostenibilità dei fondi pensione; i sistemi per gestire la trattazione di casi seriali (trasferimenti nel pubblico impiego; gestione e decisione di domande relative ad autorizzazioni ecc.); i sistemi idonei a elaborare e gestire procedure di gara pubbliche per l'individuazione delle imprese con cui la pubblica amministrazione potrà negoziare; i sistemi in grado di fare valutazioni sulla tendenza a delinquere di un certo soggetto o sulla sua tendenza a fuggire; sistemi per gestire i contenziosi o, in genere, i dubbi relativi all'applicazione della legge a casi concreti, in relazione al presumibile

[8] Su tali aspetti F. Mattassoglio, *Algoritmi e regolazione. Circa I limiti del principio di neutralità tecnologica*, in Riv. della regolazione dei mercati, 2018, fasc.2.

comportamento delle corti giudiziarie pronosticato sulla base della raccolta e dell'analisi dei precedenti[9].

In definitiva, potenzialmente l'IA pare applicabile a tutte le attività amministrative sinora di fatto riservate all'intervento esclusivamente umano. Esistono, peraltro, già applicazioni dell'IA anche nel settore giudiziario.

I vantaggi sono tangibili in termini di potenziamento dell'efficienza dei vari servizi pubblici, maggiore garanzia di imparzialità, velocità, accuratezza dell'analisi di base e dunque migliore qualità della decisione finale.

Nel momento in cui, tuttavia, queste nuove tecnologie iniziano ad essere applicate al cuore dei processi decisionali dell'amministrazione – alla scelta discrezionale - e dei giudici – la decisione giudiziaria -, sorgono problemi più delicati rispetto all'uso delle medesime nell'attività tra privati: si pensi ad esempio agli *smart contract*; ai servizi di di profilazione della clientela, ai ricordati servizi di consulenza e investimento nei mercati finanziari; agli scambi di beni e servizi su piattaforme mediante l'uso di criptovalute ecc..

L'affidamento a meccanismi di IA delal gestione di transazioni tra privati può essere facilmente giustificata dal fatto che la scelta di avvalersi di tali tecnologie poggia, in ultima analisi, sul preventivo consenso degli interessati alla transazione e incide su interessi disponibili degli stessi, laddove, invece, l'attività della pubblica amministrazione – come anche quelle giurisdizionale - si esplica secondo moduli autoritativi che devono trovare una fonte di legittimazione nei sempre validi principi della giustificazione dell'esercizio del potere, della riferibilità soprattutto della scelta discrezionale ad un organo democraticamente legittimato, del contraddittorio con i

---

[9] Sul punto sono interessanti le applicazioni sviluppate in Argentina su cui si veda, J.G. Corvalán, *Administración Publica digital e inteligente: trasformaciones en la era de la inteligencia artificial*, in Rivista de Direito Econômico e Socioambiental, vol. 8, n.2 maio/agosto 2017, pp.26 -66; su cui anche si può consultare D.U. *Galetta Juan Gustavo Corvalán, Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto, in federalismi.it - n. 3/2019, pp.2-23;*
Le applicazioni dell'IA alla pubblica amministrazione e le riflessioni sulle implicazioni sono all'ordine del giorno in tutti gli ordinamenti. Per citare solo alcune significative esperienze su possono consultare le pagine web del Governo britannico *www.gov.uk/publications/understanding-artificial-intelligense/aguide-to-using-artificial -intelligense-in -the -publi -sector; per quanto concerne l'esperienza della Germania si può consultare il sito www.ki-deutschland.de;* per l'esperienza francese è interessante lo studio, anche perché condotto su incarico del Primo ministro e da un gruppo di esperti di varia estrazione culturale, coordinati dal deputato e matematico Cédric Villani, *For a meaningful artificiale intelligence, towards a French and european strategy,* 2018, reperibile su https://www.aiforhumanity.fr; si vedano poi i documenti elaborati dall'amministrazione degli Stati Uniti a seguito dell'executive order del Presidente Trump dell'11 febbraio 2019 avente ad oggetto "*Maintaining American Leadership in AI*", reperibile su https://www.whitehouse.gov/ai/; infine, si veda il libro bianco elborato dall'AGID *sull'Intelligenza artificiale al servizio del cittadino,* reperibile su https://ia.italia.it/assets/librobianco.pdf.

destinatari del potere, della trasparenza e conoscibilità dei processi decisionali pubblici e, infine, della sindacabilità degli stessi in sede giudiziaria.

Per questa ragione, in tutti gli ordinamenti nei quali si pone il tema della regolazione delle applicazioni dell'IA nell'ambito dei processi decisionali pubblici il dibattito sottolinea con forza queste medesime esigenze.

A seconda delle tradizioni culturali, più o meno use a convivere con lo sviluppo della tecnica, si riscontrano risposte più o meno aperte ai nuovi fenomeni.

Non desta meraviglia allora che in Paesi come Stati Uniti o il Regno Unito, ispirati all'empirismo e alla fiducia nel progresso tecnologico, i governi stessi abbiano già pragmaticamente avviato un ampio dibattito sul punto che coinvolge l'amministrazione, l'accademia, gli esperti di saperi tecnici e i giuristi e, parallelamente, applicano in modo sempre più esteso l'IA, in fondo poggiando su un atteggiamento di fiducia nei confronti dell'innovazione.

Si nota, invece, un approccio più cauto e attento alle conseguenze dell'applicazione dell'IA ad esempio da parte delle istituzioni dell'Unione europea[10]. Nell'ambito dell'Unione poi si osservano rilevanti divaricazioni di approccio anche tra Paesi per molti versi simili.

È il caso, ad esempio, della Francia e dell'Italia. In Francia il tema è certamente all'attenzione delle istituzioni e gli stessi rappresentanti più autorevoli della cultura giuridico amministrativa hanno maturato un approccio consapevole del problema e convinto della opportunità di accompagnare le trasformazioni, senza inibirne le potenzialità. Esemplare in tal senso è la posizione espressa dagli esponenti del Consiglio di Stato[11]. Rilevante è anche la recente legge n. 2019-222 (di programmazione 2018-2022 e di riforma della giustizia) che prevede sanzioni penali per chiunque, raccolga, analizzi e riutilizzi i dati di identità dei magistrati con lo scopo o l'effetto di valutare, analizzare, confrontare o prevedere le loro pratiche effettive o presunte pratiche professionali.

---

[10] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al comitato delle Regioni, L'intelligenza artificiale per l'Europa, COM(2018) 237 final; si veda in particolare il documento sugli Orientamenti etici per un'intelligenza artificiale affidabile, elaborato da un Gruppo di esperti istituito dalla Commissione nel 2018 e costituito da rappresentanti del mondo accademico, dell'industria e della società civile, reperibile su https://europa.eu/rapid/press-release_IP-19-1893_it.htm;

[11] Jean-Marc Sauvé, *Le juge administratif et l'intelligence artificielle*, Discours prononcé lors de la conférence des présidents des juridictions administratives, le vendredi 20 avril 2018 à Rennes, reperibile su https://www.conseil-etat.fr/actualites/discours-et-interventions/le-juge-administratif-et-l-intelligence-artificielle.

In Italia il dibattitto è in una fase più embrionale[12] e si caratterizza per l'estrema cautela della cultura giuridica e per i primi esperimenti di dialogo interdisciplinare.

Se, ad esempio, si arriva ad ammettere l'uso dell'IA per nell'ambito dei procedimenti amministrativi, ma con esclusivo riguardo alle decisioni vincolate, con la conseguente necessaria prospettiva di apertura del sapere giuridico ai saperi tecnici, molteplici perplessità solleva l'applicazione della stessa alla decisione giurisdizionale. Emerge, invece, una sorta di riserva di ultima istanza di sapere giuridico che non dovrebbe contaminarsi con altro e che sarebbe detenuto, protetto e imposto in via esclusiva dal giudice. Questi, secondo alcune prospettive ermeneutiche, assume un ruolo quasi oracolare[13]. In questa prospettiva si dubita quindi che lo strumento informatico possa essere anche solo d'ausilio a simile funzione sovrana consistente appunto nel rendere la giustizia nel caso concreto. L'algoritmo, si afferma, non potrebbe mai avere quella capacità di valutare e soppesare le diverse peculiarità del caso concreto e dunque di garantire la giustizia.

Queste perplessità trovano riflesso in recenti pronunce del giudice amministrativo.

Una decisione del TAR Lazio, sede di Roma (sezione terza bis, Sez. III bis, sentenza del 27.5.2019, n. 6606) ha di nuovo portato alla ribalta il tema delle condizioni di legittimità alle quali è subordinato l'utilizzo degli algoritmi nel procedimento decisionale amministrativo e delle garanzie che chi lamenti una lesione di un proprio diritto possa far valere nei confronti di simili procedure. La pronuncia pare escludere in radice la legittimità dell'uso di procedure informatizzate per assumere decisioni su un numero elevato di soggetti in relazione a cui sussiste un altrettanto elevato numero di variabili da tenere in considerazione ai fini del decidere. Secondo i giudici amministrativi di prima istanza gli "*istituti di partecipazione, di trasparenza e di accesso, in sintesi, di relazione del privato con i pubblici poteri non possono essere legittimamente mortificati e compressi soppiantando l'attività umana con quella impersonale, che poi non è attività, ossia prodotto delle azioni dell'uomo, che può essere svolta in applicazione di regole o procedure informatiche o matematiche*".

[12] Danno conto dello stato del dibattito anche accademico, F. Patroni Griffi, *La decisione robotica e il giudice amministrativo,* Intervento al Convegno "Decisione robotica", organizzato nell'ambito dei Seminari 'Leibniz' per la teoria e la logica del diritto – Roma, Accademia dei Lincei, 5 luglio 2018, reperibile su https://www.giustizia-amministrativa.it/-/patroni-griffi-la-decisione-robotica-e-il-giudice-amministrativo-28-agosto-2018; Alessandra Carleo (a cura di), Decisione robotica, Bologna, 2019.

[13] Sulla critica a queste diffuse teorie dell'interpretazione si veda persuasivamente M. Luciani, *La decisione giudiziaria robotica*, in Rivista AIC, n .3 del 2018, pubblicato il 30.9.2018, reperibile su https://www.rivistaaic.it

Su analoga questione il Consiglio di Stato (Sezione sesta, sentenza del 8.4.2019, n. 2270) aveva in realtà espresso una posizione più aperta: ammettendo in astratto la legittimità della c.d. decisione algoritmica e considerando anzi il software stesso come "atto amministrativo informatico". In concreto la legittimità di una simile decisione, secondo il giudice di ultima istanza, dovrebbe essere tuttavia subordinata alla conoscibilità - anche per i profani non informatici - dell'algoritmo in tutti gli aspetti "…*dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fine di poter verificare che gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare - e conseguentemente sindacabili - le modalità e le regole in base alle quali esso è stato impostato*".

Inoltre, il Consiglio di Stato nel riconoscere che"…*l'utilità di tale modalità operativa di gestione dell'interesse pubblico è particolarmente evidente con riferimento a procedure seriali o standardizzate, implicanti l'elaborazione di ingenti quantità di istanze e caratterizzate dall'acquisizione di dati certi ed oggettivamente comprovabili e dall'assenza di ogni apprezzamento discrezionale*", di fatto circoscrive l'utilizzabilità delle medesime informatizzate solo alle decisioni vincolate. Nel caso di attività discrezionale esisterebbe una sorta di riserva di valutazione umana.

Sembra doversi osservare che, nel complesso, alla luce delle prime indicazioni della dottrina e di questi primi arresti giurisprudenziali, emerge un certo disorientamento che a volte si connota di vera e propria diffidenza nei confronti delle decisioni algoritmiche se applicate nell'ambito dei processi decisionali dell'amministrazione e, a maggior ragione, nelle decisioni giurisdizionali.

Ora un simile atteggiamento pare da attribuirsi a un condizionamento di natura culturale che induce in particolar modo il sapiente in diritto per eccellenza, come detto il giudice, a evitare qualunque confronto con altri saperi, a non condividere con nessun'altro l'esercizio del proprio potere e a diffidare, in ultima analisi, delle innovazioni tecnologiche.

In realtà, a intendere bene il funzionamento dei sistemi di IA, pare che essi possano apportare, alla luce delle applicazioni cennate, relative a esperienze che si realizzano ormai in tutto il mondo, grandi vantaggi sia all'attività amministrativa, ma anche a quella giurisdizionale.

Con riguardo all'attività amministrativa di natura vincolata non sembra possano esserci particolari ostacoli. Riguardo l'attività discrezionale occorre distinguere. Infatti, mentre potrebbe essere di grande supporto al decisore umano una previa analisi fattuale, dei precedenti e delle prassi amministrative svolta da un applicativo di IA, più complesso appare il ruolo del medesimo nell'ambito della ponderazione tra i vari interessi pubblici e privati in gioco che costituisce il cuore della discrezionalità pura tradizionalmente intesa. Ponderazione e decisione che non possono che trovare fondamento in una scelta da ricondurre a un decisore umano democraticamente legittimato. Non v'è dubbio però che l'IA potrebbe essere di grande aiuto nella fase istruttoria di un procedimento volto all'adozione di una decisione discrezionale.

In altri termini, il processo che conduce l'IA all'elaborazione di problemi complessi e all'individuazione dei risultati presenta oggettivi margini di superiore affidabilità rispetto alle valutazioni meramente umane e, pertanto, non si vede la ragione per cui tali strumenti non possano essere impiegati anche a supporto dell'istruttoria finalizzata alle scelte discrezionali.

Il problema vero risiede nella corretta costruzione dell'algoritmo, nell'assenza di incidenti durante il suo funzionamento e nella correttezza qualitativa dei dati inseriti per l'elaborazione[14]: sono questi i momenti nei quali il controllo umano diviene veramente insostituibile e l'interazione tra il sapere giuridico e quello tecnico informatico davvero essenziale.

Anzi è da ritenere che proprio il dialogo, oggettivato nella motivazione del provvedimento discrezionale, tra le acquisizioni dell'IA e la scelta assunta dal decisore umano consentirebbe di attingere un più alto livello di garanzia per i diritti dei singoli. La scelta discrezionale umana che dovesse essere assunta in contrasto con le risultanze istruttorie elaborate dall'algoritmo e in assenza di oggettive ragioni riconducibili a una delle cause di malfunzionamento richiamate, dovrebbe essere adeguatamente motivata.

In fondo sembra andare in questa direzione 22 del nuovo Regolamento europeo in materia di protezione dei dati personali che, se è vero che afferma, al primo paragrafo, che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca

[14] I casi da cui le pronunce ricordate nel testo traevano origine riguardavano ad evidenza situazioni nelle quali la decisione amministrativa era stata affidata a software assolutamente inadeguati, mal concepiti e alimentati per giunta con dati sbagliati. Non sarebbe corretto pertanto inferire da queste esperienze, l'inadeguatezza strutturale delle decisioni algoritmiche per l'attività amministrativa.

effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, ma poi ai paragrafi successive ammette la possibilità in un novero ampio di situazioni, seppur con alcune cautele.

Analoghe considerazioni possono essere svolte per l'attività giurisdizionale.

Già sono in uso algoritmi che sostengono il lavoro di giudici, anche di ultima istanza[15].

Sull'applicazione della decisione algoritmica alla decisione giurisdizionale sono state sollevate essenzialmente tre obiezioni principali. La prima si basa sulla convinzione che un algoritmo – anche se ben congegnato – non potrebbe mai essere in grado di apprezzare l'unicità irripetibile del caso concreto[16]. Ma questa obiezione, da un lato, prova troppo. Infatti, a trarre le conseguenze ultime di questa tesi si giungerebbe alla assurda conseguenza che la regola di ogni caso concreto sarebbe in realtà decisa, di volta in volta, dal giudice che è chiamato ad applicarla e nel momento in cui la applica. Simile esito contraddice le più elementari acquisizioni della cultura

[15] Si pensi al sistema CED della Corte di Cassazione italiana, non accessibile al pubblico; si pensi all'uso da parte di alcune corti statunitensi americane di un algoritmo in materia penale che è in grado di elaborare previsioni del rischio di recidiva del condannato che incidono sul suo trattamento sanzionatorio. Si tratta di COMPAS (Correctional Offender Management Profiling for Alternative Sanctions). È un algoritmo proprietario, il cui meccanismo di funzionamento – che si basa sulla raccolta e sull'elaborazione dei dati emersi dal fascicolo processuale e dall'esito di un test a 137 domande a cui viene sottoposto l'imputato riguardanti età, attività lavorativa, vita sociale, grado di istruzione, legami, uso di droga, opinioni personali e percorso criminale – non è pubblicamente noto. Sulla legittimità dell'uso di simili procedure decisionali è intervenuta una pronuncia della Corte Suprema del Wisconsin, case 2015AP157-CR, July 13, 2016, reperibile su https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690. La Corte ha ammesso la legittimità dell'uso degli algoritmi nelle decisioni giudiziarie indicando anche le condizioni che tuttavia devono essere rispettate per evitare di incorrere nella violazione del *due process*. In primo luogo, le risultanze dell'elaborazione algoritmica non possono da sole costituire la ragione per imporre una decisione giudiziaria; si legge infatti che "*A COMPAS risk assessment is only one of many factors that may be considered and weighed at sentencing*" e poi l'interessato deve avere la possibilità di verificare ed eventualmente contestare l'accuratezza e la pertinenza dei dati inseriti per l'elaborazione. In altri termini, la decisone giudiziaria può basarsi anche su COMPAS ma le elaborazioni di questo non possono costituire l'unica base di decisione; inoltre, la necessità di individualizzare il giudizio impone di controllare attentamente se il caso concreto possa effettivamente rientrare nella serie statistica individuata dall'algoritmo.
Ancora si possono citare le esperienze della Corte suprema di Buenos Aires, della Corte costituzionale della Colombia e della Corte interamericana dei diritti umani, sui cui si veda la nota n.8. Nelle fonti ivi citate si dà conto di Prometea, un sistema di intelligenza artificiale che consente la soluzione di casi giudiziari più semplici e ripetitivi in pochi secondi. Il sistema ha dimostrato avere un elevato tasso di successo – in termini di conformità delle decisioni assunte a diritto accertato anche successivamente dai giudici umani e ha ridotto sensibilmente il lavoro delle Corti.

[16] Simile presupposto pare essere alla base della regola inserita nel nostro codice di procedura penale all'art.220, comma 2, secondo cui non è ammessa perizia per stabilire l'abitualità o la professionalità nel reato, la tendenza a delinquere, il carattere e la personalità dell'imputato e in genere le qualità psichiche dell'imputato indipendenti da cause patologiche. Una simile regola non sembra poggiare su basi scientifiche oggettive, ma sul timore di utilizzare procedure informatizzate in queste valutazioni. La solitudine del giudice umano è pregiudizialmente ritenuta preferibile.

giuridica degli ordinamenti democratici secondo cui il giudice non dovrebbe porre la regola che per lui dovrebbe essere un dato eteronomo[17]. La tesi in esame, dall'altro lato, presuppone che un algoritmo non possa essere in grado di elaborare e ricondurre a sistema i dati che individuano il caso concreto al pari di un essere umano; tuttavia, tale presupposizione appare smentita dai fatti e dalle potenzialità dell'I.A. sopra ricordate.

La seconda critica attiene alla circostanza che l'applicazione di algoritmi predittivi a volte ha dato luogo alla amplificazione di pregiudizi derivanti dai dati immessi a monte nell'elaborazione; ne è risultato, ad esempio, nella prassi decisionali di alcune corti americane, che i neri schedati per qualche crimine sono stati ritenuti soggetti alla recidiva secondo un grado di probabilità più elevato di quello dei bianchi, ma alcune indagini fatte *ex post* hanno clamorosamente smentito le previsioni dell'algoritmo[18]. In tali circostanze, tuttavia, l'obiezione mette in evidenza la necessità di un accurato controllo sui dati che vengono immessi nell'algoritmo: se già essi sono espressione di valutazioni discriminatorie, non giustificate da ragioni oggettive, è evidente che l'algoritmo non potrà che amplificare il pregiudizio. Tale critica sottolinea, quindi, ancora una volta la necessità di un attento controllo dei dati, ma non è tale da inficiare in radice l'utilizzo delle procedure algoritmiche per sostenere anche le decisioni giudiziarie.

La terza critica all'uso dell'IA nell'attività giurisdizionale appare più penetrante e risiede nel fatto che l'algoritmo basato sulla elaborazione dei precedenti avrebbe una tendenza a sclerotizzare la giurisprudenza.

In realtà, però a una più attenta analisi, l'obiezione pare porre un falso problema. Di fronte alla consapevole necessità di cambiare orientamento, sulla pressione delle novità della realtà sociale, il giudice umano avrebbe senz'altro la possibilità di non seguire la proposta dell'algoritmo, ma dovrebbe esplicitamente motivarne le ragioni.

Lo stato dell'arte delle conoscenze non consente di affermare la possibilità di sostituire integralmente la decisone giurisdizionale umana, se non per vicende bagatellari, con la decisione robotica: tuttavia, appare sempre più pressante l'esigenza che anche la decisione giurisdizionale sia assistita dall'IA.

---

[17] Sul punti si rinvia alla necessità di riaffermare la distinzione tra legislazione e giurisdizione argomentata da M. Luciani, *La decisione giudiziaria robotica* cit.

[18] Kehl, Danielle, Priscilla Guo, and Samuel Kessler, *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative, Berkman Klein Center for Internet & Society*, Harvard Law School, 2017.

L'uso dell'algoritmo in funzione di supporto all'attività del giudice farebbe acquisire alla sentenza un sicuro valore aggiunto. Gli interessati al processo e la collettività avrebbero una maggiore sicurezza che il giudice sarebbe messo in condizione di vagliare tutti i formanti del diritto rilevanti, ovvero le norme nazionali, sovranazionali e locali, le prassi amministrative e gli orientamenti giurisprudenziali; inoltre, si avrebbe una maggiore certezza che il giudice sarebbe messo in grado di apprezzare tutti gli elementi del caso e che, quindi, ove ritenesse di discostarsi dalle proposte di soluzione del caso concreto prospettate dell'algoritmo dovrebbe convincentemente motivare.

I vantaggi dell'ausilio dell'IA alla decisione giurisdizionale umana sono evidenti: maggiore prevedibilità delle decisioni; maggiore garanzia della parità di trattamento tra i cittadini, maggiore garanzia della più completa ricognizione del quadro normativo rilevante, sempre più complesso e frastagliato; individuazione immediata delle contraddizioni del ragionamento; maggiore garanzia di imparzialità.

Chi abbia la ventura di frequentare i tribunali, sa quanto le decisioni giudiziarie siano spesso il frutto di meri errori inconsapevoli del giudice umano che il sostegno di un algoritmo avrebbe evitato. I nostri uffici giudiziari poi sono spesso caratterizzati dalla assenza di consapevolezza tra gli stessi giudici addetti circa gli orientamenti presi in casi simili dai loro colleghi di altre sezioni o della medesima sezione dello stesso Ufficio; i giudici di prima istanza spesso non conosceranno mai l'esito dell'impugnazione delle loro sentenze.

L'uso adeguato di tecnologie informatiche consentirebbe di superare questi problemi e agli stessi giudici di avere maggiore consapevolezza del loro operato a beneficio dell'alto servizio che svolgono per la collettività.

3.Alcune conclusioni: necessità di dialogo interdisciplinare e ripensamento del metodo giuridico.

Per illustrare il tema dei saperi di cui oggi l'amministrazione ha bisogno e per comprendere come si pone oggi il rapporto tra sapere giuridico e saperi tecnici nell'attività amministrativa o comunque nell'esercizio delle funzioni pubbliche, si sono prese le mosse dalle conseguenze di alcune delle innovazioni portate dalla c.d "quarta rivoluzione industriale".

Si è preso in considerazione l'impatto dei *big data* e delle procedure di elaborazione degli stessi ai rapporti tra Stati, tra Stati e grandi imprese e tra Stati e

cittadini sottoposti alla regolazione. Si è notato che le nuove tecnologie hanno comportato, da un lato, l'accrescimento del potere dei grandi Stati e delle grandi imprese: è un potere ad oggi non regolato ed espressione della forza del fatto.

Tale realtà esigerebbe un potenziamento delle strutture di conoscenza proprie degli Stati al fine di conservare margini di sovranità effettiva nei confronti degli altri Stati e delle grandi imprese detentrici e dei gestori dei *big data*; esigerebbe poi anche il potenziamento delle strutture conoscitive dei parlamenti che oggi non sembrano in grado di sindacare efficacemente l'attività dei governi nella gestione dei *big data* svolta dalle varie articolazioni dell'amministrazione stessa a tutela dei cittadini.

Sotto altro profilo, Stati, amministrazioni e imprese sono oggi più vulnerabili di ieri, in quanto i sistemi informatici su cui basano la propria attività sono interconnessi attraverso la rete internet e, per ciò solo, sono esposti ad abusive intromissioni dall'esterno.

Il problema diventa di grande rilievo quando sono in gioco servizi di grande rilievo economico e sociale. La regolazione approntata per questi problemi delinea una tecnica di vigilanza pubblica nuova (definita *by design*) che poggia sulla assenza di standard predefinibili e stabili che possano costituire un parametro puntuale di comportamento; sul principio dell'autovalutazione del rischio che grava sui soggetti obbligati a garantire la sicurezza dei sistemi e del controllo cooperativo tra autorità e soggetti controllati. Tali nuovi approcci regolatori, invalsi non solo per la *cyber security*, ma anche, ad esempio, per la regolazione delle operazione totalmente robotizzate che già si svolgono nei mercati finanziari, esigono il supporto di competenze tecniche specialistiche e giuridiche tra loro dialoganti.

La stessa tradizionale frammentazione delle competenze, presente nell'ambito dell'apparato amministrativo, appare oggi inadeguata a cogliere le sfide delle nuove tecnologie e le implicazioni che queste ultime comportano nella vita sociale ed economica; ne consegue che non solo sono necessari diversi saperi tra loro dialoganti, ma anche una più intensa e costante collaborazione tra le diverse amministrazioni per consentire una più piena comprensione dei fenomeni oggetto di regolazione[19].

Si sono poi analizzate le problematiche inerenti l'uso dell'IA nell'ambito dell'attività amministrativa e giurisdizionale. Dall'analisi sono scaturite osservazioni

[19] Si pensi in questo senso all'Indagine conoscitiva congiunta avviata da AGCOM, AGCM e Garante per la protezione dei dati personali sul tema dei big data che nel giugno del 2019 ha già prodotto alcuni risultati provvisori, reperibile su www.agcm.it

sulla tipologia e sul *modus* operandi dei saperi necessari per l'applicazione di queste nuove tecnologie.

Da questi esempi significativi si possono trarre alcune conclusioni sul tema.

La tendenza attuale, come detto, esige l'interdisciplinarietà degli approcci tra i saperi di cui l'amministrazione si avvale.

Inoltre pare emergere un esigenza per la quale la cultura giuridica dovrebbe aprirsi di più alle istanze di razionalizzazione portate dall'applicazione delle nuove tecnologie se vuole adempiere al proprio ruolo di garanzia dei diritti delle persone. La tecnologia attuale pone con grande forza la scommessa del necessario dialogo tra il diritto e le scienze dell'informazione evolute.

L'uno e le altre sono linguaggi che devono convergere tendenzialmente: una società nella quale si afferma sempre di più il potere della tecnologia che è espressione di una razionalità obiettiva, proprio per conservare i tratti di umanità, deve elaborare un diritto che sia espressione anch'esso di una razionalità controllabile e obiettivata, almeno tendenzialmente.

Gli sviluppi dell'IA, anziché essere guardati con sospetto dallo studioso del diritto, dovrebbero essere adeguatamente inclusi nelle sue riflessioni e utilizzati per rendere il linguaggio giuridico – nei vari atti in cui si declina e cioè le leggi, gli atti amministrativi e le sentenze - più trasparente, più comprensibile, meno contraddittorio, più coerente con i dati fattuali su cui pretende di incidere: in una parola più razionale.

L'approccio suggerito dall' "Ars combinatoria", pubblicata nel 1666 da Leibniz, oggi pare essere una prospettiva di studio e sperimentazione da riprendere con rinnovato vigore.

L'etica nell'era del digitale[20] si potrà affermare solo se il linguaggio giuridico – a cominciare dalla legislazione - riuscirà, per quanto possibile, ad avvicinarsi alla controllabilità intersoggettiva del formalismo logico che è alla base dell'evoluzione sorprendete e non certo esaurita dell'IA.

Non si ignorano gli ostacoli fattuali che l'amministrazione nazionale incontra nell'adeguarsi alla situazione. La digitalizzazione, a più di trenta anni dalla sua formalizzazione legislativa, resta ancora un obiettivo da realizzare; le immense potenzialità consentite dalle nuove tecnologie non sono sfruttate. Purtroppo il *computer* tutt'ora per la gran parte delle amministrazioni ha semplicemente sostituito

[20] Su cui sono fondamentali le riflessioni di L. Floridi, *Infosfera, Etica e filosofia nell'età dell'informazione*, Torino, 2009.

e potenziato le macchine da scrivere. Mancano risorse strumentali e umane idonee. Riguardo a queste ultime non aiuta certo l'età media dei dipendenti pubblici (50 anni, tra le più alte d'Europa), nè i meccanismi di ingresso e selezione appaiono congrui, perché ancora eccessivamente basati su criteri di selezione che prediligono una conoscenza giuridico formale.

È rimasto sinora assente un forte *commitment* politico volto ad attuare più incisive politiche di potenziamento delle capacità e degli usi delle tecnologie nella pubblica amministrazione.

Resta però la necessità per l'amministrazione di adeguare la disciplina e le modalità di reclutamento delle professionalità idonee a consentire quella insostituibile funzione di *governance* pubblica di un processo di tale rilevante impatto. Se, come detto, la formazione giuridico formale che caratterizza la maggior parte dei funzionari pubblici non è palesemente in grado da sola di fronteggiare simili sfide, neanche appare utile la mera moltiplicazione e giustapposizione di saperi specialistici, intesi come ambiti chiusi che non comunicano tra loro. Gli sviluppi dell'intelligenza artificiale e delle nuove tecnologie in genere impongono un dialogo serrato e anzi una sinergia tra i settori scientifici e tecnici; l'interdisciplinarietà, da non intendersi come sterile eclettismo o superficiale genericità, dovrà guidare sempre più le attività dell'amministrazione.