Tra protezione dei dati e intelligenza artificiale, in Europa e oltre

di Andrea Pin e Lucia Scaffardi[1]

Abstract: *Between Data Protection and Artificial Intelligence in Europe and Beyond* - This introduction summarizes some of the most pressing issues that Europe and other legal systems are dealing with in the field of data protection and AI. It sketches out the content and deep significance of the contributions of this special issue, which cover biometric and emotion detection and recognition, the value of the notions of 'synthetic data' and 'differential privacy', the promises and risks of digital technology in female healthcare, the relationship between judicial analytics and judicial accountability, and the dystopian perspective of pervasive social credit systems, just to name a few challenges. It contrasts the status of EU law with other jurisdictions that are pioneering the regulation of digital technologies.

Keywords: Data protection and AI; AI Act; GDPR; Synthetic data; Differential privacy; Automated face recognition; Biometric recognition; Judicial analytics; Social scoring; Femtech.

1. Introduzione: la tutela dei dati personali e l'AI

Il dibattito sui modelli di regolazione delle nuove tecnologie e in particolare dell'intelligenza artificiale (IA) normalmente si snoda all'interno di tre scenari alternativi – quelli che, con una espressione fortunata, Anu Bradford ha definito "imperi digitali": L'Unione europea, gli Stati Uniti e Cina[2]. Ciascuno di questi svolge un ruolo da protagonista, anche se con dinamiche e impatto cangiante, nel regolare la tecnologia e persino nell'orientarne lo sviluppo futuro. Seguendo la logica della Bradford, sarebbero tre infatti i paradigmi che questi tre grandi interlocutori seguono[3]. Gli Stati Uniti promuoverebbero la tecnologia innanzitutto quale strumento di avanzamento economico e nuovo fronte occupazionale – influenzerebbero il digitale grazie all'impatto della ricerca, degli investimenti e di un certo lassismo normativo, che avrebbe tenuto le briglie sciolte all'impresa digitale. L'Unione europea avrebbe adottato una logica protettiva dei diritti, che,

[1] Sebbene frutto di una riflessione unitaria, i paragrafi 1 e 3 sono attribuibili ad A. Pin; i paragrafi 2 e 4 a L. Scaffardi.

[2] A. Bradford, *Digital empires: the global battle to regulate technology*, New York, 2023.

[3] Sulle differenti impostazioni di questi tre macroregolatori, si veda anche G. Resta, *Cosa c'è di "europeo" nella proposta di regolamento UE sull'intelligenza artificiale*, in *Il diritto dell'informazione e dell'informatica*, 2/2022, 323 ss.

DPCE online
ISSN: 2037-6677

combinata con il benessere europeo, imporrebbe all'industria digitale globale di adeguarsi al fine di vendere i propri prodotti nei territori UE, mentre ispirerebbe anche altre giurisdizioni a raggiungere analoghi livelli di tutela. La Cina, infine, avrebbe dalla sua una forte spinta agli investimenti, che proietterebbe non solo nel mercato interno, ma anche esternamente, condizionando i finanziamenti per gli interventi infrastrutturali nei Paesi in via di sviluppo all'acquisto di tecnologie cinesi: queste, a loro volta, imporrebbero a tali Paesi di adottare norme congruenti con quelle esistenti in Cina.

Sebbene si tratti di un'approssimazione, la metafora "imperiale" proposta da Bradford coglie nel segno, suggerendo che si tratterebbe di tre paradigmi normativi che, proprio come gli imperi, sono in grado di proiettare la propria influenza al di fuori dell'area sottoposta al loro diretto controllo. Non è dunque un caso che diversi dei contributi che si confrontano con la disciplina del digitale e dell'IA in diverse giurisdizioni finiscano inevitabilmente per rinvenire spesso soluzioni intermedie tra questi tre poli – segno che si tratta di elementi ispiratori dell'approccio regolatorio in numerosi contesti normativi.

Per chiudere con la metafora, Bradford preconizza tre diversi destini per i modelli: gli Stati Uniti sarebbero destinati al declino se non s'incamminano in un'attività regolatoria federale, finora confinata largamente ai singoli Stati, e in un rafforzamento dei diritti legati al digitale, mentre il successo del modello dell'Unione europea si mostra molto dipendente dalla sua potenza economica, che la rende punto di passaggio obbligato. Se l'analisi tuttavia pare in alcuni punti scricchiolare, come si vedrà più avanti, conviene partire proprio dal contesto che più ha maturato, prima con la normativa sulla protezione dei dati personali, poi con la normativa organica sull'IA, la reputazione di regolatore globale.

2. Le sfide viste dall'Europa

I contributi presentati nella sezione europea propongono uno spaccato degli interessanti quanto articolati quesiti derivanti da ciò che potremmo chiamare "la sfida dei dati": la raccolta, conservazione e trattamento di informazioni personali, ma anche di dati biometrici e genetici nonché di metadati[4] e tutte le interazioni che, spesso inconsapevolmente, ci fanno lasciare tracce nella rete[5], impongono al mondo del diritto di trovare risposte innovative ad una profonda e sempre rinnovata esigenza di garanzia della libertà informatica positiva, come la definiva Vittorio Frosini[6], o della autodeterminazione

[4] Si intende con tale termine l'"involucro delle comunicazioni elettroniche" (G. Caggiano, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *MediaLaws*, 2/2018, 65 ss).

[5] V. Zeno-Zencovich, *Dati, grandi dati, dati granulari e la nuova epistemiologia del giurista*, in *Medialaws*, 2/2018, 32 ss.

[6] V. Frosini, *La protezione della riservatezza nella società informatica*, in N. Matteucci, *Privacy e banche dei dati*, Bologna, 1981, 41 ss.

informativa, per prendere a prestito l'espressione impiegata in una nota sentenza del Tribunale costituzionale federale tedesco del 1983[7].

Il riconoscimento nelle carte costituzionali, nella giurisprudenza o nei testi sovranazionali dei diritti alla protezione dei dati e alla riservatezza[8], infatti, non può rappresentare punto statico e unico di salvaguardia; al contrario, il rapido progresso scientifico, tecnologico e informatico richiede con urgenza pressante soluzioni normative nuove – talvolta audaci –, insieme a tutele giurisdizionali attente ed interventi precisi di autorità indipendenti, quali le autorità garanti per la protezione dei dati. Ciò nella consapevolezza che non sono solo i diritti citati quelli messi in pericolo ma che con essi è in gioco il concetto costituzionalmente centrale della dignità umana, della libertà e, infine, della stessa democraticità delle nostre società, che vedono nell'assenza di un incontrollato e celato potere – pubblico o privato – di sorveglianza e profilazione sulle nostre informazioni – e sulla nostra vita – un baluardo irrinunciabile[9].

Proprio le domande che attengono ai rischi dell'impiego di dati – personali o "personalissimi", come nel caso dei dati biometrici – e alle soluzioni, spesso ancora *in fieri*, fornite da parlamenti, corti – nazionali e sovranazionali – o soggetti garanti con compiti di vigilanza e poteri sanzionatori, sono quindi poste al centro dei lavori presentati da giovani studiosi; questi hanno cercato di porre a sistema minacce tecnologiche e tentativi di reazione da parte del mondo del diritto e delle sue istituzioni, evidenziandone successi ma anche criticità e profili ancora in attesa di essere compiutamente affrontati e risolti.

In tale contesto non stupisce, allora, che l'esercizio di studio e approfondimento proposto nei tre contributi che si focalizzano sull'ambiente eurounitario si sia concentrato primariamente su talune particolari tipologie di dati: i dati raccolti nei *database* pubblici delle decisioni di merito, nell'elaborato di Valentina Capasso, e i dati biometrici – addirittura in grado di rivelare emozioni e stati d'animo – nelle analisi di Sabrina Akram Ibrahim El Sabi e Lorenzo Sottili. Ne emerge come i lavori presentati riescano a delineare "sfide dei dati" rese ancor più delicate o dal contesto in cui il trattamento avviene e al quale il dato appartiene, quello giudiziario, o dalla tipologia estremamente sensibile – per richiamare un termine che il Codice della privacy nostrano impiegava[10] – dei dati in gioco.

[7] BVerfG 65, NJW, 15 dicembre 1983. Per un commento, A. Di Martino, *La protezione dei dati personali*, in S. Panunzio (a cura di), *I diritti fondamentali e le Corti in Europa*, Napoli, 2005, 365 ss.

[8] Qui primario riferimento è alla Carta europea dei diritti fondamentali (c.d. Carta di Nizza). Tra i tanti, per un'analisi di questa e altre disposizioni, si veda F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016; sia consentito il rinvio a L. Scaffardi (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, 2017.

[9] Sull'intrinseco legame tra tutela della riservatezza, protezione dei dati, garanzia delle libertà e dignità, si legga, *ex multis*, S. Rodotà, *Privacy, libertà, dignità*, 2004, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293.

[10] Sul tema, sia consentito di rinviare, tra i tanti, a L. Scaffardi, *Il trattamento dei dati particolari: il dato genetico*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021, 249 ss.

DPCE online
ISSN: 2037-6677

Così è interessante evidenziare, per iniziare, come, nel contributo di Valentina Capasso, l'utilizzo di dati personali in grado di fornire informazioni circa il magistrato che ha adottato determinate decisioni apra a prospettive problematiche, che si intrecciano persino con la preservazione del corretto funzionamento della giustizia. Se siamo soliti pensare ai pericoli della profilazione ricordando il noto caso Cambridge Analytica[11], il lavoro proposto apre le prospettive di analisi a parimenti complessi e preoccupanti fenomeni di *profilage*, in questo caso riguardanti i magistrati e le loro linee interpretative del diritto; simili fenomeni possono condurre a nuove forme di *forum shopping*, di pressione nei confronti dei giudici e persino di minacce all'incolumità del magistrato stesso. In questo caso, dunque, il difficile bilanciamento ha ad oggetto esigenze contrapposte ma certamente rilevanti: la pubblicità delle decisioni e la tutela della protezione dei dati e della riservatezza degli operatori di giustizia nello svolgimento di un compito che può anche assumere tratti particolarmente delicati.

L'avvento dell'IA ha imposto, così, una riflessione ulteriore e ben più articolata rispetto al passato, che ravvisa nella elaborazione di algoritmi informatici il pericolo di addivenire ad una "giustizia predittiva" capace di minare equo processo e diritti fondamentali dei soggetti giudicanti, non solo – e non tanto – intesi come singoli individui, quanto più come facenti parti della magistratura intesa quale organo la cui immagine, funzione e funzionamento vanno salvaguardati con attenzione.

La richiesta, più che condivisibile e necessaria, di trasparenza e pubblicità delle decisioni da un lato e, dall'altro, di garanzia che i dati derivanti dalle decisioni giurisprudenziali non vengano impiegati per scopi di *judicial analytics* dagli esiti controversi, è stata posta alla base dell'analisi comparata; quest'ultima ha condotto l'Autrice ad osservare le diverse soluzioni regolatorie poste in campo in differenti ordinamenti, dal Belgio alla Francia, al Regno Unito, sino al contesto nostrano[12], nonché gli interventi di istituzioni sovranazionali, tra cui la "Commissione per l'efficienza della giustizia del Consiglio d'Europa" e la Corte di Giustizia dell'UE[13]. Il vaglio di proporzionalità e il bilanciamento, così oggetto di studio, hanno permesso di mettere in luce la necessità di una disciplina volta primariamente a determinare la possibilità di riutilizzo dei dati, così disponendo tutele intermedie che non eccedono né nella direzione di una trasparenza totalizzante, né in quella di una anonimizzazione assoluta.

Se il richiamato caso britannico del *Find Case Law Service* e la sua regolamentazione, che pone dei paletti ad una incontrollata analisi

[11] *Ex multis*, su questo noto caso, D. Messina, *Il Regolamento EU 2016/679 in materia di protezione dei dati personali alla luce della vicenda 'Cambridge Analytica'*, in *Federalismit.it*, 20/2018, 1 ss.; G. Ziccardi, *Tecnologie per il potere. Come usare i social network in politica*, Milano, 2019.

[12] Si fa riferimento qui alla banca dati pubblica delle decisioni di merito richiamata in apertura di contributo da Capasso e contenente le decisioni di Tribunali e Corti d'Appello a far data dal 2016.

[13] Sul punto, oltre al lavoro qui analizzato, si rinvia anche a C. Iannone, E. Salemme, *L'anonimizzazione delle decisioni giudiziarie della Corte di Giustizia e dei giudici degli Stati membri dell'Unione europea*, in A. Ciriello, G. Grasso, D. Lo Moro (a cura di), *Il trattamento dei dati personali in ambito giudiziario*, Quaderni della Scuola Superiore della Magistratura, 2021, 103 ss.

computazionale dei dati relativi ai casi – e dunque anche ai magistrati coinvolti nella decisione[14]–, pare poter essere osservato quale esempio virtuoso, il dibattito normativo risulta ancora tutt'altro che chiuso. Esso, anzi, mostra di essere ancora in divenire, con un punto di equilibrio e bilanciamento tutt'altro che semplice da tracciare; quest'ultimo merita senza dubbio ulteriori analisi e riflessioni capaci di adattarsi all'evolversi di un progresso tecnico-scientifico ed informatico che rende possibile analisi aggregate e algoritmiche dei dati dai sempre più imprevedibili risvolti per la tutela dei diritti fondamentali.

Simili sfide, dai contorni tutti in attesa di definizione, sono quelle tracciate poi da Sabrina Ibrahim El Sabi Akram e Lorenzo Sottile che focalizzano l'attenzione sulle – ancora in parte ignote – tecniche di determinazione delle emozioni (c.d. *emotion recognition systems*) la prima e di riconoscimento facciale il secondo. Del resto, una riflessione giuridica sulle nuove frontiere e sfide per la protezione dei dati non può ignorare, oggi, le richieste di tutela che emergono dall'impiego massiccio di dati biometrici[15], divenuto estremamente insidioso con l'avvento dell'IA e della capacità di quest'ultima di provvedere ad una lettura aggregata di una mole notevole di informazioni. Basti pensare all'utilizzo del riconoscimento facciale da parte di autorità di pubbliche, principalmente per finalità di salvaguardia della sicurezza, per il controllo di luoghi potenzialmente affollati quali stadi, metropolitane o aeroporti o, ancora, alle scuole[16]; ma anche da parte di soggetti privati che hanno compreso le potenzialità dei dati biometrici per finalità di controllo sui luoghi di lavoro o, più recentemente, per scopi commerciali, come mezzi di *micro-targeting*[17]. Come già ricordava Stefano Rodotà nel 2012[18], infatti, "si ricorre sempre più frequentemente a questi dati biometrici non solo per finalità d'identificazione o come chiave per l'accesso a diversi servizi, ma anche come elementi per classificazioni permanenti, per controlli ulteriori rispetto al momento dell'identificazione o dell'autenticazione/verifica, cioè della conferma di una identità". Queste parole paiono estremamente lungimiranti se lette alla luce degli ultimi sviluppi della tecnologia e dell'IA che paiono realizzare una pericolosa scomposizione dell'identità – di cui già Rodotà parlava – attraverso uno strumentario inedito e sofisticato capace persino di carpire – e sfruttare – informazioni che attengono alla sfera più intima di ciascuno di noi, quella delle emozioni, con sviluppi ancora poco esplorati ma evidentemente insidiosi.

[14] Messo a disposizione online dai *National Archives*.

[15] Con "dati biometrici" si fa riferimento a "dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici", Art. 4, co. 1, n. 14) del Reg. UE 679/2016, General Data Protection Regulation (GDPR).

[16] Sugli utilizzi del riconoscimento facciale da parte di autorità pubbliche, si veda ampiamente G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021.

[17] Su tale tematica, G. Lugli, M. Riani (a cura di), *Espressioni ed impronte facciali nel marketing*, Torino, 2018.

[18] S. Rodotà, *Il diritto di avere diritti*, Bari-Roma, 2012, 302.

DPCE online
ISSN: 2037-6677

Per quanto noti, e solo per fornire alcune coordinate preliminari, pare utile specificare che il riconoscimento facciale è da ricondursi alla branca del c.d. *deep learning*[19] e consiste, in estrema sintesi, in un trattamento automatizzato dei dati biometrici per finalità che possono andare dalla identificazione al riconoscimento, all'autenticazione sino alla categorizzazione di soggetti[20]. Ciò che viene svolto, anche mediante sistemi di IA fondati su algoritmi, è una operazione di *match* tra un'immagine – e quindi i dati biometrici catturati da un dispositivo, come ad esempio una telecamera – e i dati invece presenti all'interno di un *database* o una *watch list* di riferimento, laddove il riconoscimento avvenga secondo sistemi c.d. *one-to-many*[21]. Negli ultimi anni, poi, il progresso tecnologico ha determinato l'avvento di ulteriori evoluzioni: la creazione di sistemi di c.d. *facial emotional recognition*; attraverso il *machine learning*, quindi, sono esaminate le espressioni del viso, i movimenti del corpo ma anche il tono della voce e altri dati biometrici al fine di determinare una vera e propria classificazione di emozioni e stati d'animo. Questa avveniristica tecnologia rientra nella c.d. *affective computing*[22] ovvero quegli strumenti e processi che colgono, interpretano e tipizzano il linguaggio non verbale e che hanno conosciuto un salto notevole, prima impensabile, proprio con il diffondersi delle tecnologie di riconoscimento facciale e di IA. Il ricorso a tali strumenti è già oggetto di sperimentazione in diversi campi, dalla medicina – dove il *facial emotional recognition* viene utilizzato per verificare la risposta emotiva di un paziente ad una terapia, soprattutto nel caso di cure psichiatriche –, o ancora nell'ambito del marketing, per determinare il livello di gradimento e soddisfazione di un cliente o l'interesse verso specifici prodotti, così adottando tecniche di *micro targeting* e di precisa personalizzazione delle comunicazioni; in questo senso "quantifying, tracking and manipulating emotions is a growing part of the social media business model"[23].

In contesti diversi e ben più lontani – non solo geograficamente – dall'Europa, questi strumenti sono impiegati, in diversi progetti pilota, per stabilire l'umore e addirittura il livello di attenzione degli alunni a scuola o il livello di impegno di un lavoratore, in entrambi i casi con effetti piuttosto preoccupanti per la tutela dei diritti fondamentali[24]. In particolare, con

[19] Si rinvia, su questi profili tecnici, a P. Traverso, *Breve introduzione tecnica all'Intelligenza Artificiale*, in questa Rivista, 1/2022, 155 ss.

[20] Sul punto sia consentito di rinviare a L. Scaffardi, *Dati genetici e biometrici: nuove frontiere per le attività investigative*, in L. Scaffardi (a cura di) *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, cit., 37 ss.

[21] Nell'approccio *one-to-one* invece la comparazione non preveda un confronto (un *match*) con dati biometrici inseriti all'interno di un *database*. Sul punto, per considerazioni sulle differenti insidie per i diritti fondamentali che questi due diversi sistemi comportano, si legga G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le corti*, in questa Rivista, 2/2019, 1107 ss.

[22] Con tale termine si intende far riferimento a quella branca dell'IA che si pone quale obiettivo quello di rilevare comportamenti, emozioni e stati d'animo.

[23] P. Valcke, D. Clifford, V.K. Dessers, *Constitutional challenges in the emotional AI era*, in H.W Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (eds.), *Constitutional challenges in the algorithmic society*, Cambridge, 2021, 57 ss.

[24] È interessante osservare il caso cinese, in questo senso, in cui l'impiego sistematico di tecnologie di controllo biometrico è ormai pervasivo e diffuso in svariati ambiti e in

riferimento all'impiego di strumenti di classificazione delle emozioni, la libertà di espressione può risultare fortemente compressa da una onnipresente sorveglianza che permea persino la sfera più intima dell'individuo, quella della sua identità ed emozioni, che può condurre, in ultima analisi, ad una manipolazione della libertà di informazione e di autodeterminazione, che risultano essenziali tasselli per una libera formazione di convincimenti, personalità e identità[25].

A questi pericoli, tutt'altro che astratti, sono da sommarsi due ulteriori profili giuridici problematici che accomunano tutti i sistemi di riconoscimento fondati sull'impiego di dati biometrici: il *bias* algoritmico e suoi potenziali effetti discriminatori[26]. L'opacità, la scarsa conoscibilità degli algoritmi e del loro funzionamento devono essere tenuti in debita considerazione, specialmente quando decisioni fortemente impattanti sui diritti fondamentali vengono prese sulla base di tali tecnologie che debbono essere considerate nella loro fallibilità e nel margine di errore (o falsi *match*) ad essi connesso.

Simili insidie sono state ben riconosciute, del resto, in diversi documenti e dichiarazioni, tra cui il rapporto dell'European Parliamentary Research Service titolato *Regulating facial recognition in the EU* in cui si legge: "these second wave biometrics bear new and unprecedentedly stark risks for fundamental rights, most significantly the right to privacy and non-discrimination"[27]. Da simili considerazioni, condivise da diverse NGOs[28], si è aperta una discussione, in seno al Parlamento europeo quanto alla opportunità di richiedere un divieto generalizzato di impiego di queste tecnologie per scopi securitari, almeno per il periodo di tempo necessario a limitare i rischi e istituire una cornice regolatoria adeguata a salvaguardare i diritti fondamentali. Da qui, nel 2021, l'appello alla Commissione europea non solo di valutare una limitazione di sistemi di riconoscimento facciale in determinati luoghi pubblici, tra cui quelli relativi all'educazione (scuole o Università) o luoghi di cura, come ospedali, ma anche di introdurre uno specifico *ban* di tutti i sistemi di *biometric mass surveillance* negli spazi

tantissimi luoghi pubblici e privati. Sul punto, M. Standaert, *Smile for the camera: the dark side of China's emotion-recognition tech*, in *The Guardian*, 3 marzo 2021.

[25] Per riflessioni ampie su quanto controlli rispetto all'accesso alle informazioni e tecniche di manipolazione possano avere un impatto sull'autodeterminazione personale, sia consentito di rinviare a L. Scaffardi, *Internet fra auto-limitazione e controllo pubblico*, in *Rivista AIC*, 4/2023, 355 ss.

[26] Su questi temi centrali, si rinvia, tra i tanti, a: G. Mobilio, *Tecnologie di riconoscimento facciale*, cit.; R. Ducato, *Il riconoscimento facciale tra rischi di 'mitridatizzazione sociale' e prospettive di regolamentazione*, in L.E. Rios Vega, L. Scaffardi, I. Spigno (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Napoli, 2021, 187 ss.; F. Paolucci, O. Pollicino, *Digital constitutionalism to the test of the smart identity*, in *Journal of e-Learning and Knowledge Society*, 3/2022, 8 ss.

[27] European Parliamentary Research Service, *Regulating facial recognition in the EU*, 2021, PE 698.021.

[28] Tra le tante, NOYB, European Digital Rights, Privacy International. Molte di queste hanno peraltro sottoscritto nel settembre 2023 uno *statament* rivolto a governi e parlamenti europei e nazionali per addivenire ad un divieto totale di utilizzo di tecnologie di riconoscimento facciale per finalità di sorveglianza nei luoghi pubblici e come strumento di controllo alle frontiere (https://edri.org/our-work/global-civil-society-and-experts-statement-stop-facial-recognition-surveillance-now/).

DPCE online
ISSN: 2037-6677

pubblici[29]. Questi primi approcci regolatori hanno dimostrato così l'esigenza di soluzioni normative specifiche e ulteriori rispetto al quadro regolatorio ad oggi fornito dal noto GDPR. Quest'ultimo prevede all'Art. 9 una disciplina apposita per i dati biometrici, rientranti nella categoria particolare di dati e dei quali viene riconosciuta la delicatezza e l'unicità e dunque la necessità di tutele rafforzate e restrizioni ulteriori; all'Art. 22 invece rinveniamo apposite tutele per le decisioni automatizzate in grado di avere un impatto grave sugli individui; nonostante tali disposizioni, l'esigenza di considerare le insidie del tutto inedite derivanti dai sistemi di IA hanno portato ad aprire un dibattito legislativo di grande rilievo ed estremamente innovativo: quello sul c.d. *AI Act*, di cui si attende, al momento in cui si scrive, la pubblicazione nella Gazzetta Ufficiale dell'UE[30].

È proprio sui profili di criticità determinati dal quadro normativo europeo vigente, sulle prospettive di innovazione sancite nell'*AI Act* nonché sulle sfide ancora aperte che si sono concentrati i contributi di Lorenzo Sottile e Sabrina El Sabi; i loro lavori, infatti, si sono spinti a opportune quanto importanti riflessioni sul dibattito normativo *in fieri*, anche in ottica

[29] Si fa riferimento alla Risoluzione del Parlamento europeo del 6 ottobre 2021, nella quale viene richiesto l'intervento della Commissione europea al fine di sancire "una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto con funzione di identificazione, a meno che non siano usate strettamente ai fini dell'identificazione delle vittime di reati, finché le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali, i risultati ottenuti siano privi di distorsioni e non discriminatori, il quadro giuridico fornisca salvaguardie rigorose contro l'utilizzo improprio e un attento controllo democratico e adeguata vigilanza, e vi sia la prova empirica della necessità e proporzionalità della diffusione di tali tecnologie; osserva che i sistemi non dovrebbero essere utilizzati o diffusi nei casi in cui i criteri di cui sopra non siano soddisfatti", para. 27.

[30] Si fa riferimento al grande osservato speciale di questi ultimi anni: il Regolamento europeo sull'Intelligenza Artificiale (*AI Act*), che ha ottenuto approvazione dai legislatori eurounitari ma che non è ancora stato pubblicato nella Gazzetta ufficiale dell'UE. Merita sin da ora evidenziare che, in attesa di leggere tale importante atto, la cui applicazione sarà comunque integrale solo dal 2026 (da quanto ad oggi disponibile), si rilevano iniziative a livello di Stati membri: "queste proposte normative si muovono nello spazio lasciato libero dall'Ai Act il quale definisce l'accesso al mercato europeo dei sistemi e dei prodotti di intelligenza artificiale, classificandoli in base al rischio che essi possono causare, e richiedendo attività di *compliance* differenti a seconda del livello di rischio. Il legislatore europeo ha ritenuto di tutelare, con questo approccio, i valori e i diritti fondamentali", G. Finocchiaro, *In attesa dell'Ai Act fervono le proposte*, in *Sole24Ore*, 9 maggio 2024. Come sottolineato anche dal Presidente del Garante per la protezione dei dati personali, Pasquale Stanzione, tratto distintivo dell'*AI Act* europeo "(anche rispetto a scelte di altri ordinamenti, come si evince dal raffronto con il Biden Administration's Executive Order on Artificial Intelligence), risiede, infatti, nella scelta preliminare in favore di una regolazione volta a coniugare l'innovazione con la tutela dei diritti e delle libertà fondamentali dai rischi potenzialmente derivanti da un uso scorretto dell'i.a." (*Segnalazione al Parlamento e al Governo sull'Autorità per l'i.a.*, 25 marzo 2024, Doc. 9996493). Per alcuni commenti su questo nuovo Regolamento, dalla fase della sua iniziale proposta ai più recenti sviluppi: A. Simoncini, E. Cremona, *La AI fra pubblico e privato*, in questa Rivista, 1/2022, 253 ss.; C. Casonato, *Unlocking the synergy: Artificial Intelligence and (old and new) Human Rights*, in *BioLaw Journal*, 3/2023, 2 ss.; V. Zeno-Zencovich, *Artificial intelligence, natural stupidity and other legal idiocies*, in *MediaLaws*, 1/2024, 1 ss.; F. Paolucci, *Whatever it takes? The AI Act regulatory crucible*, in *Diritti comparati*, 22 gennaio 2024.

comparata, nonché sulla rilevanza dell'intervento tanto di corti quanto di autorità garanti nel campo delle tecniche di riconoscimento. El Sabi, nella sua accurata disamina delle tecnologie di IA utilizzate per riconoscere le emozioni e predire sentimenti e stati d'animo, ha fatto riferimento proprio al richiamato *AI Act* europeo, ponendo particolare attenzione alle esigenze di tutela finalizzate ad assicurare la protezione di una categoria specifica di soggetti vulnerabili, cioè gli anziani, cui spesso tali sistemi sono rivolti. Se pare evidente – almeno dalla versione del testo normativo ad oggi disponibile – il divieto assoluto di questi strumenti in specifici luoghi, quali istituti di insegnamento e luoghi di lavoro, restano più sfumati e in parte ancora da determinarsi con precisione e concretezza i limiti e le condizioni di impiego in altri ambiti[31], tra cui appunto quelli assistenziali o sanitari che potrebbero riguardare proprio soggetti fragili. Nello specifico, l'attuazione e i limiti sanciti da principi indispensabili quali la garanzia della *privacy by design*, la trasparenza, la minimizzazione dei dati, la non discriminazione e la tracciabilità sono tutti da verificare e vi è da chiedersi, come fa l'Autrice, se e come l'opacità giuridica e la natura scientificamente – ed eticamente – discutibile delle *Emotion Tech* possano essere affrontate e risolte compiutamente dalle disposizioni normative proposte nell'*AI Act*. La lettura combinata di quest'ultimo Regolamento e delle tutele offerte già dal GDPR, nonché di disposizioni nazionali cui i Regolamenti stessi lasciano un certo margine di azione[32] meriteranno certamente riflessioni approfondite che dovranno contemperare esigenze di tutela dalle dimensioni e caratteri innovativi e in continuo movimento, da un lato, e normative per loro natura piuttosto statiche, dalla cui elasticità e capacità di predisporre garanzie anche dinnanzi ad inediti sviluppi della scienza e della tecnologia dipenderà l'efficacia e la portata stessa dell'assetto regolatorio europeo.

Vagliare questi profili, ancora in attesa di piena definizione, risulta di grande interesse sotto il profilo comparato, per determinare differenze di approcci e soluzioni virtuose specialmente rispetto allo scenario oltreoceano, negli Stati Uniti, dove il frammentario panorama legislativo richiamato dall'Autrice pare esemplificativo di un approccio *business friendly* e meno rigido, che al momento fissa ampi principi generali e discipline di dettaglio solo in determinati e ristretti ambiti[33].

---

[31] Alcune prime analisi dell'impatto dell'*AI Act* sulle tecnologie di riconoscimento facciale, per quanto talune basate sulla versione non definitiva del Regolamento, sono reperibili: I. Barkane, *Questioning the EU proposal for an AI Act: the need for prohibitions and a stricter approach to biometric surveillance*, in 27 *Information Policy* 155, 2022; G. Mobilio, *Your face is not new to me. Regulating the surveillance power of facial recognition technologies*, in 12(1) *Internet Policy Review* 1, 2023; F. Paolucci, *AI Act e riconoscimento facciale: I rischi di delegare la questione agli Stati membri*, in *Agenda Digitale*, 26 aprile 2024.

[32] G. Finocchiaro, *In attesa dell'Ai Act fervono le proposte*, cit.

[33] Basti pensare alle disposizioni adottate da talune città come San Francisco, che vietano taluni impieghi dei sistemi di riconoscimento facciale in luoghi pubblici. Per alcuni spunti di riflessione sulla diversa regolamentazione dell'IA al di là e al di qua dell'Oceano, si legga: B. Marchetti, L. Parona, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in questa Rivista, 1/2022, 237 ss; M. Bassini, *The global race to regulate AI: Biden's Executive Order spillover effects on the EU AI Act*, in *IEP@BU*, dicembre 2023; ma si vedano sul punto anche le riflessioni di Andrea Pin, nel prosieguo del presente contributo.

DPCE online
ISSN: 2037-6677

Se sul fronte dei sistemi di riconoscimento delle emozioni, dunque, restano ancora prospettive di studio ampie e aperte, anche le tecnologie di riconoscimento facciale per scopi securitari continuano a porre sfide regolatorie che attendono di essere pienamente risolte.

Sotto questo profilo, il contributo di Lorenzo Sottile permette di porre in evidenza non solo il portato degli interventi legislativi in questi ambiti contraddistinti da nuove ed emergenti tecnologie, bensì anche il rilievo delle decisioni giurisprudenziali o di autorità garanti per la protezione dei dati. Osservando il caso studio specifico dell'impiego di tecniche di *facial recognition* negli stadi di calcio europei, vengono pertanto illustrati una serie di diversi provvedimenti o sentenze adottate nel Regno Unito, in Danimarca, in Italia, in Francia e infine in Spagna che concernono la legittimità dell'impiego di simili strumenti. Questo esercizio di comparazione consente di mettere in luce questioni critiche caratterizzanti soprattutto la determinazione di quei limiti e condizioni che l'attuale assetto normativo europeo, formato primariamente dal GDPR e dalla direttiva 2016/680/UE sulla protezione dei dati nelle attività di polizia e giudiziarie (c.d. LED), stabilisce quando vi sono in gioco necessità di *law enforcement* e quindi di prevenzione, indagine e perseguimento di reati o minacce alla sicurezza pubblica e nazionale.

Non è un caso, dunque, che proprio l'impiego di tecnologie di riconoscimento facciale per finalità securitarie si sia moltiplicato nell'ultimo decennio, divenendo oggetto di attenzione da parte di corti nazionali o sovranazionali; emblematico è il richiamo alle vicende giurisprudenziali registratesi nel Regno Unito, in cui una corte per la prima volta si è occupata della legittimità di tali sistemi e della compatibilità con i diritti fondamentali sanciti, nel caso inglese, nella Convenzione europea per i diritti dell'uomo. Ebbene, la controversia ha visto sottoporre a vaglio il sistema di *Automated facial recognition* impiegato dalla polizia del *South Wales* a partire dal 2017 con un progetto pilota basato sull'utilizzo di una *watch list* contenente i dati biometrici di soggetti attenzionati dalle forze di polizia, quali ricercati, soggetti con precedenti o con ordini di restrizione o ancora soggetti vulnerabili o di interesse per l'intelligence.

È bene sin da ora precisare come talune salvaguardie fossero inizialmente previste: i dati raccolti dalle telecamere e utilizzati per essere raffrontati con la citata *watch list* venivano immediatamente distrutti a seguito di un *match* negativo; era assicurata una supervisione umana delle operazioni; veniva garantita una corretta informativa circa l'esistenza di sistemi di riconoscimento facciale operativi in determinate aree, ad esempio attraverso l'esposizione di cartelli segnaletici che garantivano quindi un minimo di trasparenza quanto alle operazioni disposte. In questo noto caso[34], la *Civil Division* della *Court of Appeal* nel *South Wales* ha ribaltato la sentenza di primo grado e riconosciuto la mancata proporzionalità dell'ingerenza operata dalla tecnologia in esame rispetto alle finalità perseguite nonché

[34] Sentenza *Bridges v. The Chief Constable of South Wales Police et al.*, Case n. C1/2019/2670 del 11 agosto 2020. Per un commento della sentenza di primo grado: A. Pin, *Non esiste la "pallottola d'argento": l'artificial face recognition al vaglio giudiziario per la prima volta*, in questa Rivista, 4/2019, 3175 ss.

l'inadeguatezza delle salvaguardie predisposte[35], sollevando anche il problema ormai riconosciuto dei rischi di c.d. discriminazione algoritmica e dunque di affidabilità del sistema nel suo complesso.

Se questo primo intervento giurisprudenziale ha destato grande interesse, esso non rappresenta un caso isolato: altre corti, benché ad oggi non ancora numerose, si sono occupate di strumenti di riconoscimento facciale in tempi più o meno recenti. Cito, ad esempio, la decisione del Tribunale amministrativo di Marsiglia del 2020[36] con riferimento all'uso di tale tecnologia all'interno delle scuole per scopi securitari (impiego che aveva ricevuto peraltro un parere negativo da parte del CNIL[37], l'autorità garante dei dati francese); ma anche la sentenza della Corte europea dei diritti dell'uomo nel caso *Glukhin c. Russia*[38] che ha condannato la Federazione russa per violazione degli Articoli 8 e 10 della Convenzione europea dei diritti dell'uomo con riferimento all'impiego di strumenti di riconoscimento facciale per – quantomeno dichiarati – scopi di tutela della sicurezza e dell'ordine pubblico.

L'elevata intrusività di queste tecnologie è stata rilevata poi anche da diverse Autorità garanti della protezione dei dati nazionali: al di là degli interessanti casi concernenti lo specifico impiego negli stadi, nel contesto nostrano meritano certamente un breve richiamo anche altri provvedimenti del Garante per la protezione dei dati che si è confrontato con la complessità delle sfide poste da tali tecnologie dettando principi e indicazioni interpretative delle normative vigenti di grande interesse. Nel caso di sistemi semplici di *face detection*, che prevedono una memorizzazione breve e limitata a pochi secondi e che non comportano una conservazione di dati biometrici, anzi prevedendo una anonimizzazione delle informazioni trattate solo a fini statistici, il Garante si è pronunciato, con decisione n. 7496252 del gennaio 2018, quanto alla legittimità del trattamento derivante dalle colonnine pubblicitarie usate nella Stazione centrale di Milano che miravano a determinare solo il sesso, l'età e l'espressione facciale dello spettatore dinnanzi alla pubblicità/totem. In quel caso, con tutta evidenza di gran lunga meno invasivo rispetto ai sistemi di riconoscimento facciale che operano un *match* con una *watch list*, il Garante ha infatti avuto l'occasione di affermare come "l'impiego di software di elaborazione in grado di estrapolare dati di tipo statistico dalle immagini riprese in modo pressoché immediato, senza elaborazioni biometriche né registrazioni di immagini né accessi live valgono a far ritenere che siano previste adeguate cautele affinché non siano messi a rischio i diritti e le libertà fondamentali nonché la dignità e la riservatezza

[35] L. Woods, *Automated facial recognition in the UK: The Bridges Case and beyond*, in 6(3) *European Data Protection Law Review* 455, 2020.

[36] Tribunale amministrativo di Marsiglia, n. 1901249, 3 febbraio 2020.

[37] *Commission nationale de l'informatique et des libertés.*

[38] Corte EDU, *Glukhin c. Russia*, n. 1519/20, del 4 luglio 2023. Per alcuni commenti, si rinvia a G. Gallo, *Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso Glukhin c. Russia dinnanzi alla Corte europea dei diritti dell'uomo*, in *MediaLaws*, 3/2023, 189 ss.; G. Mobilio, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso Glukhin c. Russia*, in questa Rivista, 1/2024, 695; C. Nardocci, *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU Glukhin c. Russia*, in *BioLaw Journal*, 1/2024, 279 ss.

DPCE online
ISSN: 2037-6677

degli interessati"; in tal modo è stata quindi operata una distinzione tra "profilazione con identificazione" e "profilazione senza identificazione", così che quest'ultima è stata considerata più attenta alla privacy e meno invasiva.

Ad un diverso esito ha invece portato l'intervento del Garante nel 2021, con riferimento a ben più sofisticati strumenti di riconoscimento *real time* disposti dal sistema S.A.R.I. Con provvedimento del 25 marzo 2021[39], il Garante, in questo caso, ha rilevato l'esistenza di minacce per la riservatezza e la protezione dei dati, derivanti da un sistema impiegato su larga scala e riguardante anche soggetti non previamente sottoposti all'attenzione delle forze dell'ordine. Nonostante la cancellazione immediata dei dati una volta rilevato il mancato *match* con una *watch list*, secondo il Garante è da ritenersi nondimeno sussistente un trattamento biometrico e di confronto dei dati stessi che può condurre alla realizzazione di una forma di sorveglianza universale e non mirata; ciò in assenza peraltro di una specifica previsione normativa che disciplini nel dettaglio la raccolta e il trattamento dei dati biometrici e che disponga salvaguardie specifiche nonché una valutazione di proporzionalità e stretta necessità di tali strumenti.

E ancora, il 10 febbraio 2022, con Ordinanza di ingiunzione[40], il Garante ha sanzionato Clearview AI per aver realizzato un pericoloso e illegittimo "monitoraggio biometrico", reso possibile dalla creazione di un *database* di immagini ma anche di dati di geolocalizzazione estratti dal web; questo avrebbe consentito la predisposizione di sofisticate forme di profilazione e financo tracciamento dei cittadini italiani e dei soggetti che si trovano sul territorio italiano. L'assenza di una base giuridica, di un legittimo interesse, del rispetto di principi di trasparenza, di limitazione del trattamento entro i confini della finalità comunicate ai soggetti interessati nonché di limitazione della conservazione, hanno condotto il Garante a rilevare una violazione del diritto alla riservatezza e alla non discriminazione.

Infine, più recentemente, vi è di certo il caso estremamente interessante quanto articolato che ha visto il Comune di Trento destinatario del provvedimento del Garante. Con disposizione n. 9977020 del 11 gennaio 2024, è stata infatti comminata una sanzione per illecito trattamento dei dati personali – tra cui anche dati biometrici – posto in essere dal Comune di Trento nella realizzazione dei progetti di ricerca scientifica Marvel e Protector (co-finanziati peraltro dall'UE) e volti alla realizzazione di strumenti tecnologici nell'ambito delle c.d. *smart cities*. Le violazioni del GDPR rilevate dal Garante hanno riguardato sistemi di raccolta e trattamento mediante IA di dati biometrici, pur anonimizzati, ottenuti da strumenti di videosorveglianza o mediante raccolta di messaggi e commenti presenti sui social. Ancora una volta, l'assenza di un quadro giuridico idoneo a legittimare una invasione così significativa nella privacy e nella garanzia di protezione dei dati nonché carenze in termini di salvaguardie (per esempio rilevando rischio di reidentificazione) o ancora sotto il profilo delle garanzie di trasparenza e di una appropriata valutazione dei rischi e d'impatto, hanno portato il Garante a bloccare forme di trattamento di dati personali così

[39] Su tale provvedimento, E. Raffiotta, M. Baroni, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in *BioLaw Journal*, 1/2022, 165 ss.

[40] Registro dei provvedimenti n. 50 del 10 febbraio 2022.

delicati come quelli biometrici. Meritevole di attenzione è l'affermazione dell'Autorità stessa che riconosce come "simili forme di sorveglianza negli spazi pubblici possono modificare il comportamento delle persone e condizionare anche l'esercizio delle libertà democratiche"[41].

Questi esempi, così rapidamente richiamati e aventi ad oggetto diverse forme di trattamento dei dati biometrici basate sulla lettura aggregata dei dati o sull'impiego di strumenti di IA, dimostrano non solo l'attivismo e l'attenzione del nostro Garante ma anche la difficoltà da parte di aziende ed enti pubblici di porre in essere tecnologie in grado di rispettare appieno le normative vigenti, in primis il GDPR, e, in ultima istanza, quindi, conformi a quei diritti e valori così essenziali per la salvaguardia di una società veramente libera da manipolazioni e ingerenze illecite nella sfera personale dei consociati.

Insomma, volendo in conclusione tentare di trarre considerazioni di insieme dai contributi presentati nella prima sessione, è possibile innanzitutto muovere due ordini di riflessioni. La prima e più immediata consente di sottolineare il carattere ancora estremamente aperto e oggetto di vivace discussione che contraddistingue la "sfida dei dati" nel contesto europeo – e non solo –, dinnanzi all'affermarsi e al propagarsi rapido di strumenti di IA. Sia con riferimento ai dati biometrici, sia ai dati personali che vengono in gioco nell'ambito giurisdizionale, gli scenari di sviluppo appaiono tutti ancora in via di determinazione e debbono pertanto essere osservati – e con ciò giungo alla seconda valutazione – sotto tre diverse direttrici da considerare con attenzione e nel loro intrecciarsi: quella normativa, quella giurisdizionale e quella che vede l'intervento delle autorità garanti della protezione dei dati.

Sotto il primo profilo, in estrema sintesi, le soluzioni normative vedono l'UE impegnata a valutare con attenzione le evoluzioni dell'*AI Act* e i suoi riverberi sulla normativa nazionale. È innegabile che tale inedito ed estremamente significativo sforzo regolatorio abbia tenuto in grande considerazione i rischi derivanti da tecnologie di IA quali quelle fondate sull'uso dei dati biometrici: nel determinare livelli diversificati di rischio, i legislatori sovranazionali hanno previsto coraggiosi divieti generalizzati di impiego di talune tecnologie[42] ma hanno anche disposto eccezionali condizioni alle quali l'impiego di strumenti anche invasivi è legittimato e considerato proporzionato. È proprio il caso di taluni sistemi di riconoscimento facciale, laddove impiegati allo scopo di garantire la sicurezza – per esempio dinnanzi a minacce terroristiche –. Le previste eccezioni sono accompagnate da specifiche salvaguardie, tra cui conviene sottolineare la necessità di un previo *impact assessment* e l'autorizzazione da parte di un'autorità giudiziaria o amministrativa indipendente. Lasciando però un certo margine di intervento agli Stati membri, almeno nella versione del testo ad oggi disponibile, la futura attuazione e la portata garantista e restrittiva di tale atto regolatorio è ancora difficile da definire con precisione;

[41] Così si legge nel comunicato stampa del Garante del 25 gennaio 2024 (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9977299).

[42] Si pensi alle tecnologie di *social scoring* già impiegate in taluni ordinamenti, quale quello cinese; sul punto, si rinvia al contributo di Vanessa Previti, commentato da A. Pin nel prosieguo di questo contributo e pubblicato in questa Rivista.

DPCE online
ISSN: 2037-6677

e del resto, fino ad ora, sono state anche la flessibilità e la discrezionalità lasciate, entro taluni limiti, ai legislatori o alle autorità nazionali con riferimento a GDPR e LED, ad aver condotto talvolta ad una frammentarietà e disomogeneità di soluzioni, come il caso studio sul riconoscimento facciale negli stadi di calcio proposto da Lorenzo Sottile ha ben dimostrato. Una elasticità che, forse, potrebbe essere difficilmente superabile e che senza dubbio ha rappresentato una sfida per le Istituzioni europee, impegnate a garantire da un lato un elevato standard di tutela dei diritti fondamentali per assicurare la centralità dell'uomo nello sviluppo e implementazione di sistemi di IA, mentre dall'altro lato ha dovuto fare i conti tanto con un quadro di riparto di competenze tra UE e Stati membri che limita in taluni ambiti la portata di azione della prima, quanto con l'esigenza di scongiurare il pericolo di una rigidità eccessiva dell'assetto normativo; una rigidità tale da poter danneggiare gli investimenti nell'innovazione in ambito europeo e la delocalizzazione di aziende operanti nel settore dello sviluppo dell'IA in ordinamenti dotati di un impianto normativo meno restrittivo ed oneroso.

Il dibattito che si sta sviluppando in Europa è tuttavia parte di uno scenario dinamico più ampio, che mostra come diversi regimi dosino in modo diverso preoccupazioni analoghe, conducendo a soluzioni solo in parte convergenti e talvolta persino significativamente differenti.

3. Le sfide nel mondo

Nei contributi raccolti nella sezione extraeuropea si identificano abbastanza agevolmente alcuni denominatori comuni. In questo senso, tali lavori permettono di leggere "in trasparenza" il momento attuale, nel quale, seppur per ragioni e con traiettorie diverse, i tre "imperi" appaiono tutti impegnati a coniugare una protezione dei diritti della persona – ciò che è sovente confluito nella macrocategoria della privacy e più ampiamente dei dati personali – e insieme a regolarne il loro uso. Questo si documenta nella contemporanea fioritura di normative o quantomeno di tentativi regolatori mirati sulla privacy e sull'IA, i quali paiono a questo punto quali mezzi indispensabili e non sostituibili l'uno all'altro. È infatti ormai superata la convinzione che l'IA possa essere tenuta sotto controllo limitandone soprattutto la capacità di acquisire e processare i dati personali tramite i quali essa si addestra e sviluppa la profilazione e targetizzazione massiva. Come Woodrow Hartzog – insieme ad altri – ha efficacemente messo in luce, è infatti impraticabile attribuire alla nozione del "consenso" dell'interessato un ruolo-valvola, consentendo a ciascuno di decidere se condividere o meno i propri dati con l'interfaccia[43]. L'uso pervasivo di internet e di numerosi oggetti *smart*, unito ad un sapiente *design*, ha consentito – e tuttora consente – ai protagonisti del web di ottenere agevolmente i dati che loro interessano: spuntare le informative privacy ad ogni accesso ad un sito web è talmente complesso e laborioso che ciascuno tende ad accettare le condizioni del sito senza riguardo per la propria privacy. In buona sostanza, sembra di assistere ad una contesa sui dati che generalmente i singoli perdono a favore dei

[43] W. Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*, Cambridge (Mass.), 2018.

protagonisti del web, con effetti di due ordini: in primo luogo, un fenomeno di pervasivo monitoraggio, sorveglianza e profilazione degli utenti che condividono i dati; in secondo luogo, un potenziamento delle tecniche di IA, che possono ottenere un *training* più ricco e completo proprio grazie ai dati messi loro a disposizione e che dunque possono sviluppare inferenze anche riguardo a utenti meno proclivi a condividere i propri dati. Questo secondo aspetto pare di non secondaria importanza, in quanto evidenzia che il problema della tutela dei dati non riguarda semplicemente gli individui che condividono i propri dati, ma la generalità su cui si riversa una IA potenziata da questi ultimi.

Maria Vittoria Malinconi, ad esempio, mostra la vulnerabilità della condizione femminile al tema, che ha preso piede negli Stati Uniti ma con ripercussioni potenzialmente globali, delle *Femtech*: le industrie che mappano la salute riproduttiva femminile, con effetti a cascata su una molteplicità di piani – da quello lavorativo a quello familiare, fino a quello sanitario o sociale. Come il lavoro dell'autrice mette in luce, si tratta di un enorme mercato, che inevitabilmente attira l'attenzione e l'interesse dei giganti digitali. Esso si nutre dell'interesse delle utenti a monitorare la propria salute, per utilizzarne i dati in maniera per nulla controllata Oltreoceano e limitata a fatica dalla tutela dei dati personali nell'Unione europea. Il fenomeno delle *Femtech* è dunque paradigmatico di un processo di condivisione del dato che nasce su base volontaria, ma che si irradia orizzontalmente nella vita della singola donna e della società nel suo complesso: le informazioni sulle tendenze delle donne che utilizzano tali app possono infatti essere incrociate con altri dati per tentare delle inferenze capaci di mappare l'intera popolazione, femminile e non soltanto.

La contesa tra singoli e potenze digitali si sviluppa lungo la dorsale normativa, con sviluppatori e imprese impegnati ad estrarre il massimo potenziale dai dati raccolti, ricavandosi spazi di lavoro ai margini delle normative che regolano la privacy. Sembra di assistere dunque ad una dinamica che vede l'attività normativa spingere chi fa tecnologia a ideare nuovi strumenti per sfruttarne le potenzialità in modo lecito almeno formalmente: la medesima corsa al *design* per carpire il consenso rappresenta una risposta alle normative sulla tutela dei dati personali. Se l'esperienza insegna, sarà forse da attendersi un atteggiamento simile nei confronti dell'*AI Act*, che, con la distinzione della disciplina applicabile sulla base del grado di rischio dell'attività, imporrà a chi se ne occupa di decidere che grado di rischio assumersi per scegliere il tipo di IA da sviluppare e dove operare. In altri termini, la parabola della privacy pare suggerire che, più che vietare alcune formule tecnologiche e imporre delle salvaguardie, con la legislazione si possano indicare delle linee di sviluppo del settore.

Ne è un esempio il contributo di Valentina Cavani relativo ai dati sintetici. Se per un lungo tratto i dati sono stati considerati il nuovo petrolio per l'economia globale, lo sviluppo delle norme a tutela dei dati personali ha fatto dei dati sintetici una sorta di nuovo combustibile, capace di offrire la quadratura del cerchio tra tutela dei dati ed estrazione di valore dalle informazioni relative agli utenti. I dati sintetici, infatti, come spiega l'autrice, seppure in grado diverso mantengono diverse proprietà del dato personale senza tuttavia averne la qualifica – offrono in sostanza un valore senza dover sottostare, ad esempio, al GDPR. Si tratta tuttavia di un campo ancora solo

DPCE online
ISSN: 2037-6677

in parte inesplorato, persino nella sua fondamentale qualifica – alcuni tipi di dati sintetici sono infatti in alcuni casi riconducibili al soggetto da cui sono originati, e dunque il loro utilizzo potrebbe esporre il fianco, nuovamente, alla identificazione che il GDPR sorveglia tanto attentamente.

Altro esempio di questo tentativo di quadrare il cerchio è la logica della privacy differenziale – una nozione che Roberta Nobile esplora nella sua complessità, suggerendone il carattere bifronte. Da un lato, l'idea di differenziare la privacy sulla base del dato e del suo utilizzo pare ricalcare gli orientamenti più recenti anche nel campo della normazione dell'Unione europea: la stessa nozione di rischio che presiede lo sviluppo dell'IA nell'*AI Act* tenta infatti di superare la logica contenuta nel GDPR, che contrappone la protezione dei dati personali alla loro raccolta e condivisione. Queste sono in effetti due alternative piuttosto radicali, cui ha fatto da cerniera lo strumento del consenso, che normalmente permette di raccogliere e utilizzare dati altrimenti non attingibili. D'altronde, per quanto importante, l'idea di privacy differenziale non è in sé risolutiva ma anzi pone nuove sfide, sia perché postula che il dato non circoli se non nell'area di interesse alla quale è destinato, sia perché richiede un bilanciamento che, come il contributo mette in luce, si presenta delicato e caratterizzato da un forte tecnicismo e da una particolare complessità, poiché chi stabilisce gli standard deve contemperare criteri molto eterogenei, che dipendono dagli interessi coinvolti e dalla vulnerabilità degli strumenti che elaborano e conservano le informazioni.

Alcuni contributi mettono in luce, inoltre, come la relazione tra poteri pubblici e privati non sia sempre la medesima, soprattutto quando si tratta di usare le tecnologie e in particolare l'IA per meglio conoscere, controllare e profilare le persone: talvolta istituzioni pubbliche e *Big Tech* sembrano impegnate in maniera simile nell'utilizzare in maniera diffusa le tecnologie digitali anche a sacrificio dei diritti individuali. Nei loro contributi, infatti, Vanessa Previti e Alberto Orlando pongono in luce alcune delle dinamiche che coinvolgono simmetricamente poteri pubblici e privati, ugualmente coinvolti in pratiche controverse: il *social scoring* e il riconoscimento facciale. Si tratta di ambiti nei quali, per ragioni diverse, gli "imperi digitali" mostrano strane ma comprensibili sovrapposizioni. Il *social scoring* o le tecniche di riconoscimento automatico non sono aspetti di un nuovo *Panopticon* immaginato da Bentham, ripreso da Foucault, e approdato solo in Cina, sebbene sia senz'altro vero che in quest'ultimo contesto più che altrove strumenti di monitoraggio massivo controllano la popolazione, talvolta irrogano sanzioni automaticamente esecutive e classificano le persone, distribuendo privilegi o limitazioni in maniera opaca, inducendo in tal modo non semplicemente una forma di obbedienza alla legge, ma una vera e propria soggezione al potere: se gli individui non possono prevedere le conseguenze delle loro azioni, essi terranno un atteggiamento remissivo e prudente in tutte le circostanze in cui avvertono di essere potenzialmente sorvegliati[44].

Queste tecniche, per ragioni di sicurezza e tutela, sono ampiamente utilizzate anche in Occidente. Se gli Stati Uniti conoscono il *social scoring* e forme di identificazione facciale condotti da privati, entrambe queste formule

[44] M. Foucault, *Surveiller et punir: naissance de la prison*, Parigi, 2003, 197-201.

vengono utilizzate o sono utilizzabili in Europa, in modo diverso, dai pubblici poteri. Talvolta il loro sviluppo trova un'eco insospettabile: ormai strumenti di valutazione e ricompensa si rinvengono non solo sul piano statale, ma persino substatale e locale – in Italia diversi enti locali sono ricorsi a strumenti premiali o sanzionatori che valutano il comportamento delle persone sulla base di indici più o meno complessi[45]. Le premesse di questo uso pervasivo delle tecnologie dunque non sono sempre ed inevitabilmente di stampo economico e imprenditoriale, né si contraddistinguono per una forte ascendenza autocratica. Al contrario, le condizioni fondamentali possono essere poste dalla regolazione e dall'atteggiamento tenuto da istituzioni democratiche, le quali possono nel tempo mutare con la percezione sociale e con le prevalenti istanze politiche: in tempi di incertezza, le esigenze di sicurezza possono promuovere forme di controllo sociale pervasivo, mentre epoche di ristagno possono stimolare il recupero di un'economia basata sui dati e sull'IA anche al prezzo di erodere la riservatezza e l'autodeterminazione dei cittadini.

Sebbene l'Unione europea, insieme a molti altri ordinamenti che appaiono seguirla da vicino, affermi con insistenza che i "dati personali non possono essere considerati un bene disponibile"[46] e più generalmente di voler generare uno sviluppo tecnologico che riflette le esigenze delle persone, la lotta per assicurare l'effettività di questi principi-cardine sta scontando diverse difficoltà. Tali resistenze non derivano soltanto di un rapporto impari tra i singoli e i protagonisti del web, ma anche da un forte interesse pubblico al controllo sociale.

A queste esigenze se ne aggiungono altre che, come si anticipava, paiono far scricchiolare l'opinione secondo cui l'approccio regolatorio dell'UE sarebbe più fortunato di altri. Se, da un lato, sia l'*AI Act* sia ad esempio il *Digital Services Act* interpretano la necessità di andare oltre la tutela dei dati, al contempo aprono spazi all'utilizzo e allo sviluppo del digitale da cui sembra trapelare un certo affanno europeo nel tenersi al passo della rivoluzione digitale e dello spazio che altri ordinamenti le riservano – ad esempio imponendo solo alle grandi piattaforme alcuni obblighi di sorveglianza e protocolli.

Queste misure da un lato mostrano di voler stimolare – o quantomeno non impedire con misure troppo draconiane – l'ingresso di nuove realtà più piccole, che sarebbero altrimenti incapaci di ottemperare ai requisiti imposti alle attività più rischiose o più affermate. Al contempo, tali soluzioni però mostrano la consapevolezza che la capacità dell'UE di garantire a sé stessa un ambiente *online* sicuro passa attraverso la sua prosperità economica e un certo primato commerciale.

[45] A.D. Signorelli, *Vite a punti: il credito sociale tenta anche i Comuni italiani*, *Wired*, 13 ottobre 2022, https://www.wired.it/article/credito-sociale-italia-comuni/.

[46] La recente decisione dell'European Data Protection Board, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, 17 aprile 2024, par. 130, definisce in tali termini il divieto di considerare i dati una "tradeable commodity".

DPCE online
ISSN: 2037-6677

Se l'UE ha governato con il suo *Effetto Bruxelles*[47] (altro fortunato conio di Anu Bradford) l'agenda nel mondo, va in effetti riconosciuto che questo primato è conteso sia dalle altre giurisdizioni sia dai grandi protagonisti del digitale, i quali si trovano in una situazione di quasi-monopolio che consente loro di limitare l'impatto normativo anche dell'UE, adeguandovisi solo nella misura del necessario, mentre perseguono la massima espansione altrove. Valga in questo senso il caso di *Chat-GPT*, il quale ha effettivamente ottemperato alle misure richieste dal Garante Privacy italiano, ma, secondo quanto afferma l'informativa che Open AI ha pubblicato sul sito web del suo *large language model*, si è limitato ad estendere tali tutele soltanto all'area interessata dall'ordinamento dell'Unione europea. Il ruolo probabilmente per il momento senza pari di *Chat-GPT* gli consente dunque di dettare le condizioni alle quali erogare i propri servizi ove tali norme non valgono: gli utenti infatti non hanno altre opzioni realistiche, in quanto non esistono servizi alternativi ugualmente efficaci messi a disposizione da operatori più attenti alla loro tutela.

Gli autori qui coinvolti sembrano offrire al lettore varie e importanti sottolineature di fenomeni più vasti, cogliendo sia la fase di transizione da una protezione dei dati a una sua integrazione con la regolazione dell'IA, sia la sfaccettata relazione tra poteri pubblici e privati, talvolta conflittuale ma spesso concorrente, sia infine la continua fuga in avanti (e altrove) di chi sviluppa la tecnologia. Si tratta di un campo di forze molto composito, nel quale, come è stato fatto notare, prendono forma contemporaneamente tecnologie che valorizzano sottomissione e gerarchia, come le tecniche di sorveglianza, accanto a quelle della privacy differenziale o dei dati sintetici, che tendono a promuovere le esigenze individuali[48].

4. Conclusioni

L'interventismo e l'apporto delle corti e, in maniera al momento ancor più marcata, delle autorità indipendenti rappresenta una duplice ulteriore prospettiva di osservazione della "sfida dei dati", che non può essere letta solo nell'ottica delle soluzioni normative. I provvedimenti del Garante nostrano, anche dinnanzi a nuove frontiere dell'IA e dell'impiego di dati biometrici, hanno evidenziato l'accentuato ruolo che tali autorità di controllo sono sempre più chiamate ad assumere[49], chiarendo, interpretando e attuando il diritto nazionale ed europeo in una materia così delicata e in rapido divenire quale la protezione dei dati.

---

[47] A. Bradford, *The Brussels effect: how the European Union rules the world*, New York, 2020.

[48] Per riprendere le osservazioni di M. Tegmark, *Life 3.0. Being Human in the Age of Artificial Intelligence*, New York, 152-153.

[49] Per un approfondimento del ruolo del Garante, si rinvia a L. Califano, *Il ruolo di vigilanza e l'esercizio del potere sanzionatorio del Garante per la protezione dei dati personali*, in L. Califano, V. Fiorillo, F. Galli, *La protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale*, Giappichelli, 2023, 109 ss.; ma anche V. Pagnanelli, *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, in *Osservatorio sulle fonti*, 2/2021, p. 783 ss.

Dinnanzi alle sfide profonde e senza precedenti portate dalla rivoluzione dell'IA, servirà di certo l'azione congiunta di legislatori, corti e autorità di controllo per poter assicurare la piena realizzazione di un "umanesimo digitale"[50] che sappia cioè indirizzare digitalizzazione e datificazione verso la salvaguardia dei diritti fondamentali, dello stato di diritto, del costituzionalismo[51]. Grandi passi avanti sono stati certamente fatti ma tanto ancora bisogna fare per colmare quello che Massimo Luciani recentemente ha definito un "dislivello prometeico", richiamando Gunther Anders[52], cioè la distanza che caratterizza il progresso tecnologico e la capacità di governarlo e gestirne appieno le conseguenze.

In ultima analisi, sta maturando, ma solo con fatica e lentamente, la convinzione che nel passaggio da una regolazione dei dati alla disciplina dell'IA ci si stia inoltrando all'interno di un campo di forze molto più stratificato, nel quale interessi pubblici e privati si dispongono in maniera talvolta confliggente, talvolta congruente. In tale scenario magmatico sembra emergere potentemente, e trasversalmente, quantomeno nella dottrina, ma talvolta anche nella giurisprudenza e nella vita delle istituzioni di sorveglianza, l'esigenza di una *governance* della tecnologia che tenga conto non solo degli interessi individuali, ma anche di quelli sociali e politici[53]. Da una contrapposizione tra *Big Tech* e privati si passa ad una triade nella quale sono compresenti anche considerazioni sistemiche, relative al funzionamento delle istituzioni. Come conciliare tale triade è una delle sfide che attendono al varco la dottrina.

Andrea Pin
Dipartimento di Diritto pubblico, internazionale e comunitario
Università degli studi di Padova
andrea.pin@unipd.it

Lucia Scaffardi
Dipartimento di Giurisprudenza, studi politici e internazionali
Università di Parma
lucia.scaffardi@unipr.it

[50] Parla di umanesimo digitale A. Soro, *Democrazia e potere dei dati: libertà, algoritmi, umanesimo digitale*, Milano, 2019.

[51] In questi termini G. Cerrina Feroni, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9977187.

[52] M. Luciani, *La sfida dell'Intelligenza artificiale*, in Associazione Italiana dei Costituzionalisti (La Lettera), 12/2023, https://www.associazionedeicostituzionalisti.it/it/la-lettera/12-2023-liberta-di-ricerca-e-intelligenza-artificiale/la-sfida-dell-intelligenza-artificiale.

[53] J. Simons, *Algorithms for the People: Democracy in the Age of AI*, Princeton-Oxford, 2023, 207.

DPCE online
ISSN: 2037-6677