Intelligenza artificiale e protezione dei dati personali: problemi di metodo e di procedura*

di Rolando Tarchi e Andrea Gatti

Abstract: *Artificial intelligence and the protection of personal data: methodological and procedural problems* - The constitutional challenges posed by AI systems implicate a range of rights and interests (from personal freedom, equality and non-discrimination, health protection, to the proper functioning of democratic institutions). At the core of all these issues lies the protection of personal data as a fundamental right, and at least two other fundamental values of general importance shared by all the Western constitutional tradition: individual identity and personal freedom. The aim of this paper is to summarise and analyse, in a comparative perspective, how the different strategies for the AI governance implemented by the European Union and by some key-US states affect these constitutional interests and are consistent with the goals they seek to achieve.

Keywords: Artificial intelligence; Data protection; Privacy; European union; United states; Fundamental right

1. Le sfide dell'Intelligenza artificiale con riferimento alla protezione dei dati personali e agli altri diritti fondamentali

La crescente espansione dell'orizzonte tecnologico si impone oggi come una componente inevitabile dell'esperienza umana. La nostra vita quotidiana è sempre più dipendente da interazioni con macchine, strumenti e sistemi di crescente complessità e autonomia. L'onnipresenza della computerizzazione permea tutte le sfere dell'attività umana quotidiana, e pur essendo resa evidente nelle illimitate funzionalità degli smartphone, si esprime anche in numerose forme più istituzionalizzate: programmi GPS, sistemi di social scoring, diagnosi mediche, algoritmi commerciali e di trading nel commercio e nella finanza[1]. La tecnologia stessa sta ridefinendo le modalità dell'esistenza umana, permette l'emergere di fenomeni di ibridazione tra umano e macchina, tra naturale e artificiale, in una dinamica di scambio bidirezionale possibile sia perché le macchine assumono caratteristiche

[1]* Il lavoro è frutto di riflessione congiunta degli *autori*; tuttavia, la stesura dei paragrafi 2, 2.1, 3 e della postilla è da attribuire a Rolando Tarchi, quella dei paragrafi 1, 2.2, 4, 4.1, 4.2, 5, e 6 ad Andrea Gatti.

Ex multis, M. Cantero Gamito, M. Ebers (a cura di), *Algorithmic Governance and Governance of Algorithms: An Introduction. Legal and Ethical* Challenges, vol. 1 (*Data Science, Machine Intelligence and Law*), Cham (CH), Springer, 2021.

DPCE online
ISSN: 2037-6677

umane – e rivendicano prerogative quali soggettività, pensiero, capacità decisionale e di apprendimento[2] – sia perché l'uomo si "meccanicizza", i suoi processi cognitivi si trasformano in modelli matematici, finendo per riflettere un'immagine di sé nei dispositivi che crea[3]. Permettendoci di parafrasare anche noi un autore citatissimo come Luciano Floridi, possiamo dire che Turing ha trasformato la nostra concezione antropologica tanto profondamente quanto figure storiche quali Cartesio, Darwin o Freud[4]. In un contesto dove si venera un *pantheon* di divinità digitalizzate, l'uomo ha creato uno strumento per interpretarle e, in qualche modo, governarle: l'algoritmo[5]. I valori di probabilità calcolati tramite metodi matematici, che forniscono indicazioni sul comportamento futuro, sono in effetti simili in tutto e per tutto ad un responso oracolare: l'algoritmo fornisce, sì, risposte ma poche spiegazioni, e le conclusioni tratte dalle analisi appaiono talvolta ugualmente oscure (sibilline) anche per i suoi moderni sacerdoti[6].

Proprio perché tali mutamenti hanno sconvolto profondamente il mondo del diritto, quest'ultimo si trova impegnato nell'assimilare e talvolta nell'anticipare le sollecitazioni del progresso tecnico-scientifico.

Come sappiamo, l'avvento dell'IA ha trasformato i dati forniti da individui e accumulati nel tempo in un autentico tesoro, particolarmente appetibile soprattutto per le aziende poiché permette loro non solo di conoscere, archiviare e trattare una quantità infinitamente più grande informazioni, ma soprattutto di indagare ipotesi del tutto inconoscibili a intelligenze naturali, scoprendo informazioni che vanno ben al di là delle richieste formulate dal programmatore[7].

Le sfide che si pongono in tema di Intelligenza artificiale con riferimento alla materia del diritto costituzionale coinvolgono una serie di diritti e di interessi (dalla libertà della persona, all'eguaglianza e non-

[2] Questa mescolanza di terminologie e significati porta al progressivo sfumare delle distinzioni tra natura e artificio, culminando in una "rivoluzione simbolica" che permea ogni aspetto della vita umana. Così già V. Frosini, *Cibernetica, diritto e società*, Milano, 1968, 104-105, il quale parlava del calcolatore
elettronico come «*simia hominis*», programmato per «mimare» il pensiero umano.

[3] Sulle «mutazioni antropologiche» nell'era delle macchine, si rinvia a S. Rodotà, *Il diritto di avere diritti*, Bari-Roma, 2012, 312 ss., spec. 313.

[4] L. Floridi, *Pensare l'infosfera. La filosofia come design concettuale*, Milano, 2020, 130.

[5] A. Vespingani, R. Rijtano, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, Roma, Il Saggiatore, 2019.

[6] Un responso, che, come quello dell'oracolo, "ha sempre ragione, pur non dando mai ragioni", così A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Biolaw Journal*, n. 1/2019, 63-98, sepc. 64.

[7] È ciò che rende possibile il c.d. *Discovery Driven Approach*: invece di limitare l'analisi alla verifica dell'ipotesi iniziale, con l'approccio di scoperta vengono analizzate tutte le caratteristiche disponibili nel database: l'età dell'interessato, ma anche il luogo di residenza, il sesso, l'istruzione, il colore dei capelli e così via, finendo per scoprire correlazioni impensabili all'inizio dell'indagine, come ad esempio quella tra il consumo di biscotti, il luogo di residenza e la solvibilità di un mutuo (Cfr. A. Canhoto, J. Backhouse, *General Description of the Process of Behavioural Profiling*, in Hildenbrandt, S. Gutwirth, *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, 2008, 47-63, spec. 48 ss.). Questo permette dunque di rilevare caratteristiche personali che nemmeno l'interessato sa di avere.

discriminazione, alla tutela della salute fino al corretto funzionamento delle istituzioni democratiche), ma alla base tutto, quale diritto in qualche modo prodromico, sta la protezione dei dati personali e almeno due altri valori ad essa sottesi, di portata generale e comuni alle differenti esperienze costituzionali occidentali: quello dell'identità del soggetto (tra cui vanno annoverati anche i dritti alla personalità) e la libertà personale.

Ad oggi sono due i macro-temi di primario interesse per l'indagine, il primo riguarda la *governance* dei dati, vale a dire le regole volte a garantire che i dati siano sicuri, privati, accurati, ma anche disponibili, utilizzabili e interscambiabili, il secondo "la *governance* della *governance*", diciamo così, cioè il modo in cui viene concepita la struttura di governo dell'AI.

In questo contributo vorremmo però evitare di approfondire gli aspetti legati al merito della disciplina della tutela dei dati personali di fronte alla intelligenza artificiale per concentrarci invece sugli aspetti metodologici e procedurali. Il particolare riferimento va, ovviamente, all'ordinamento europeo e al recentissimo Regolamento sull'intelligenza artificiale (comunemente conosciuto come AI Act).

2. Questioni di metodo e rilievo della comparazione

Le undici relazioni che abbiamo ascoltato in questa giornata, peraltro già discusse nei loro contenuti dagli interventi dei colleghi Lucia Scaffardi e Andrea Pin, affrontano una pluralità di argomenti che non è possibile riprendere in questa sede; posso solo complimentarmi con loro per la cura che hanno posto nell'elaborazione dei loro contributi, esposti con chiarezza e comprensibili a persone che, come il sottoscritto, non possono certo dirsi esperti della materia. Riteniamo sia più utile, in queste sintetiche riflessioni che proponiamo, di limitarci a considerare alcune questioni di carattere macro, riferibili in primo luogo al metodo di studio da utilizzare per l'approfondimento di questi fenomeni, che, in buona misura, richiedono ancora di essere messi a fuoco e non costituiscono per il momento un patrimonio di conoscenza acquisito dalla scienza giuridica nel suo complesso. Riflessioni, generali e metodologiche, che almeno in parte sono state anticipate nell'introduzione di Ginevra Cerrina Feroni, da noi pienamente condivise, che ci ricorda anche l'enorme potenziale economico dell'A.I., ormai fattore determinante per la crescita del PIL. Dobbiamo aggiungere come il giurista venga sfidato a percorrere un terreno impervio (che richiede conoscenze extra giuridiche), in continua evoluzione, con un progressivo spostamento in avanti dettato dallo sviluppo, che ormai pare inarrestabile, delle nuove tecnologie e, in particolare, dell'intelligenza artificiale che tengono a progredire costantemente a fronte di un sistema di regole e di controlli piuttosto lacunoso, che arranca per tenere il ritmo di questa progressione e deve sempre inseguire. A questo riguardo si profila, preliminarmente, un problema di carattere definitorio riferito alla formula «intelligenza artificiale». Nell'Enciclopedia italiana si utilizza questa definizione: «la capacità di un computer o di un robot di eseguire compiti tradizionalmente eseguiti da esseri intelligenti. Realizzare l'A.I. significa quindi sviluppare sistemi dotati delle funzioni tipiche dei processi intellettivi umani, quali percepire, associare un significato e ragionare su ciò che si

DPCE online
ISSN: 2037-6677

percepisce, decidere, compiere azioni, comunicare o apprendere dall'esperienza», cui fanno poi seguito una serie di esemplificazioni che tengono conto degli sviluppi più recenti. Sul piano linguistico non pare si sia andati molto avanti rispetto alla definizione «di intelligenza delle macchine" utilizzata nel 1956 dal già ricordato Alan M. Turing e di fronte a questa genericità non possiamo che rimanere insoddisfatti, ma è questa la base da cui dobbiamo prendere le mosse.

Tornando al rilievo della dimensione giuridica, ad essa non possiamo comunque mai rinunciare, essendo comunque coinvolta la sfera dei diritti fondamentali delle persone (umane e non artificiali), che possono certo trarre importanti benefici dall'uso di tecnologie sempre più sofisticate, ma, per questo, sono costrette a pagare il prezzo di invasioni nella sfera della loro privacy; invasioni difficilmente contenibili ex ante e non sempre rimediabili *ex post*.

La dimensione globale e transnazionale del fenomeno ha immediate ripercussioni sulla metodologia di studio che i giuristi devono adottare; per noi l'unica modalità possibile e utile e quella del ricorso agli strumenti ed alle tecniche proprie della comparazione giuridica, da intendersi non soltanto quale ausilio in termini di conoscenza (secondo la nota indicazione della prima tesi di Trento), quanto, piuttosto, secondo l'impostazione di Mauro Cappelletti è necessario andare alla ricerca di soluzioni, per finalità di politica del diritto; solo il confronto tra soluzioni diverse offre la possibilità di individuare quella più utile (la *promising solution*) per adottare le modifiche necessarie e colmare le insufficienze esistenti. Una concezione del metodo comparativo, quella appena richiamata, che propone, inoltre, un allargamento degli oggetti e delle esperienze da porre a confronto, in una visione che tende a divenire globale, quasi universalistica.

Tornando alle questioni di cui dobbiamo occuparci più direttamente, la comparazione tra esperienze diverse diventa quindi necessaria per capire come viene concepita l'architettura almeno dei principali sistemi, considerati nella loro dimensione normativa e di *policy*, con un'attenzione particolare, all'importanza che si vuole riconoscere ai diritti fondamentali nel loro complesso ed alla posizione che vengono ad occupare, con un focus specifico dedicato al diritto alla protezione dei dati personali.

In una materia così nuova e autenticamente transnazionale la comparazione giuridica si pone, quindi, in primo luogo come un ausilio per tutti gli operatori giuridici che devono affrontare questioni continuamente nuove: i legislatori chiamati ad aggiornare le regole; le autorità di garanzia preposte alla regolazione, in un dialogo costante tra *hard* e *soft law*; i giudici, cui compete il bilanciamento finale tra i differenti interessi in gioco; fino agli studiosi che possiedono le competenze per decifrare le nuove problematiche che si affacciano sulla scena e sono in grado di elaborare idee e proporre riflessioni critiche a legislatori e giudici. via e ciò ha permesso una mutua comprensione non solo fra culture giuridiche non omogenee (l'UE, l'USA e la Cina, appunto)

Ma il coinvolgimento di tutti i formanti diventa poi un elemento necessario per consentire una circolazione dei modelli rapida e complessiva: prima ancora di permettere lo sviluppo di riflessioni di portata generale emergenti dal confronto tra i diversi approcci e la loro proiezione temporale, l'indagine comparata facilita la stessa comprensione dei problemi che, a

livello di singola esperienza, possono restare sottotraccia e accettati acriticamente. Questo vale anche con riguardo al confronto tra sistemi tra loro eterogenei quanto a tradizione giuridica sottostante; in questa sede il riferimento è agli USA, la Cina e l'Unione europea le cui rilevanti difformità consentono di individuare quello che si configura come il modello dal rendimento migliore quanto almeno a tutela della libertà personale.

Va anche considerato che in materia di *privacy* e Intelligenza artificiale il ricorso alla comparazione si lascia preferire non soltanto per ragioni legate al peculiare strumentario metodologico che hanno in dote i comparatisti quali cultori di un settore autonomo di studi; per quanto privilegiati sotto questo profilo, essi non possono rivendicare l'esclusività del metodo, che, al fine di consentire l'identificazione di percorsi analitici tali da far emergere visioni di portata generale dei fenomeni giuridici senza oscurare le differenze tra le esperienze, deve essere utilizzato anche dagli studiosi delle altre discipline. Una conferma diretta è offerta proprio da questo seminario, le cui relazioni, siano esse state sviluppate con la sensibilità propria del privatista rispetto a quella del pubblicista, piuttosto che del processualista, non trascurano i necessari riferimenti comparatistici, con la presa in esame di una pluralità di sistemi anche piuttosto distanti tra loro. Per concludere su questo punto dobbiamo osservare come nell'ambito considerato l'approfondimento dei temi richieda inevitabilmente una doppia interdisciplinarità: interna alla scienza giuridica la prima, dettata dal superamento dei tradizionali confini materiali, con contaminazioni di conoscenze tecnologiche la seconda, indispensabili per sviluppare ragionamenti consapevoli riguardo alle conseguenze determinate dal progresso scientifico[8].

Altro aspetto che sottolinea il ruolo di bussola offerta al dibattito sulla regolazione dell'intelligenza artificiale dal diritto comparato riguarda la possibilità "spaziale" e "temporale" della comparazione; intanto, oltre che sul tradizionale piano orizzontale, tra ordinamenti giuridici o tra macro-sistemi collocati sul medesimo piano, la comparazione deve essere sviluppata anche nella sua dimensione verticale nei casi in cui siano interessati sistemi multilivello, come nel caso dell'Unione europea con riguardo agli Stati membri o dell'ordinamento federale). Come sarà meglio precisato *infra* (§ 2.2), in questi contesti convive un doppio livello di regolazione normativa, seppure con una qualche inversione delle rispettive posizioni, con l'approvazione di normative generali da parte dell'U.E. e gli Stati membri chiamati al loro recepimento secondo il tradizionale schema discendente, con una sostanziale latitanza delle autorità federali in America (ove si registra anche l'assenza di un'Agenzia indipendente preposta al settore, che resta nella competenza della Federal Trade Commission, a conferma di un approccio in chiave prettamente economica) ed una supplenza attiva esercitata dai legislatori statali, con una significativa espansione della *statute law* a questo livello.

[8] A. Pajino, *La costruzione dell'infosfera e le conseguenze sul diritto*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol 1, Bologna, Il Mulino, 2022, 9-26, spec. 15, «L'intelligenza artificiale ha attraversato tutti i campi del diritto ed è stata da questo attraversata, proprio perché essa è suscettibile di applicazione in ogni attività».

DPCE online
ISSN: 2037-6677

Allo stesso modo, in particolare in questo momento di passaggio che caratterizza tutti i macro-sistemi, la comparazione è utile per capire l'evoluzione della disciplina nel tempo e rendere più agevoli forme di interpretazione storico-evolutive funzionali all'individuazione delle modifiche che si è inteso apportare ed alla loro pratica applicazione. La grande importanza che ha avuto, ad esempio, l'approvazione dell'AI Act e, prima di esso, gli altri tasselli della strategia digitale comunitario, segnano un prima e un dopo, confermando come l'esperienza europea più recente tenda ad allontanarsi dall'impostazione liberista statunitense, oltre a porsi in maniera del tutto antitetica rispetto alla posizione collettivista e anti-individualista che caratterizza l'anti-modello cinese.

2.1 Punti di divergenza nella comparazione orizzontale e verticale tra modelli di regolazione dell'Intelligenza artificiale

E qui si apre il grande tema, di grande rilievo per il comparatista, delle relazioni che si sviluppano tra la regolazione di questo fenomeno di dimensioni globali e le diverse tradizioni giuridiche sottostanti, che fanno emergere significative diversità di approccio e di regolazione, tenuto conto, in particolare, del doppio binomio autorità-libertà da una parte, individuo-comunità dall'altra[9].

Trattando con riferimenti sintetici e sommari una questione che meriterebbe ben altro approfondimento, la principale divaricazione che si registra è quella tra Western Law e Asian Law, considerato quest'ultimo limitatamente all'esperienza cinese considerata quale epifenomeno (nella consapevolezza che considerazioni diverse dovrebbero essere sviluppate per gli altri Paesi dell'Estremo oriente). L'esperienza del *social scoring* attivato nel 2014 in Cina per decisione del Governo (il Consiglio di Stato), di cui riferisce la relazione di Vanessa Previti che ben ne evidenzia le differenze rispetto ad alcuni tentativi europei, è esemplare per evidenziare la distanza che separa questi due mondi. La pervasività del sistema di controllo introdotto per monitorare i comportamenti dei cittadini, anche per le tecnologie utilizzate, abbinato all'acquisizione di forme di credito sociale in base al carattere più o meno virtuoso dei comportamenti tenuti, evoca un parallelismo con la situazione preconizzata da George Orwell in "1984", di un Grande fratello che alla fine degli anni '40 del secolo scorso poteva essere solo immaginata dalla fervida fantasia di uno scrittore ed oggi appare concretamente realizzabile. Difficile stabilire se la pervasività del controllo imposto da un regime autoritario come quello cinese, nel quale si registra anche un travisamento della nozione di *Rule of Law* fatta coincidere con il mero riconoscimento del diritto di proprietà privata, segua o preceda una convinzione radicata nella tradizionale *forma mentis* del suo popolo. Certamente si può rilevare la situazione ormai stabilizzata di questo Paese si regga su una sovrapposizione simbiotica tra il formante tradizionale di matrice sociale di derivazione confuciana e la prassi marxista declinata in

[9] *Ex multis*, M. Zalnieriute, L. Bennett Moses e G. Williams, *The Rule of Law and Automation of Government Decision-Making*, in *The Modern Law Review*, 2019, n. 82, 433 ss.

salsa orientale[10]. Così, l'antico comunitarismo[11] che permea la società cinese e che continua a tratteggiarne le relazioni interpersonali (il guanxi) ed a imporre la subordinazione dell'individuo rispetto all'interesse dei gruppi di appartenenza a qualsiasi livello, si somma con il collettivismo proprio dell'ideologia comunista e della sua vocazione dirigista che ha l'epicentro nel partito guida e nel principio cardine del centralismo democratico[12].

In ogni caso in Cina, diventata ormai una delle superpotenze tecnologiche e nel campo delle applicazioni dell'A.I, il governo del mercato digitale con la connessa gestione dei dati, resta saldamente nelle mani del partito comunista, che lo gestisce attraverso canali informali con le aziende e per scopi sociali ben determinati come dimostra la ricordata vicenda del *social scoring* di Stato. Il mercato privato in Cina, invero, non esiste, o meglio, esiste nella misura in cui esso avvantaggia gli indirizzi politico-strategici del regime. È dunque un sistema allo stesso tempo anarchico (perché privo di valori) e totalitario (perché non libero nei suoi fini ultimi); per questo, tenuto conto dei valori su cui si regge la tradizione giuridica occidentale, poco sopra abbiamo utilizzato la definizione di anti-modello.

La tradizione euro-atlantica ha invece in comune alle varie esperienze che la compongono il valore primario del riconoscimento e della tutela dei diritti individuali, seppure con una diversa percezione del principio personalista tra le due sponde dell'Atlantico; conseguentemente, per quanto qui ci interessa, risulta più agevole una valorizzazione del diritto di protezione dei dati e della riservatezza degli utenti dei servizi digitali e di quelli legati all'uso dell'A.I. Come noto, tuttavia, la stessa tradizione giuridica occidentale non si presenta al suo interno come una realtà omogenea ed uniforme per ragioni storico-culturali, nonché riconducibili alla differente percezione dell'importanza dell'economia e dei diritti proprietari, minore nell'Europa continentale rispetto alla sponda nord-americana.

In particolare il modello europeo di protezione dei dati personali, persino prima dell'entrata in vigore del "Regolamento generale sulla protezione dei dati" (GDPR), si è da sempre caratterizzato per una impostazione fortemente personalista e ciò si deduce dalla elasticità e ampiezza della definizione di dato personale, dalla sua applicabilità ad ogni settore e per l'attenzione ad una serie di situazioni giuridiche soggettive azionabili in capo all'interessato, tanto con riferimento a trattamenti automatizzati che non: il diritto di aggiornamento, di modifica, di conoscenza, di accesso, di cancellazione dei dati nonché quello di opporsi al trattamento stesso; per quanto riguarda specificamente il trattamento interamente algoritmico, anche il diritto di ottenere l'intervento umano e di

[10] La stratificazione di cui parla anche H.P. Glenn, *Tradizioni giuridiche nel mondo. La sostenibilità della differenza* (trad. it.), Bologna, 2011, pp. 540 ss.

[11] Secondo un'accezione comune agli studiosi delle tradizioni giuridiche; cfr., ex multis, M. Van Hoecke, M. Warrington, «*Legal Cultures, Legal Paradigms and Legal Doctrine. Towards a New Model for Comparative Law*», in *International and Comparative Law Quarterly*, 1998, 495 ss.

[12] Sulla commistione tra elementi tradizionali e costruzione di un ordinamento ispirato all'ideologia comunista fonda la propria tassonomia dei sistemi giuridici G. Cuniberti, *Grands systemes de droit contemporains. Introduction au droit comparé*, 3° ed., Paris, 2015.

DPCE online
ISSN: 2037-6677

ottenere una spiegazione della decisione. Alla base di tutto la presenza di un nucleo di principi procedurali che garantiscono un elevato livello di protezione durante tutto il ciclo di vita dell'informazione (trasparenza, minimizzazione, *by design/by default*, e, soprattutto, l'indispensabile apporto umano nel processo decisionale), così come la previsione di una regolamentazione specifica e più restrittiva nei confronti di particolari categorie di dati (pensiamo all'esclusione della profilazione per i minori). Come rilevato da Pasquale Stanzione nelle sue considerazioni introduttive a questo seminario, il fulcro dell'approccio europeo risiede nella convergenza tra innovazione e libertà, risultando, allo stato, il modello più garantista e, per questo preferibile.

La modalità americana di concepire a governance dell'A.I. è, invece, diretta derivazione della concezione liberale di origine ottocentesca propria della società statunitense e mai superata, che, sulla base di una visione proprietaria e borghese, pone la libertà iniziativa economica e il mercato al centro del sistema e considera la politica in una posizione per lo più servente ai suoi bisogni. Il diritto alla *privacy*, che ha trovato in questo paese la sua culla d'origine a partire dall'ultimo decennio del XIX secolo, grazie al contributo di Warren e Brandeis[13] e che poi è diventato un principio "fisarmonica" esteso per la tutela costituzionale di situazioni diverse tra loro sotto l'ombrello del I emendamento, nell'ambito di cui ora ci occupiamo è, dunque, ancora considerato come un bene economico, oggetto di possibile scambio o commercio. Ciò comporta l'adozione di un modello autoregolativo neoliberista in cui il governo della rete è di fatto di stampo privatistico e dove le aziende digitali possono muoversi senza troppi "fastidi" legislativi.

Le differenze sono verificabili anche in relazione ai singoli istituti o alle singole prassi giuridiche. Si prenda la questione affrontata da una delle relatrici sul problema legato all'anonimizzazione dei nomi dei magistrati[14]. Ecco, dalla tradizione di *common law* emerge chiaramente il principio che impone l'applicazione alle decisioni giudiziarie la massima trasparenza. Tale principio è legato innanzitutto all'importanza rivestita alle *opinions* dei singoli giudici nelle singole decisioni. La tradizione continentale di matrice francese (ma di derivazione canonistica), invece, si basa soprattutto sul principio collegialità sentenze, in quanto ciò che conta è la pronuncia e "la *bouché*" che le declama non assume né deve assumere nessuna rilevanza. Un confronto tra queste esperienze non può quindi essere limitato ad una mera analisi del dato normativo vigente e delle singole decisioni giurisprudenziali, ma va contestualizzato tenendo conto del peso esercitato dalle tradizioni giuridiche sottostanti che, nonostante la condivisione dei valori di fondo, mantengono differenze significative sia di matrice culturale che giuridica.

Anche sotto il profilo della comparazione verticale emergono significative differenze tra Europa e Stati Uniti. Mentre in Europa sono decisive le fonti comunitarie, tanto quelle primarie come l'art. 39 TUE, l'art. 16 TFUE e l'art. 8 della Carta di Nizza, quanto le fonti quadro secondarie, prima di tutte il GDPR e l'AI Act, ma anche gli innumerevoli regolamenti

[13] V. ora S. D. Warren, L. D. Brandeis, *The Right to Privacy* (1890), trad. It. cura del Garante per la protezione dei dati personali, Verona, 2005.

[14] V. Capasso, *Tra protezione dei dati personali e accountability del giudice: spunti di riflessione dall'esperienza franco-belga*, in questa Rivista.

parte della Digital Strategy, negli Stati Uniti, invece, assistiamo ad un perfetto ribaltamento di prospettiva: al *self restraint* delle autorità federali (che solo ultimamente cominciano ad aprirsi alla discussione su una possibile regolazione) fa pari un attivismo dei livelli di governo più periferici e persino localistici. È il caso che interessa le tecnologie di riconoscimento facciale evidenziato da Alberto Orlando che riferisce come negli Stati Uniti le entità federate abbiano in più di un caso colmato il "vuoto" del livello federale[15].

In definitiva si può ritenere che i tentativi europei (sia a livello sovranazionale che statale) di contenere la pervasività dello sviluppo tecnologico alla ricerca di un difficile bilanciamento tra interessi economici di portata colossale e garanzie da assicurare ai diritti di libertà, siano riconducibili all'onda lunga del costituzionalismo europeo del Secondo dopoguerra ed a quel patrimonio costituzionale comune[16], che pone al centro il principio della dignità della persona come principio supremo (art. 2 Legge fondamentale tedesca); un patrimonio, la cui esistenza è stata esplicitata già con l'art. 2 del Trattato di Maastricht, per trovare poi una sistemazione definitiva, prima ancora che nella Carta dei diritti fondamentali dell'Unione europea (artt. 1,6,7,8 in particolare[17]), nell'art. 2 dell'attuale Trattato UE, con il richiamo del rispetto della dignità umana, della libertà dei diritti umani, quali valori fondanti dell'Unione stessa. Riteniamo, pertanto, che lo stesso potere discrezionale riconosciuto alle autorità dell'U.E. titolari di poteri normativi possa essere esercitato solo restando all'interno del perimetro tracciato da questi principi generali, come, peraltro, in buona misura si sta facendo.

2.2 Punti di convergenza: il "Brussels effect" verso gli U.S.A.

Sulla spinta della strategia europea, negli Stati Uniti sono stati introdotte, a livello statale, numerose norme per la protezione dei consumatori che contemplano la regolazione del processo decisionale algoritmico. Il Colorado Privacy Act (CPA), il Connecticut Data Privacy Act (CTDPA), il California Privacy Rights Act (CPRA), il Tennessee Information Privacy Act (TIPA) e il Virginia Consumer Data Protection Act (VCDPA) regolano in modo specifico l'utilizzo dei sistemi di intelligenza artificiale anche con riferimento alla profilazione[18]. Secondo il CPA, ad esempio, le aziende devono consentire

[15] A. Orlando, *La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA:* alea IActa est? in questa Rivista.

[16] Nell'accezione, ancora attuale, di A. Pizzorusso, *Il patrimonio costituzionale europeo*, Bologna, 2002.

[17] Non dobbiamo dimenticare che la Carta di Nizza è uno dei pochi testi che richiama espressamente la "Protezione dei dati di carattere personale", assicurando la protezione ad ogni individuo, ponendo dei limiti al loro trattamento, imponendo l'istituzione di autorità indipendenti preposte al controllo.

[18] Anche in Utah dal 1° gennaio 2024 è entrata in vigore un ampio corpo normativo di tutela della privacy, il quale però non comprende condizioni per l'utilizzo di sistemi di decisione algoritmica, ma solo diritti standard di accesso e cancellazione dei propri dati che hanno impatto anche con riferimento al loro utilizzo. Entro i prossimi 2 anni dovrebbero essere altri sei gli Stati che adotteranno una legge generale sulla protezione dei dati personali.

DPCE online
ISSN: 2037-6677

ai consumatori di rinunciare al trattamento dei dati personali per qualsiasi decisione automatizzata che produca effetti giuridici o altri effetti significativi per il consumatore, come le decisioni automatizzate che hanno un impatto sulle opportunità finanziarie, educative, abitative o lavorative[19]. Le aziende sono tenute poi ad effettuare valutazioni d'impatto sulla protezione dei dati prima di procedere al trattamento automatizzato, laddove quest'ultimo rischi di comportare un trattamento iniquo o un danno finanziario, fisico o di altro tipo per i consumatori, nonché a consentire il controllo da parte del Procuratore Generale dello Stato che ne verifica la conformità con le norme in materia[20]. Si tratta di una normativa che il frutto del modello sperimentato in Europa, che dall'Europa trasla i criteri ispiratori generali dell'intera disciplina di protezione dei dati personali e le linee direttrici per l'interpretazione delle norme, ma anche alcune innovazioni in senso stretto, come quella riguardante la profilazione.

Da ultimo è da segnalare un'iniziativa che trae le mosse dal processo di adozione dell'AI Act europeo: il procuratore generale del Connecticut, William Tong, sta guidando una coalizione bipartisan di ventitre *State Attorneys General* per esortare la *National Telecommunications and Information Administration*[21] a promuovere politiche federali di *governance* unitaria dell'Intelligenza artificiale che diano priorità alla trasparenza, alla certificazione attraverso la predisposizione di requisiti affidabili e la supervisione degli usi dell'A.I. ad alto rischio[22]. Anche sotto il profilo della *governance* procedurale, la lettera congiunta dei procuratori generali statunitensi ha esortato le autorità federale ad istituire un'Autorità di controllo ed *enforcement* centralizzata "*in any Federal regulatory regime governing AI*"[23].

3. Alcune questioni in tema di fonti

Le sfide poste dall'invasione delle nuove tecnologie hanno, tra gli altri effetti, inciso in maniera determinante sui sistemi delle fonti del diritto e sulla scelta degli atti normativi più adatti ad intervenire. Si è posta immediatamente l'alternativa tra il ricorso alle fonti tradizionali, con l'alternativa tra discipline impostate in termini generali e di principio, piuttosto che di

[19] Colorado Privacy Act, 6–1–1303, § 10.

[20] Colorado Privacy, 6–1–1309, §§ 1 e 4.

[21] Agenzia solo lontanamente assimilabile al nuovo *AI Office* della Commissione europea con compiti consultivi in materia di telecomunicazioni ed avanzamento tecnologico.

[22] D. Pipier, *Regulatory Update: Developments in Artificial Intelligence Governance*, in *Journal of Internet Law*, vol. 27, n. 1, luglio-agosto, 2023, 1-16, spec. 5: «The foundation of any effective AI governance framework is appropriate transparency. For example, consumers must be told when they are interacting with an AI rather than a human being and whether the risks of using an AI system are negligible or considerable. To the extent organizations employ AI systems to handle critical functions, the best practice to use is to commit to ongoing cycles of testing, assessment, and external audits».

[23] D. Pipier, *Regulatory Update*, cit., 8, aggiunge: «*Significantly, State AG authority can enable more effective enforcement to redress possible harms*».

dettaglio, con un problema sullo sfondo: la rapida obsolescenza delle discipline adottate, costantemente superate dal progresso tecnologico incessante; in ogni caso si è registrata una dilatazione delle normative tecniche, spesso di difficile intelligibilità per il giurista e per la cui stesura è necessario il ricorso a competenze proprie di altri saperi.

Fino agli anni recenti sono stati soprattutto strumenti normativi di *soft law* a regolare la disciplina dell'A.I.; ciò è spiegabile non solo in virtù della loro natura latamente consensuale e dunque anti-autoritativa, rispettosa della libertà degli attori del mercato, ma anche perché essi posseggono una funzione regolatoria intrinsecamente comparativa: pongono regole cui i destinatari debbono conformarsi in virtù di un certo interesse pubblico, perseguito dalla regolazione, pur rimanendo questi soggetti liberi di discostarsi dalle disposizioni impartite qualora ciò sia reso utile o necessario[24]. La *soft law* rappresenta quindi il banco di prova proprio per situazioni come quella presente, perché permettere una valutazione dell'operato di questi soggetti da parte degli altri consociati senza irrigidire troppo la disciplina di una materia ancora tutta in divenire. Questa forma di atti *lato sensu* normativi sono ancora oggi quelli che in larga parte disciplinano la materia dell'Intelligenza artificiale negli Stati Uniti e che, di conseguenza, caratterizzano l'approccio per una sostanziale *self-regulation* delle piattaforme. Diversamente l'Europa, già con il GDPR e successivamente dal 2020 in poi, anno in cui *Digital Strategy* è stata lanciata, ha intrapreso una rilevante campagna di codificazione delle regole sui mercati digitali e, con essi, delle applicazioni dell''Intelligenza artificiale, pur con deroghe importanti. Tra queste, da ultimo, lo spostamento dell'efficacia di molte delle disposizioni dell'AI Act a 36 o 48 mesi dal momento dell'entrata in vigore del testo[25]. La scelta di queste tempistiche estremamente dilatate può essere considerata un compromesso tra l'approccio *hard* e quello *soft*, tra le scelte di prevedere una regolazione normativa, ma anche dare tempo ai privati di mettere in atto gradualmente le prescrizioni attraverso la progressiva auto-regolazione in ottemperanza degli standard normativi comunitari.

Va anche ricordato che il procedimento legislativo comunitario stesso prevede in maniera capillare i modi e tempi di utilizzo delle forme di democrazia partecipativa che portano *de facto* a una co-regolazione legislativa tra istituzione e *stakeholders*. È vero che in Europa agli *interessati* è data una "voce" e non un "voto"; tuttavia, il rilievo concreto che riveste il policentrismo della fase dibattimentale dell'Unione è indiscusso: l'immissione nel processo pre-decisionale di queste altre "voci" evidenzia la struttura del potere sovrano come articolazione/competenze e, almeno sulla

[24] E. Mostacci, *La* soft law *nel sistema delle fonti. Uno studio comparato*, Wolters Kluwer, 2008, spec. 46 ss.

[25] Per quanto riguarda i sistemi di IA già immessi sul mercato o messi in servizio, l'accordo di compromesso stabilisce in particolare che: le autorità pubbliche che sono fornitori o utilizzatori di sistemi di IA ad alto rischio avranno quattro anni di tempo per rendere conformi i propri sistemi; i modelli immessi sul mercato prima della data di applicazione delle disposizioni a loro relative (ossia 12 mesi dopo l'entrata in vigore del regolamento) avranno due anni di tempo dalla data di applicazione di tali disposizioni (quindi 3 anni in totale) per conformarsi.

DPCE online
ISSN: 2037-6677

carta, lo dota di una trasparenza e di una legittimità democratica che non esiste negli altri metodi di produzione giuridica[26].

L'importanza degli strumenti di *soft law*, per la loro duttilità e capacità di adeguamento, è innegabile; non deve tuttavia trattarsi dagli unici tipi di fonte chiamati ad occupare il campo, essendo necessario pretermettere loro atti normativi di carattere vincolante, magari formulati in termini di principio per ridurre il rischio di una loro obsolescenza in tempi brevi, che siano in grado, con le procedure proprie della decisione politica, di assicurare un bilanciamento a priori dei molteplici interessi in gioco e di garantire un minimo di certezza e di stabilità al quadro normativo. La presenza di regolamenti/direttive europee o leggi nazionali, di per sé necessaria, al tempo stesso non pare sufficiente. La molteplicità dei casi che possono presentarsi in concreto e gli elementi imprevedibili di novità che possono caratterizzarli, rende indispensabile il rafforzamento degli strumenti di bilanciamento in concreto; diventa, quindi, centrale il ruolo che possono esercitare gli organi di garanzia, a partire dalle Autorità indipendenti (delle quali devono essere garantite le competenze tecniche necessarie e l'indipendenza effettiva dal potere politico), per finire con i giudici, in grado di utilizzare tutti gli strumenti ermeneutici a loro disposizione, compresa l'interpretazione analogica ed il ricorso alla comparazione, che mai come in questi casi può diventare l'amica che aiuta a risolvere i casi controversi, secondo l'accezione a suo tempo formulata da Aharon Barak.

Per completare i riferimenti alle questioni di carattere generale poste dal complesso delle relazioni presentate in questa giornata, dovremmo approfondire anche le questioni relative all'uso delle nuove tecnologie nell'ambito della sicurezza, nonché quella relativa al valore che può essere riconosciuto all'espressione del consenso da parte degli interessati all'accesso ed all'uso dei loro dati personali. L'importanza di tali questioni viene certamente svilita dai rapidi riferimenti di carattere problematico che seguiranno, ma dai quali non possiamo esimerci.

Riguardo al primo tema, di una cosa ci sentiamo sicuri: in materia penale e più in generale di sicurezza pubblica, ambito nel quale il ricorso agli strumenti di controllo offerti dalle tecnologie si sta diffondendo sempre più, gli standard di tutela della *privacy* devono risultare diversi e più rafforzati rispetto alle materie del diritto privato e del diritto commerciale, allorché si tratta di diritti di natura prevalentemente economica. Questo è imposto dagli statuti costituzionali che presidiano la libertà personale intesa anche come libertà fisica oltre che spirituale, le libertà di manifestazione del pensiero, di circolazione, di riunione, di associazione, definiti dalla compresenza di una riserva assoluta di legge e da una riserva di giurisdizione. Anche in questo campo sussiste l'esigenza di contemperare interessi diversi, quali la libertà personale nelle sue svariate declinazioni con gli interessi pubblici al perseguimento dei reati e, prima ancora ad una loro possibile prevenzione, al fine di garantire la sicurezza delle comunità. Sotto questo profilo, un'attenzione particolare in questo seminario è stata rivolta all'uso delle tecniche di riconoscimento facciale (oggetto di ben due relazioni, quelle di Lorenzo Sottile e di Alberto Orlando), uno strumento formidabile per

[26] Si consenta un rinvio a A. Gatti, *La legittimazione del diritto transnazionale tra partecipazione degli interessati e partecipazione democratica*, in *Lo Stato*, 4, 2020, 421-426.

l'identificazione delle persone ma piuttosto controverso ed ancora in attesa di una disciplina compiuta tanto nei paesi europei che negli Stati Uniti. In proposito ci sembra particolarmente interessante l'emersione di un indirizzo giurisprudenziali nelle corti americano volto ad estendere all'utilizzo di questo strumento delle garanzie dell'habeas corpus, in un parallelismo che ci porta a riflettere sulla possibilità, alle nostre latitudini, di utilizzare la riserva di giurisdizione quale canale autorizzatorio preventivo per lo svolgimento delle attività connesse alla tutela dell'ordine pubblico con strumenti telematici e tecnologie avanzate.

Collegato a quello appena richiamato è un altro tema particolarmente spinoso e sul quale, a nostro modo di vedere, non si è ancora riflettuto abbastanza, anche per la carenza di informazioni, quello dell'uso per finalità di spionaggio nei confronti di persone ritenute evidentemente pericolose e da tenere sotto controllo. Il confine tra finalità istituzionali e di altro tipo è, tuttavia, sottile e non si possono escludere abusi difficilmente controllabili. Come sempre, fenomeni di questo tipo vengono colti in sede letterario o da rappresentazioni filmiche; così, nella serie americana *House of cards*, compare il personaggio di Rachel Posner, una giovane prostituta che arriva ad intrecciare una relazione tossica con uno dei principali collaboratori del Presidente federale, del quale poi si libera rifugiandosi in un altro Stato e cambiando lavoro e identità. Il funzionario pubblico, con la complicità di un dirigente dell'FBI riesce a farla spiare ed a rintracciarla, in modo, alla fine, in modo da poterla uccidere per liberarsi di un testimone scomodo. Certamente un caso limite, viziato dalla disonestà e dall'interesse personale di alcuni funzionari pubblici, ma illuminante riguardo alle enormi potenzialità dei mezzi investigativi che utilizzano tecnologie avanzate e strumenti di A.I., e, come tale, utile per una riflessione più generale riguardo ai pericoli che ciascuno di noi può correre.

4. La *governance della governance*: quali strutture e perché?

Il tentativo normativo di guidare lo sviluppo dell'Intelligenza artificiale, oltre che profili regolatori sostanziali, contiene anche un livello di *governance* organizzativa, cioè cerca di delineare una struttura che, da una parte, accompagni le misure che devono assumere i soggetti che condividono e processano i dati, dall'altra che ponga in essere misure di coordinamento e controllo per assicurare la massimizzazione del valore dei dati e, allo stesso tempo, la minimizzazione dei rischi.

Qui merita trascurare le fonti di *soft law* che disciplinano il caso statunitense per concentrarci sulla esperienza di punta, quella dell'Unione europea.

Mentre nel caso del GDPR l'Unione europea stessa ha strutturato un impianto regolatorio multilivello omogeneo, l'AI Act si è limitata a indicare le Autorità competenti del piano comunitario (Titoli VI, VII, e VIII), lasciando agli Stati ampi margini di scelta sull'individuazione degli enti nazionali.

4.1 (Segue) Il piano comunitario

DPCE online
ISSN: 2037-6677

Per il piano comunitario il Titolo VI prospetta una *governance* estremamente più complessa rispetto al GDPR poiché prevede la presenza di soggetti dalle prerogative giuridiche diversificate. L'art 56 istituisce il Comitato (*Board*) per l'IA, composto da rappresentanti degli Stati membri, che sarà una piattaforma di coordinamento e organo consultivo della Commissione il cui compito sarà quello di controllare e certificare i sistemi A.I. a uso generale e di progettare codici di buone pratiche. *Il Board* è composto dalle Autorità nazionali di controllo, rappresentate dal capo di tale Autorità o da un alto funzionario di livello equivalente, e dal Garante europeo della protezione dei dati.

Al Comitato la Commissione europea ha deciso di affiancare un ulteriore organo, l'Ufficio AI (istituito formalmente nel febbraio scorso), a cui va il compito di adiuvare i processi interni della Direzione Generale *Reti di Comunicazione, Contenuti e Tecnologie*, in particolare di fornire – anche con l'aiuto di un *panel* di esperti indipendenti – linee guida per lo sviluppo dei sistemi e dei modelli di IA, avviare indagini, imporre misure correttive, monitorare l'effettiva applicazione della normativa e avviare consultazioni per la stesura di codici di condotta. La sua istituzione non dovrebbe incidere sui poteri e sulle competenze delle Autorità nazionali competenti e degli organi e organismi dell'Unione in materia di vigilanza dei sistemi di A.I.[27].

L'Ufficio dovrà supervisionare i modelli di A.I. generali più avanzati e contribuire a promuovere norme e pratiche comune di prova dei modelli (ad esempio verificare di volta in volta l'emergere di modelli alto impatto e monitorando i possibili rischi materiali di sicurezza connessi ai modelli di base). In tal modo l'Unione, all'interno del sistema di governance multilivello, si riserva alcuni poteri di esecuzione a livello sovranazionale.

Infine, sarà istituito un forum consultivo per i portatori di interessi, quali i rappresentanti dell'industria, le PMI, le *start-up*, la società civile e il mondo accademico, al fine di fornire competenze tecniche al comitato per l'A.I.

4.2 (Segue) Il piano statale: le differenti scelte dei vari Stati membri

Per quanto riguarda il piano statale, il nuovo Regolamento dispone genericamente che gli Stati istituiscano una o più Autorità nazionali, sebbene tale denominazione debba intendersi in senso a-tecnico come testimonia il parere (orale) dato al Governo italiano dalla DG *Reti di Comunicazione, Contenuti e Tecnologie* della Commissione europea nell'aprile 2024 (e come dimostra la conseguente scelta del Governo italiano)[28].

[27] https://digital-strategy.ec.europa.eu/it/library/commission-decision-establishing-european-ai-office

[28] Oltre alla designazione di autorità di regolazione, gli Stati sono chiamati anche ad indicare autorità competenti per la vigilanza sul mercato dei sistemi di IA e dei prodotti con componenti di IA a presidio della sicurezza dei consumatori quali utenti finali di tali sistemi successivamente alla loro immissione sul mercato. Le autorità di vigilanza del mercato sarebbero investite dunque del compito di verificare la segnalazione di incidenti e malfunzionamenti correlati all'IA e di indagare in merito al rispetto degli obblighi e dei requisiti per tutti i sistemi di IA ad alto rischio già immessi sul mercato. Cfr. Art. 43 comma 1, art. 46 comma 1 lett. d), e art. 59, comma 2 Ai Act. È da capire,

Alcuni Stati hanno già proceduto a scegliere la rete di *governance* degli enti responsabili, ma solo i Paesi Bassi, invero hanno conferito al Garante per la protezione dei dati personali ("Autoriteit Persoonsgegevens") ulteriori risorse per esercitare la competenza derivante dall'AI Act.

La Spagna ha designato la "Agencia Española de Supervisión de la Inteligencia Artificial" (AESIA), come Autorità di regolazione competente ai sensi dell'AI Act, che si situa all'interno del Ministero per la Trasformazione Digitale. Questa Agenzia avrà poteri ispettivi, correttivi e sanzionatori nell'ambito dell'IA[29]. In Grecia, già nel 2022[30] fu o istituito un Comitato di Coordinamento per l'IA con la funzione di definire la Strategia nazionale per l'IA e un Comitato per la supervisione di tale strategia, che ne assicuri l'applicazione coerente (ciò per non pregiudicare le competenze delle due maggiori Autorità coinvolte, *privacy* e regolazione del mercato). Con ogni probabilità tale comitato sarà anche responsabile per l'enforcement dell'AI Act. In Francia la CNIL ha annunciato di aver creato al proprio interno un dipartimento, "SIA" (Servizio per l'Intelligenza Artificiale), per rafforzare il proprio expertise in materia, preparandosi per l'entrata in vigore dell'AI Act[31], sebbene ad oggi risulti soltanto la nomina di un coordinatore interministeriale della strategia nazionale sull'intelligenza artificiale, organo monocratico di raccordo tra il Ministero della ricerca e quello delle telecomunicazioni. In Italia la competenza sarà ripartita tra l'Agenzia per l'Italia Digitale (AgID) e l'Agenzia nazionale per la cybersicurezza.

Questa breve panoramica ci mostra come il *framework* sia del tutto eterogeneo sia per natura delle fonti sia per composizione, ma che quasi in tutti i casi, la maggior parte degli organismi siano sottoposti all'indirizzo politico del Governo, che dunque rimane il *dominus* nella *governance* della materia.

5. Un sistema complesso e interoperabile: un compromesso politico o una scelta pragmatica?

Che considerazioni si possono trarre dallo studio dell'impostazione comunitaria?

In primo luogo, che il grado di complessità della regolazione dell'IA è tale da richiedere necessariamente una gestione multilivello, interistituzionale ed interdisciplinare: troppi sono gli interessi coinvolti (*privacy*, diritto dei consumatori, tutela dei diritti della personalità, della

nel caso di creazione di altri organismi, come faranno a mantenere un ruolo di primo piano le esistenti autorità di vigilanza del mercato, per intenderci quelle già competenti in materia di sicurezza e conformità di alcuni prodotti rischiosi, come i dispositivi medici.

29 BOE-A-2023-18911 Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial).

30 Legge 4961 del 27 luglio 2022 (G.U. 146/A/27-07-2022).

31 Cfr. CNIL, *Création d'un service de l'intelligence artificielle à la CNIL et lancement des travaux sur les bases de données d'apprentissage*, 23 febbraio 2023, online su https://www.cnil.fr/fr/creation-dun-service-de-lintelligence-artificielle-la-cnil-et-lancement-des-travaux-sur-les-bases-de.

DPCE online
ISSN: 2037-6677

sicurezza pubblica, della salute, e così via). È dunque del tutto comprensibile che la responsabilità sia stata ripartita tra più organismi e tra più livelli.

In secondo luogo ne deduciamo che non esiste quasi dovunque alcun ruolo diretto e generale delle Autorità *privacy* nella regolazione della materia che invece è stato previsto a beneficio delle Agenzie o della stessa Commissione europea. Tale scelta può essere letta in due modi diversi. Da una parte ciò potrebbe evidenziare una mancanza di attenzione al profilo della tutela, malgrado la *ratio* stessa dell'operazione legislativa fosse orientata proprio a garantire i consumatori e cittadini contro possibili violazioni dei loro diritti e libertà fondamentali compiute da o tramite tecniche algoritmiche. La finalità della regolazione dell'A.I. ha infatti una natura duale: non è funzionale solo alla creazione di uno spazio giuridico ed economico che massimizzi i benefici della ricerca e dell'applicazione tecnologica, ma pone al centro del sistema di tutele l'individuo e i suoi diritti fondamentali. Per questo il modello più consono cui ascrivere il novero dei soggetti destinatari di competenze di supervisione dovrebbe risultare soprattutto quello delle Autorità e non quello delle Agenzie che, al contrario delle prime, restano sottoposte all'indirizzo politico del Governo.

Dall'altra parte, però, più semplicemente questa scelta può essere anche vista anche come un esercizio di pragmatismo. Effettivamente, al di là delle altisonanti aspettative che ha suscitato l'annuncio del "primo Regolamento sull'Intelligenza artificiale al mondo", se si guarda al suo contenuto notiamo che lo sforzo regolatorio-applicativo è incentrato in larga parte sull'aspetto tecnico di certificazione dei sistemi.

Nonostante l'elevato impatto su una vasta gamma di diritti fondamentali dell'individuo e sugli interessi generali della collettività, l'AI Act non è un *Bill of Right* dell'intelligenza artificiale, non ha il respiro di una carta di diritti, ma – salvo alcune previsioni oggettivamente rilevanti[32] – si iscrivere piuttosto nel novero di norme relative alla sicurezza dei prodotti. Rispetto ai divieti e ai limiti che prescrive all'utilizzo di intelligenze artificiali ciò che si chiede agli organismi di *governance* è quasi esclusivamente di verificare e certificare (cioè regolare) gli standard di qualità alla luce dei criteri individuati nel Regolamento stesso o indicati da questo[33]. In altre parole, l'Ai Act già individua preventivamente elementi per l'analisi del rischio operando quella regolazione *ex ante* dei principi e quella operazione

[32] Ad esempio i criteri di regolazione (proibizioni e parziali deroghe) che riguardano la profilazione che sono in effetti tutele sostanziali e di principio per un fenomeno molto delicato. Si tratta però quantitativamente (anche se non qualitativamente) di elementi marginali nell'impianto generale del Regolamento.

[33] Un compito che l'Autorità Garante non potrebbe ricoprire anche per via della sua stessa natura e delle sue funzioni, che non sono regolatorie in senso formale. Sebbene non si possa escludere che l'Autorità di controllo delineata dal GDPR sia chiamata ad un'opera di mediazione tar contrapposti interessi politici ed economici o di composizione di conflitti tra interessi ordinamentali, il modello a cui si ispira l'Autorità per la protezione dati personali italiana è quello dell'Ombudsman scandinavo (garante dei diritti soggettivi) piuttosto che quello delle autorità di regolazione (cfr. F. Cardarelli, *Art. 51* (*Autorità di controllo*) e Artt. 57-58 (*compiti e poteri*), in O. Pollicino et al. (a cura di), Codice della privacy e data protection, Milano, Giuffré, 2021, rispettivamente 6994-706 (spec. 699) e 743-752 (spec. 745).

di bilanciamento dei diritti e interessi che le Autorità sono chiamate a fare[34] (si pensi alle soglie predeterminate di rischio). Il Regolamento AI non lascia spazio ad alcuna "integrazione legislativa" come invece, in effetti, funziona per il GDPR[35], dove l'Autorità preposta, cioè il Garante, esercita compiti di ordine e, in senso lato, di regolazione.

Ciò che però è importante notare – anche perché è spesso trascurato o sottovalutato nelle analisi – è il ruolo di primo piano riservato in capo al Garante europeo e, di riflesso, a quelli nazionali nel processo di controllo e talora persino di *governance*: l'art. 57 prevede che l'EDPS sia parte integrante del Comitato europeo sull'AI, mentre l'art. 59 evidenzia che anche per gli atti delle istituzioni, delle Agenzie e degli organismi dell'Unione che rientrano nell'ambito di applicazione del regolamento AI, il Garante europeo della protezione dei dati agisce in qualità di Autorità competente per la loro vigilanza.

6. Prospettive future: il rischio di un difficile coordinamento tra organismi

Il ruolo di garanzia ricoperto dalle Autorità *privacy* nazionali sarà altrettanto imprescindibile in virtù delle interazioni che la disciplina sull'AI Act produce con quella della *privacy* sancita nel GDPR.

Innanzitutto perché i Garanti (in particolare quello italiano) sono stati storicamente investiti di questioni aventi un impatto rilevante per l'utilizzo di sistemi o tecniche di A.I. che comportano impatti rilevanti per gli individui (dal c.d. Redditometro in materia fiscale, al sistema "Sari" per la sicurezza pubblica, fino allo *web scraping* e all'uso del riconoscimento facciale per *microtargeting* commerciale)[36] e dunque è in possesso di una qualificata *expertise* che gli deriva da una prassi consolidata riconducibile almeno fin dal 2012[37]. Ciò vale a maggior ragione in sistemi, come quello delineato dal

[34] A. Predieri, *L'erompere delle autorità amministrative indipendenti*, Firenze, Passigli, 1997; M. Clarich, V. Zeno Zencovich, G. Corso, *Il sistema delle Autorità indipendenti: problemi e prospettive*, 2006, eprint/luiss.it.

[35] Espressione utilizzata da A. Peduto, *Art. 57*, in E. Belisario, G.M. Riccio, G. Scorza (a cura di), *GDPR e Normativa Privacy – Commentario*, Milano, Wolters Kluwer, 2022, 587-597 con riferimento al GDPR.

[36] Cfr. rispettivamente Garante per la protezione dei dati personali, *Redditometro: le garanzie dell'Autorità a seguito della verifica preliminare sul trattamento di dati personali effettuato dall'Agenzia delle* entrate, 21 novembre 2013, doc. web n. 2765110; Parere sul sistema Sari Real Time - 25 marzo 2021, provv. n. 127 del 25 marzo 2021, doc. web n. 9575877 e Sistema automatico di ricerca dell'identità di un volto, del 26 luglio 2018, provv. n. 440 del 26 luglio 2018, doc. web n. 9040256; Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022, provv. n. 50 del 10 febbraio 2022, doc. web n. 9751362; Installazione di apparati promozionali del tipo "*digital signage*" (definiti anche Totem) presso una stazione ferroviaria del 21 dicembre 2017, provv. n. 551 del 2017, doc. web n. 7496252

[37] Il primo intervento significativo del Garante in tema di trattamenti automatizzati risale al parere del 17 aprile 2012, doc. web n. 1886775, quando rilevò i rischi specifici per i diritti fondamentali, la libertà, e dignità degli interessati derivanti dalla sperimentazione di un sistema di tracciamento antievasione dell'Agenzia delle Entrate. Il sistema avrebbe comportato la classificazione dell'intera popolazione in base al rischio

DPCE online
ISSN: 2037-6677

GDPR e dall'AI Act, che riconoscono il *risk based approach* alla base di ogni attività di controllo: si pensi alla consultazione preventiva in presenza di un elevato rischio residuo non attenuabile per tecnologia disponibile o costi d'attuazione che il Garante italiano offre ai titolari del trattamento che abbiano svolto una valutazione d'impatto (Considerando n. 84 e art. 35 GDPR).

In secondo luogo, il ruolo delle Autorità *privacy* continuerà ad essere rilevante perché viene fatta salva la competenza "per materia" laddove vengano in rilievo situazioni che riguardano l'applicazione del diritto alla protezione dei dati personali. Anche in questo caso la consolidata prassi di leale collaborazione tra i diversi soggetti interistituzionali coinvolti nell'*enforcement*, in particolare tra Autorità omologhe e con il Comitato europeo per la protezione dei dati, ha dato prova di saper elaborare precedenti congiunti e di costruire una rete di buone pratiche, studi e linee guida[38].

A rivalutare ulteriormente il ruolo dell'Autorità Garante concorrerà probabilmente l'art. 77 dell'Ai Act che assegna a (ancora non meglio specificati) Agenzie o Enti nazionali il compito di vigilare sul rispetto dei diritti fondamentali violati o messi in pericolo dalle previsioni del Regolamento: "*National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights*, including the right to non-discrimination, *in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this Regulation*". Si tratta di poteri importanti tra cui quello di richiesta e informativa e di accesso documentale della documentazione formatasi in relazione all'uso dei sistemi di A.I. di alto rischio. Non è ancora chiaro a chi verrà affidato questo compito, ma lo sbocco più naturale è senz'altro l'Autorità per la protezione dei dati personali.

A questo proposito, la sfida più grande (e forse l'aspetto dove l'AI Act rivela le sue maggiori fragilità) sarà proprio quella legata all'attuazione in punto di coordinamento. Ci pare che un'efficace applicazione della normativa richiederà la creazione di efficaci quadri e canali di cooperazione tra le diverse Autorità coinvolte nel ciclo di vita dell'IA. Eppure il Regolamento non prevede efficaci procedure di coordinamento dei plessi normativi e non istituisce meccanismi di coerenza né a livello europeo né tantomeno nazionale. E non è solo una questione di composizione: come fare, ad esempio, a coordinare un'Agenzia con un Autorità? Esiste un vero e proprio

di evasione, calcolato sulla base dei dati contabili raccolti massicciamente riferiti ai soggetti già precedentemente segnalati come "a rischio" di evasione. Secondo il Garante l'Agenzia delle Entrate non aveva individuato nello specifico i criteri con cui avrebbe selezionato i contribuenti "a rischio".

[38] Ci si riferisce al meccanismo di coerenza ex art. 63 GDPR. In materia di protezione dei dati personali il principio di leale collaborazione tra Autorità il cui compasso regolatorio sia suscettibile di coprire casi e situazioni che si sovrappongono, nel rispetto delle rispettive competenze è stato ricordato recentemente dalla sentenza n. 3363/2023 del Consiglio di Stato che ha richiamato l'art. 8 del Trattato di Nizza, all'art. 16 FTUE e agli artt. 51, 57 e 58 GDPR e, prima ancora, da Corte di Giustizia, 15 giugno 2021, C-645/19 («La ripartizione delle competenze e delle responsabilità tra le autorità di controllo (…) si basa necessariamente sulla premessa di una cooperazione leale ed efficace tra tali autorità»).

rapporto gerarchico tra il Comitato europeo sull'A.I. e i differenti organismi nei vari Stati (chiamati nel testo impropriamente "Autorità") membri oppure c'è il Comitato detterà solo delle linee guida generali? Ciascuna di queste Autorità, in virtù della sua propria natura, non finirà per adottare misure che tengano conto di interessi diversi?

Insomma, il rischio è che la complessa architettura di *governance* rischi di crollare, se non verrà sorretta da efficaci canali organizzativi. Purtroppo, almeno su questo, non sembra che il legislatore europeo abbia imparato dalle esperienze normative precedenti, come quella del GDPR.

Postilla

Nel testo sono già stati effettuati richiami ad opere letterarie e serie televisive; prendendo spunto da alcune delle relazioni pubblicate intendiamo chiudere questo breve lavoro con la citazione di due pellicole cinematografiche risalenti al secolo scorso e, proprio per questo, basate su una fervida immaginazione, quasi profetica. La prima questione attiene al controllo umano sul lavoro delle macchine, quando queste vengono dotate di forme accentuate di autonomie e sono in grado di elaborare i dati in modo autonomo dopo l'impostazione iniziale: tema affrontato da Valentina Cavani con riguardo ai c.d. dati sintetici, la cui elaborazione trascende le questioni legate alla tutela della privacy. Nel film «Wargames - Giochi di guerra» del 1983, per la regia di John Badham, il protagonista principale è un supercomputer cui sono affidati il controllo e l'uso, in caso di pericolo, dell'arsenale atomico americano in caso di attacco sovietico. Sulla base di un falso allarme la macchina inizia a svolgere il compito che le è stato affidato, impedendo qualunque forma di controllo umano che possa arrestarlo. Solo l'intervento provvidenziale e un po' casuale di un giovane hacker riesce ad arrestare il disastro, con la proposta al computer di giocare a tris, che una volta accettata porta ad occupare progressivamente la memoria dello stesso, disinnescando gli altri processi attivati. La risposta finale della macchina: in questo gioco non possono esserci vincitori, è risolutiva, valendo oltre che per il gioco del tris per i conflitti nucleari.

La seconda delle pellicole che voglio ricordare è italiana e risale al 1980: «Io e Caterina», di e con Alberto Sordi e si collega agli interventi (come quello Sabrina El Sabi) che hanno evocato il riconoscimento delle emozioni, che stavolta non riguardano gli esseri umani ma le stesse macchine. Caterina è un robot, assunto da uno scapolo impenitente per assolvere le faccende domestiche, che nel tempo si affeziona al proprietario diventando gelosa delle donne che lo frequentano, per arrivare a forme di reazione anche violenta. Chiudiamo con una domanda: la tecnologia e l'A.I. potrà essere in futuro capace sviluppare un processo di antropomorfizzazione fino al punto di costruire macchine in grado di provare emozioni, quali l'amore o l'odio, allo stesso modo degli esseri umani?

Rolando Tarchi
Dipartimento
Università di Pisa
Rolando.tarchi@unuipi.it

DPCE online
ISSN: 2037-6677

Andrea Gatti
Dipartimento
Università di Teramo
agatti@unite.it