Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*

Federica Paolucci

Abstract

L'incidenza di nuovi strumenti di sorveglianza su base biometrica è sempre maggiore, imponendo una riflessione circa la effettiva necessità di un loro impiego massivo, data la loro intrusività. In particolare, la presente analisi si propone di osservare le conseguenze giuridiche che discendono dall'installazione di tecnologie basate su sistemi di riconoscimento facciale. Dopo aver, dunque, esaminato l'aspetto sociale e tecnico circa il loro funzionamento, si inserirà il fenomeno all'interno della più ampia problematica dell'obsolescenza normativa. Una mancanza di guida circa l'adozione del riconoscimento facciale non sta solamente mancando di giudizio *pro futuro*, ma sta minando a due sostanziali componenti del diritto pubblico: l'esercizio della sovranità statale, da un lato, e la protezione dei diritti fondamentali dei cittadini, dall'altro.

The employment of means of surveillance based on biometric data is every year higher provoking the emerging of many questions about the effective necessity of their massive use and application. Those very intrusive technological instruments are observed in this paper by ascertaining the constitutional and legal issues with particular referral to facial recognition. Once facing a short scrutiny of the social and technical aspects, it is delivered an analysis of the phenomenon by looking at the dangerous lack of an ad hoc legal framework for the use of such technologies. This legislative obsolescence is creating void spaces directly mining both the State stability and sovereignty, and the protection of the fundamental rights and freedoms

Sommario

Keywords

riconoscimento facciale - diritti fondamentali – sorveglianza – privacy - dati biometrici

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco"

1. Introduzione

50 miliardi di dollari è il valore che il settore biometrico acquisirà entro il 2024 secondo la stima di *Global Martket Insight*[1], azienda leader nelle ricerche di mercato. Un dato economico che cela, tuttavia, una massiva diffusione di tecnologie in grado di raccogliere, processare ed elaborare risposte sulla base di dati afferenti alle «caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca»[2]: i c.d. dati biometrici. Ne comunichiamo e condividiamo quotidianamente un grande quantitativo – dall'impronta digitale al battito cardiaco, passando appunto per il riconoscimento facciale – senza renderci effettivamente conto del fatto che dietro l'upload di un *selfie*, si nasconde molto di più di un puro e semplice scambio di *like*.
Le conseguenze di tale avvenirismo tecnologico si riversano precipuamente sul piano giuridico ed etico[3]. Stiamo assistendo a cambiamenti epocali che avvengono grazie e a causa della persistente digitalizzazione. Uno dei suoi peculiari fenomeni è, per l'appunto, il riconoscimento facciale, assunto in questa sede quale caso esemplare del connubio, progressivamente più indissolubile, tra sorveglianza e tecnologia. È, dunque, proprio vero che abbiamo tutto grazie a questo incessante interscambio di informazioni, o il prezzo che ci accingiamo pagare sarà sempre più alto? E che ruolo assumono, dunque, i diritti fondamentali nell'epoca del riconoscimento facciale?

1.1. Un *selfie* è solo un *selfie*?

«*Today's selfie is tomorrow biometric profile*»[4]: il *selfie* di oggi è la profilazione biometrica di domani. Nonostante il valore iperbolico di questa frase, i nostri *selfie*, e, più in generale, le foto che, con una certa noncuranza, carichiamo sui profili social, sono sottoposte ad un incessante e raffinato processo di analisi, in grado di raccogliere dati, anche relativi ai nostri volti. Caricare una foto su Facebook[5] significa dare ad un algoritmo l'opportunità di allenarsi a riconoscere meglio il nostro volto. Lo smartphone, così come l'intera pletora di *device* che costellano la quotidianità di ognuno di noi, aspira a conoscere cosa vogliamo, prima che il desiderio della cosa stessa diventi manifesto. Tale meccanismo è efficacemente denominato da Shoshana Zuboff[6], autrice dell'omonimo

[1] Il dato ivi citato proviene dall'analisi di mercato pubblicata da Global Market Insight con riferimento al periodo 2017-2024 in *Biometrics Market Size, Growth – Industry Share Report 2017-2024*, *Global Market Insights Inc.*, agosto 2017.

[2] Definizione di dati biometrici rintracciabile all'art. 4, par. 1, n. 14, Regolamento (UE) 2016/679 (General Data Protection Regulation, da qui in avanti, "GDPR").

[3] Le stesse verranno esaminate nel corso di questa breve analisi, ma sono state ricapitolate con un'efficace espressione, «possiamo vivere senza essere uno Stato di sicurezza», da F. Chiusi in *Intelligenza artificiale e riconoscimento facciale: perché la società della sorveglianza digitale non è più accettabile*, in *Valigia Blu*, aprile 2020.

[4] La citazione proviene dal *Think Privacy Project* dell'artista ed attivista Adam Harvey.

[5] È lo stesso social network a spiegare come funziona il proprio riconoscimento facciale.

[6] S. Zuboff, *The Age of Surveillance Capitalism,* London, 2019. La teoria della Zuboff, già docente

best-seller, capitalismo della sorveglianza: un sistema economico e sociale parassitico che si sostanzia in una logica accumulatrice di dati personali. Una raccolta che acceca qualsiasi uso propositivo e positivo della potenza tecnologica, ma lascia il posto ad un lugubre meccanismo interessato esclusivamente ad un'intersecazione tra domanda e offerta. Ogni utente della rete sta materialmente contribuendo alla continuazione di siffatto meccanismo di raccolta di dati ed informazioni. Il punto critico di tale tossicità ciclica non è semplicemente situato nelle modalità più o meno invasive di raccolta e conservazione del dato, bensì nell'esacerbata mancanza di controllo da parte dell'interessato delle informazioni – e del loro valore – che condivide attraverso e per mezzo di un caleidoscopio sempre più ampio di strumenti intelligenti.

L'oggetto di tale attività è essenzialmente legato alle radici della quotidianità: al di fuori dei dati che sono raccolti al puro e semplice scopo di migliorare un prodotto ovvero usufruire di un servizio, vi è una corposa, e tutt'altro che residuale, parte classificabile, secondo l'analisi di Zuboff, come «*behavioral surplus*»[7]: vale a dire analisi comportamentali delle azioni degli utenti che vengono utilizzate, da chi si occupa della raccolta del dato, come base per predire le sue scelte, andando a formare il c.d. *dataset*.

Tali analisi che hanno ad oggetto i comportamenti dei clienti non sono per nulla una novità istituita dalla rivoluzione digitalizzante della così detta «*uncanny valley*»[8]. Basti pensare, difatti, agli studi di mercato condotti da attività di ogni tipo, da supermercati[9] a partiti politici: tutti vogliono mettere le mani sul mezzo più prodigioso per raccogliere informazioni. Si tratta di un modello sistemico di raccolta dati che collega l'efficienza accumulatrice del *machine learning*[10] alla ricerca di profitto delle maggiori *corporations*

presso l'Università di Harvard, è tanto mai acuta quanto profondamente inquietante. Se trent'anni fa un supermercato avesse chiesto di installare nelle nostre case un microfono diretto con il loro servizio clienti di modo tale da avere carrelli sempre personalizzati, pieni di prodotti che corrispondono ai nostri gusti, avremmo risposto di no. Ora, le nostre abitazioni sono piene di Alexa, *smart devices* di ogni tipo: e semplicemente incrociamo le dita. La logica con cui questi strumenti sono costruiti è una logica accumulatrice, spinta dalle maggiori imprese. Tali dati, una volta analizzati, consentono profitto: divengono dati predittivi con i quali chi li possiede è in grado di orientare gusti, comportamenti, sentimenti ed emozioni dell'utente che ha fornito il «dato rozzo» iniziale.

[7] L'autrice, descrivendo il funzionamento del capitalismo della sorveglianza, spiega il collegamento tra surplus comportamentale ed analisi predittive: «*although some of these data are applied to product or service improvement, the rest are declared as a proprietary behavioral surplus, fed into advanced manufacturing processes known as "machine intelligence," and fabricated into prediction products that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace for behavioral predictions that I call behavioral futures markets*», S. Zuboff, *The Age of surveillance capitalism,* cit., 7.

[8] Il riferimento è al *memoir* scritto da Anna Wiener analista precedentemente attiva nella Silicon Valley, nome chiaramente storpiato dall'autrice in Uncanny Valley per sottolineare l'aurea misteriosa di cui si ammantano le attività che, nascendo dalla stessa, stanno impattando sulle vite di ognuno. A. Wiener, *Uncanny Valley: A Memoir*, New York, 2020.

[9] Si menziona la raccolta dati condotta da Wal-Mart, catena americana di supermercati, che decise di piazzare le birre nello scaffale accanto ai pannolini, come risultato di un'analisi di mercato con ad oggetto i comportamenti dei loro clienti, come descritto in *Diaper-Beer Syndrome*, in *Forbes*, 1998.

[10] Dall'idea di *learning machine* di Alan Turing a Sybil, il programma adoperato da Google per svolgere predizioni circa il comportamento degli utenti, molto è cambiato, ma l'idea di base è sempre la medesima: «insegnare ai computer ciò che gli umani già fanno, ma con migliori risultati» come spiega P. Domingos in *The Master of Algorithm. How the Quest for the Ultimate Learning Machine Will Remake Our World,* Londra, 2017.

del globo, applicando i meccanismi delle *economies of scale*[11] ai dati. Questi ultimi non sono solamente il nuovo petrolio[12]: sono il mezzo che decreta conoscenza e potere in capo a coloro che hanno le risorse e le modalità per potenziare la raccolta e l'analisi delle informazioni.

Lungi dal condannare *tout court* questo sistema o richiamare moniti del tipo «siamo sorvegliati»[13] o, ancora, «la privacy è morta»[14], è da evitare anche un certo atteggiamento non attento ai rischi che un incontrollato uso di certe tecnologie può provocare. La sorveglianza non è più, difatti, qualcosa che svolgono soltanto i cinque occhi[15] del globo, rendendoci oggetti passivi di un sistema panottico[16]. La sorveglianza è uno stile di vita[17] cui ogni individuo sta più o meno consapevolmente contribuendo, adeguandosi ad una sistematica che lo pone sul fiume dei dati raccolti «su di noi ma non per noi[18]». Si tratta di un archetipo che non consiste nella mera ricezione di notifiche relative a prodotti che potrebbero interessare, ovvero, contatti che si potrebbe conoscere: significa, altresì, essere riconoscibili da tutti, in ogni momento, ovunque.

Il riconoscimento facciale è lo *specimen* alla base della moderna concezione di sorveglianza: si tratta di una tecnologia con un enorme potenziale, ma altamente intrusiva, che dovrebbe necessitare ancora di molto studio dati gli errori (*bias*) che ancora commette sul piano decisionale, prima di una sua commercializzazione onde evitare spaventose derive datacratiche[19]. In un contesto come quello che stiamo sperimentando, dove la tecnologia è una parte integrante e fondamentale della nostra vita, è quanto mai cruciale riflettere sulle conseguenze giuridiche derivanti da una diffusione, tanto

[11] Con tale termine si indicano le c.d. economie di scala che mettono in relazione l'aumento della scala di produzione con la diminuzione dei costi. Come evidenzia S. Zuboff, *The Age of Surveillance Capitalism*, cit., 202, l'intelligenza artificiale, alla base del funzionamento dei network, necessita grandi quantità di dati, che consentono, grazie alla loro varietà, la realizzazione di predizioni sempre più precise. Questo meccanismo conduce alla estensione del mondo dei click e dei dati nel mondo offline: aspetto di cui le Internet of Things e il riconoscimento facciale sono, per l'appunto, specimen, portando così alla realizzazione di quel *behavioural surplus* di cui si diceva.

[12] Come suggeriva la ormai iconica immagine apparsa su *The Economist* in *The world's most valuable resource is no longer oil, but data,* 6 maggio 2017.

[13] Basti pensare alla famosa introduzione della serie tv fantascientifica, *Person of Interest*, diretta da Jonathan Nolan.

[14] Spunto da cui ironicamente parte H. Mance in *Is Privacy Dead?*, in *Financial Times*, 19 luglio 2019.

[15] Ci riferiamo alla Five Eyes Alliance rivelata da Edward Snowden, già tecnico della CIA, con la pubblicazione di numerosi documenti della NSA recanti informazioni circa un sistema di sorveglianza costruito dal Governo statunitense con altre quattro nazioni, Australia, Canada, Nuova Zelanda, Regno Unito, come riportato in Glenn Greenwald*, No place to hide - Sotto controllo. Edward Snowden e la sorveglianza di massa,* Milano, 2014.

[16] Un classico sul tema della sorveglianza, v. J. Bentham, *Panopticon o la casa d'ispezione,* Milano, 1997.

[17] Teoria elaborata da David Lyon per spiegare come l'odierna maniera di sorvegliare è resa possibile dai comportamenti di ognuno di noi, dai nostri click, dalle nostre foto. V. D. Lyon in *The Culture of Surveillance: Watching as a Way of Life,* Cambridge, 2018.

[18] Espressione adoperata da S. Zuboff, *The Age of Surveillance Capitalism,* cit., 11, per sottolineare come l'individuo sia sempre più sprovvisto di un controllo sui propri dati, entrando anch'egli nella logica accumulatrice alla base del capitalismo della sorveglianza

[19] Il riferimento è alla Datacrazia, più semplicemente, governo del dato: quella forma di governo che si verrebbe a sostanziare con la piena realizzazione del capitalismo della sorveglianza, come suggerito da D. Gambetta in *Datacrazia: Politica, cultura algoritmica e conflitti al tempo dei big data*, Roma, 2018.

a livello pubblico quanto a livello privato, di un sistema che consente la raccolta, l'analisi ed il *processing* dei nostri volti – sia con riferimento a quelli raccolti da telecamere di sorveglianza, sia osservando quegli algoritmi che consentono a piattaforme, quali Instagram o Facebook, di riconoscere il nostro volto. Per tal ragione, iniziando con una breve analisi relativa al funzionamento del riconoscimento facciale, arriveremo a comprendere quali sono i diritti fondamentali in gioco, evidenziando un quadro di grave opacità normativa, che contribuisce a rendere la sorveglianza la vera piaga del nostro secolo.

2. Dati biometrici e riconoscimento facciale

Definiti «categorie speciali di dati personali»[20] in quanto capaci di comunicare informazioni quali le origini etniche o razziali di un individuo, i dati biometrici sono un "concetto ombrello", in quanto, all'interno di questa definizione, si concentrano tipologie di dati molto diversi tra loro[21]. Sono rintracciabili due principali categorie: l'una riferita a dati di tipo fisiologico e l'altra a quelli di tipo comportamentale. All'interno della prima classificazione troviamo dispositivi in grado di riconoscere le impronte digitali, la geometria delle nostre mani, e, ancora, l'odore, l'iride, il DNA, ed il volto. La seconda, invece, si riferisce alla raccolta di informazioni circa il comportamento, il riconoscimento vocale, l'analisi della firma, *etc.* Com'è chiaro la nostra analisi si baserà esclusivamente sulla prima categoria di dati e, in particolare, sul riconoscimento facciale.
I dati biometrici ci mostrano come i nostri corpi siano sempre più tecnologici, nel senso che sono l'oggetto di un processo di de-composizione ove ogni aspetto viene raccolto, conservato e consegnato ad una macchina con lo scopo di sottoporlo ad un raffinato processo di analisi algoritmica. Si pensi ai vantaggi derivanti dalla possibilità di avere un *device* che possa segnalare un infarto incipiente, oppure la carenza di vitamine, o ancora, difficoltà respiratorie: non è del tutto da condannare. Tuttavia, riprendendo la domanda che ci siamo posti inizialmente, occorre chiederci: a che prezzo stiamo cedendo il controllo sui nostri «gemelli digitali»[22] – quel *cloud* di informazioni che riflette ciò che siamo sotto forma di dati e codici – e, per converso sui nostri dati? La privacy intesa al modo di Warren e Brandeis rappresentava il diritto ad essere lasciati soli[23]: la *peace of mind* che si ottiene escludendo intrusioni esterne nella sfera privata dell'individuo. Un'immagine che è fortemente discordante con l'idea sottesa l'impiego

[20] Oltre all'osservata definizione nel GDPR, i dati biometrici sono definiti *special categories of personal data* dall'art. 10, par. 1, direttiva (UE) 2016/680 (Law Enforcement Directive). Una speciale categoria in quanto da questi dati si hanno delle peculiari informazioni circa l'individuo da cui i dati sono estratti: essi rivelano importanti aspetti quali le menzionate origini etniche e razziali, l'appartenenza ad un gruppo religioso o politico. Dati in grado di indentificare in maniera unica ed inequivocabile un individuo, quali dati che riguardano la sua salute o, ancora, il suo orientamento sessuale, come anche suggerito dalla lettura dell'art. 9 par. 1 del GDPR.

[21] Per un approfondimento tecnico degli aspetti menzionati si consiglia la lettura dei testi che sono stati consultati sul punto, quali J. D. Woodward, *Biometrics: A Look at Facial Recognition, Documented Briefing Rand Corporation*, DB-396-PSJ, 2003.

[22] M. Rossignaud - D. De Kerckhove, *Oltre Orwell. Il gemello digitale,* Roma, 2020.

[23] S. D. Warren - L. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 5, 1890, 193 ss.

sempre più massivo di *devices* da parte di pubblico e privato: reattivi al motto "*the more data the better*" agiscono creando una crasi tra raccolta dei dati e controllo degli stessi, ove, *a fortiori*, l'esercizio del secondo da parte dell'interessato era lo scopo precipuo perseguito dal GDPR. Tali forme di sorveglianza ci portano, al contrario, indietro di quasi un secolo, tratteggiando un modo di intendere la protezione dei dati non tanto come un diritto positivo, quanto come un diritto negativo, orientata ad escludere taluno (tanto lo Stato quanto il privato) dalla propria sfera privata.
Si viene a tratteggiare, dunque, non solo un problema di sorveglianza, bensì una nuova relazione dell'individuo con i dati che gli sono pertinenti: non abbiamo a che fare solamente con strumenti che raccolgono informazioni relativi a comportamenti, gusti, pensieri ed opinioni, bensì con tecnologie in grado di arrivare ad aspetti unici ed insostituibili della persona umana, come nel caso della biometria[24]. Il corpo, così come il volto, diviene, dunque, «un set di coordinate nel tempo e nello spazio, ove le sensazioni e le azioni vengono tradotte in dati»[25]: un processo che consente la comunicazione di caratteristiche che rendono ognuno di noi unico ed inimitabile, con lo scopo di individuarci ed indentificarci sulla base di un processo statistico[26]. Concludendo su questo punto di criticità social-digitale, procediamo con l'analisi della problematica dal punto di vista tecnico e giuridico.

2.1. Dietro la macchina: cos'è il riconoscimento facciale?

Il riconoscimento facciale appartiene alla branca del *deep learning* e può definirsi come «il trattamento automatico di immagini digitali contenenti volti di individui, per scopi di identificazione, autenticazione/verifica, o categorizzazione di suddetti individui»[27]. Il nostro volto può, dunque, essere utilizzato per sbloccare lo *smartphone*; può essere rilevato da telecamere a circuito chiuso, per compararlo a quelli presenti in una lista di sospetti; ed, ancora, per verificare l'identità digitale, a supporto della PA nel passaggio da burocrazia cartacea a quella supportata da strumenti analogici; all'entrata di palazzi, quali uffici o palestre; all'interno delle procedure di e-boarding in numerosi aeroporti; a fini commerciali, per registrare il livello di gradimento della clientela, nell'ambito del c.d. emotive marketing. Tutti questi possibili utilizzi sono identificabili come riconoscimento facciale, ma numerosi possono essere gli aspetti che li distinguono, soprattutto con riferimento al grado di intrusività di ciascuno di essi[28]. Possono, difatti, essere studiati in cinque sottogruppi[29]:

[24] Come suggerito nel podcast *Te lo si legge in faccia. Riconoscimento facciale e pregiudizi*, di Casual Future, se viene violata una nostra password siamo, anzitutto, in grado di poter intervenire modificandola e scegliendone un'altra. Se ciò avviene al database contenente i nostri dati biometrici, e, più precisamente, il nostro volto, non possiamo di certo tutelarci cambiandolo.

[25] S. Zuboff, *The Age of Surveillance Capitalism,* cit.

[26] R. King, *What Are Biometrics?*, in *Biometric Update*, 24 January 2016.

[27] Tale definizione proviene dall'art. 29 del Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services*, 00727/12/EN, WP 192, Brussels, 22 March 2012, 2.

[28] Sul punto si veda *The Many Faces of Facial Recognition in the EU*, in *EDRi,* 18 dicembre 2019.

[29] Una nota sul metodo adottato: la classificazione ivi riportata è stata elaborata da chi scrive per

Detenzione: si tratta del primo step che il dispositivo svolge di raccolta del volto, passaggio che banalmente si verifica quando sblocchiamo lo *smartphone*;

Raggruppamento: tale processo comporta l'abbinamento di immagini simili a partire da un data set con foto diverse tra loro. Ciò consente di procedere con il passaggio successivo;

Match – identificazione[30]: consiste nell'abbinare un'immagine ad una specifica persona. Si differenzia dal mero raggruppamento, in quanto questo consente di creare un database di voti simili senza abbinarli ad un singolo individuo, cosa che avviene, invece, nel caso del "match", che l'algoritmo fa con preesistenti fotografie relative ad uno specifico individuo[31];

Verifica – autenticazione: questi sono due atti relativi ad una comparazione *one-to-one*. Con questa espressione si intende il processo di comparare due profili biometrici con un'immagine che si crede possa riferirsi a sola una delle due persone. Il processo di verifica consiste nel controllare che la persona raffigurata sia effettivamente quella fisicamente individuata, mentre quello di autenticazione si estrinseca nell'affermazione che la persona raffigurata è quella che sembrava;

Classificazione – categorizzazione[32]: quest'ultimo punto è il più cruciale di tutto il discorso attorno al riconoscimento facciale. Difatti, dopo aver raccolto un'immagine, averla posta in comparazione con un database di volti, aver, conseguentemente, individuato una persona e aver compreso, attraverso un calcolo probabilistico, che è raffigurata nella foto, il passo successivo è procedere con un'analisi di quel dato. Una foto non è una semplice foto dal momento in cui possono essere ricavate delle ulteriori informazioni preziosissime, quali l'appartenenza ad un gruppo politico, o altri aspetti personali che permettono, di converso, la creazione di categorie e classificazioni di quegli individui i cui volti sono stati sottoposti a riconoscimento facciale.

Dall'enucleazione appena presentata emerge, in maniera chiara, come non sia sempre

---

rendere più chiara e fruibile la sottolineata differenziazione tra i diversi tipi di riconoscimento facciale, grazie alla lettura integrata di FRA, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* e V. Woodward and Rand Corporation, *Facial Recognition: Defining Terms to Clarify Challenges*, 13 novembre 2019.

30 In tema di identificazione all'interno dell'appena citato studio a cura della FRA, Fundamental Rights Agency, *ibid.*, si specifica che «*identification means that the template of a person's facial image is compared to many other templates stored in a database to find out if his or her image is stored there*».

31 Un diverso discorso giova farlo con riferimento al *Live Facial Recognition Technology* (qui di seguito, LFRT), in quanto tale tecnologia svolge un processo di identificazione a partire da immagini ottenute tramite clip live. La problematica che emerge con questo genere di FRT è una generale imprecisione dell'algoritmo, in quanto, circa l'accuratezza del riconoscimento, molto dipende dalla posizione della telecamera o, ad esempio, dall'esposizione del volto alla luce, come specificano P. Fussey e D. Murray, in *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, The Human Rights, Big Data and Technology Project - University of Sussex, 2019

32 La terminologia riportata nel testo segue quanto adottato dalla FRA.

facile la realizzazione di un ragionamento per scatole chiuse quando abbiamo a che fare con il riconoscimento facciale. Tale considerazione dovrebbe guidare il legislatore – *ça va sans dire*, quello europeo[33] – nel progettare un adeguato utilizzo della tecnologia in esame. L'atteggiamento avveniristico che, al contrario, osserviamo, non senza un certo sgomento[34], sembra ricalcare le ombre di Pilato delegando una decisione chiara sul tema, all'interpretazione del GDPR[35] e al ruolo pretorio dei giudici europei e nazionali, chiamati a svolgere un *risk assessment* basato su un'analisi caso per caso, e non su una regola certa, sebbene la *Rule of Law* sia uno dei principi cardine del diritto Europeo[36]. Si tratta di una (non) presa di posizione quanto mai rischiosa, dal momento che l'incremento della presenza di questo «*unwanted gaze*»[37]sta contribuendo a modificare radicalmente ed irrimediabilmente i parametri della nostra società contemporanea.

Dal punto di vista regolatorio, occorre prendere atto del fatto che già lo scorso gennaio[38], – prima che l'emergenza provocata dal virus SARS-COV-2 diventasse la massima urgenza nelle agende politiche dell'intero globo – la Commissione Europea, nell'ambito dei lavori di scrittura del *White Paper on Artificial Intelligence*, stava considerando la possibilità di istituire un *moratorium* di cinque anni con ad oggetto proprio l'uso del FRT[39] negli spazi aperti al pubblico. Una misura che da ultimo non è stata adottata, lasciando ancora una volta in sospeso un gran numero di questioni relative al suo legittimo utilizzo nella cornice del diritto eurounitario.

Una situazione tale non va solo a minare il pacifico godimento dei diritti fondamentali, ma incide irrimediabilmente sull'esercizio del potere da parte delle istituzioni statali. Il rischio quanto mai impellente è che il vuoto lasciato dall'obsolescenza normativa venga riempito da altri attori del panorama digitale frammentando, in tal maniera, lo

[33] Si fa menzione di un necessario intervento a livello comunitario in quanto il legislatore italiano non ha preso nemmeno in considerazione la problematica, demandando al Garante della Privacy un controllo circa la legalità dei sistemi implementati a livello locale. Nonostante ciò, molte città, dalle piccole Macerata e Como, alle più grandi Firenze e Milano, hanno installato suddetti mezzi di sorveglianza, come evidenziato da B. Calderini, in *Riconoscimento facciale, il quadro internazionale: norme, mercato e sfide etiche,* in *Agenda Digitale,* 7 ottobre 2020. Una menzione particolare la merita il database SARI, impiegato dalla polizia scientifica a Como, che riporta un notevole numero di *bias*, come menziona Wired Italia in un'inchiesta a cura di R. Angius e R. Colluccini, in Riconoscimento facciale, nel database di Sari quasi 8 schedati su 10 sono stranieri, in *Wired*, 3 aprile 2019.

[34] Si vedano, in particolare, sul punto i numerosi report pubblicati da organizzazioni internazionali, quali Amnesty International e la stessa ONU, sui quali è possibile trovare un accurato commento a cura di B. Calderini, in *Sorveglianza, Europa sotto accusa: così rafforza i regimi e indebolisce i diritti umani*, in *Agenda Digitale*, 23 novembre 2020.

[35] Documento fondamentale ma non sufficiente, in quanto si fa menzione della problematica al solo art.9, precedentemente menzionato. Il GDPR ha posto i limiti, attraverso i principi che promulga, entro i quali ci si dovrebbe muovere nel trattare dati biometrici, quali quelli raccolti attraverso il riconoscimento facciale. Tuttavia, un quadro normative di riferimento è ancora mancante.

[36] Art. 2, Trattato sull'Unione europea (Treaty of Lisbon, 2007/C 306/01).

[37] Sul punto si richiama l'omonimo titolo di J. Rosen, *The unwanted gaze: The destruction of privacy in America*, New York, 2011.

[38] Il riferimento è alle consultazioni che hanno preceduto l'adozione del White Paper on Artificial Intelligence, nel febbraio del 2020. Circa il mancato *deal* sul moratorium si faccia riferimento a L. Pascu in *EU No Longer Considering Facial Recognition Ban in Public Spaces*, in *Biometric Update*, 30 gennaio 2020.

[39] Abbreviazione di Facial Recongition Technology (FRT): termine usato in alternativa a riconoscimento facciale.

Stato come istituzione di diritto. Si tratta, difatti, di un fenomeno descrivibile con l'espressione «*diabolical persistence*»[40]: *errare humanum est, perseverare autem diabolicum,* dicevano i nostri antenati. La mancanza di incisione normativa è oramai un problema sotto gli occhi delle istituzioni, le quali, tuttavia, stanno persistendo nell'adottare soluzioni di mezzo.

Ciò comporta, tra le altre cose, un'allocazione di responsabilità in capo ai soggetti privati i quali, chiamati a rispondere in qualità di intermediari delle loro decisioni come, ad esempio, l'utilizzo di strumenti di sorveglianza come il riconoscimento facciale, devono, tuttavia, autolimitarsi alla luce dei principi generali dell'ordinamento. Un aspetto che viene a rilievo se si osservano le dichiarazioni di taluni colossi digitali di cui si parlerà in seguito. Molte responsabilità che hanno come contraltare la mancanza di una regola positivamente individuata dal legislatore, intensificando, d'altro canto, la necessità di intervenire caso per caso da parte dei giudici. In questa confusione di ruoli, si sta ridisegnando in maniera sostanziale la piramide dei poteri, andando a tracciare nuovi confini tra pubblico e privato[41].

Come lamenta anche lo European Data Protection Board[42] sollevando la problematica nell'ambito dei difficili rapporti a seguito del naufragio del Privacy Shield, manca una visione condivisa sui temi legati alle nuove forme di sorveglianza, tra cui il riconoscimento facciale, salvo sparute posizioni, come, ad esempio, quella assunta recentemente dal Parlamento Europeo nell'ambito della vendita e dell'esportazione di tecnologie votate alla sorveglianza informatica[43]. Le fragilità[44], tuttavia, sono evidenti già ad una prima lettura: sebbene sia un passaggio importante con riferimento alla commercializzazione di suddetti mezzi al di fuori del Mercato Unico, nulla si dice circa le limitazioni che, invece, dovrebbero essere intraprese anche all'interno della grande famiglia europea, ove non sempre troviamo comportamenti rispettosi dei valori comunitari[45].

---

[40] Espressione fortemente evocativa dell'atteggiamento assunto dalla Corte europea che alloca sugli attori privati una grande responsabilità comportando una nuova definizione dei rapporti di potere. Questi si muovono sempre di più da una posizione verticale ad una, invece, orizzontale coinvolgendo, per l'appunto, in maniera importante gli intermediari privati, i quali non avrebbero per loro natura un siffatto ruolo, e cedendo, altresì, il controllo non solo sui dati personali degli individui (i quali dal canto loro fanno sempre più fatica ad avere contezza del flusso di informazioni che condividono), ma anche potere regolatorio, mancando le istituzioni statali di un'effettiva e calzante influenza decisionale. Si veda, dunque, O. Pollicino, *Diabolical Persistence*, in *Verfassungsblog*, 25 luglio 2020.

[41] Come nota F. Pasquale in *The Black Box Society*, Harvard, 2015, «*they were private companies, but they controlled vital resources and enjoyed a power similar to that of a public authority*».

[42] Si veda sul punto Comitato Europeo per la Protezione dei Dati, 31a Sessione Plenaria, *Creazione di una task force su TikTok, risposta ai Deputati al Parlamento europeo sull'utilizzo di Clearview AI da parte delle autorità incaricate della protezione della legge,* 10 giugno 2020.

[43] Quest'ultimo, che andrebbe ad ampliare il già adottato Accordo Wassenaar relativo alla commercializzazione di armi tradizionali, ha lo scopo di bloccare la vendita di sistemi di sorveglianza a paesi di stampo autoritario, configurandosi il rischio di un uso distorto dei menzionati strumenti, come chiarito dalla Conferenza Stampa rilasciata: *Dual Use Goods: Parliament and EU Ministers Agree on New EU Export Rules. News: European Parliament,* 9 novembre 2020.

[44] Si veda B. Calderini, *Sorveglianza, Europa sotto accusa,* cit.

[45] Si veda, ad esempio, le crisi che avvengono in molti paesi dell'est Europa, quali, ad esempio, Polonia ed Ungheria, ove i rispettivi Governi si sono schierati in numerose occasioni con atteggiamenti lesivi dei diritti fondamentali e della partecipazione democratica, come evidenziato da L. Misculin, in *Perché l'UE non espelle Ungheria e Polonia?*, *Il Post,* 17 novembre 2020.

In linea con la criticità appena puntualizzata, un altro elemento che ribadisce la scarsa effettività dell'accordo è rappresentato dal fatto che la sua attuazione è rimandata esclusivamente all'iniziativa dei governi: posizione che non viene in soccorso di una necessaria protezione dei diritti in gioco, andando ancor di più a frammentare l'area di intervento.

A sostegno della opacità e delle problematiche appena esaminate occorre menzionare la recente pubblicazione da parte del Consiglio d'Europa ove si richiede un *ban* di alcune applicazioni del riconoscimento facciale: *«for the sole purpose of determining a person's skin colour, religious or other belief, sex, racial or ethnic origin, age, health or social status to be prohibited»*[46]. Tuttavia, il nodo centrale della problematica sono sempre gli stessi due elementi che abbiamo già potuto osservare. In primo luogo, il documento in esame è uno strumento che si propone di dare dignità agli individui guidando i governi e i privati[47], ma non imponendo agli stessi alcunché. Inoltre, non è salutare distinguere tra usi buoni ed usi cattivi di riconoscimento facciale finché le discriminazioni puntualizzate esistono. Un punto di criticità importante, inoltre, delle linee guida è che consentono l'uso di questa tecnologia solo in *uncontrolled environments*, come centri commerciali, e per *law-enforcement purposes*. Sebbene si puntualizzi che l'utilizzo debba essere sottoposto ad un controllo di necessità e proporzionalità, non è ben chiaro quale sia lo standard a cui fare riferimento e quale possa essere la necessità di svolgere una sorveglianza in luoghi quali, ad esempio, centri commerciali, tramite riconoscimento facciale. Concludendo sul punto, sebbene queste linee guida abbiano dei pregi come mettere in evidenza i rischi sottesi all'utilizzo di una tale tecnologia ed affermare in modo chiaro che il consenso[48] non può rappresentare la base legale per il trattamento tanto se effettuato da una pubblica autorità quanto da un'entità privata, d'altro canto mostrano tutte le fragilità che abbiamo evidenziato: sostanziale opacità, confini labili tra pubblico e privato, rischi sostanziali per le libertà fondamentali degli individui.

Avendo, dunque, puntualizzato le problematiche a livello normativo, ed avendo tratteggiato il quadro di non trasparenza nel quale ci troviamo, urge muovere le fila del discorso andando ad evidenziare quali sono i diritti che risultano essere maggiormente minacciati da un utilizzo pressoché illimitato del riconoscimento facciale.

3. I diritti fondamentali minacciati dal riconoscimento facciale

Petkova definisce la privacy il «primo emendamento europeo»[49] rievocando la massima attenzione dedicata dal legislatore comunitario alla protezione di questo capillare

[46] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, Convention 108: Guidelines on facial recognition, 28 gennaio 2021.

[47] Sul punto, i paragrafi 1.2.2 e 1.2.3 delle Linee Guida intitolati, *«use of facial recognition technologies in the public sector»* e *«use of facial recognition technologies in the private sector»*.

[48] Il riferimento è, in particolare al punto 3.1 della I parte, *«public authorities»*.

[49] V. B. Petkova, *Privacy as Europe's First Amendment*, in *European Law Journal*, 25(2), 2019, 140 ss.

diritto in quella che da una parte della letteratura è stata definita «società della sorveglianza»[50]. La privacy è il primo dei diritti che viene messo in pericolo dall'impiego di tecnologie quali il FRT: avendo perso, come si è detto, i tratti di «un diritto ad essere lasciati soli»[51], essa si estrinseca in una *summa*[52] di diritti esercitabili nel mondo digitale, ricomprendendo tanto il rispetto per la vita privata, quanto la protezione dei dati personali[53]. Entrambe le connotazioni hanno un obiettivo comune, quali il rispetto della persona da intrusioni nella sua sfera privata, della dignità umana, del principio di autodeterminazione: sostanziali prerequisiti che riecheggiano in molti altri diritti esercitabili online, quale, ad esempio, la libertà di espressione.

Quali proporzionalità, adeguatezza, minimizzazione del dato e trasparenza, criteri cardine del trattamento previsti dalla normativa europea sulla protezione dei dati, possono essere assicurate con l'installazione di impianti di riconoscimento facciale? Tale fenomeno induce a comportamenti in linea con il c.d. *chilling effect*[54]: una modificazione delle abitudini individuali per evitare di sottostare all'occhio indiscreto di una telecamera, pur di tutelare la nostra riservatezza. Spesso i detrattori dell'epoca digitale affermano che, se desiderosi di privacy, si possono sempre cancellare i profili social: posizione che, tuttavia, sembra non prendere in considerazione la centralità di queste piattaforme nelle nostre vite. Pur non condividendo questa impostazione, potremmo esercitare il nostro diritto all'oblio e (tentare di) scomparire online. Che fare, però, con i nostri volti? Non possiamo di certo disinstallarli così facilmente come una qualsiasi *app* sullo *smartphone*. Ed ecco che quel *chilling effect* di cui si diceva diviene un fenomeno quanto mai centrale nella nostra Democrazia, in quanto gli individui potrebbero aver paura di partecipare a cortei o proteste, ed esercitare quella sacrosanta libertà di espressione che è la pietra miliare su cui si erge l'intero paradigma partecipativo della nostra società. L'unico modo per esercitarla è favorire l'anonimato, ma se il volto diviene il primo target, con quali mezzi proteggiamo non solo la nostra privacy, ma anche, ed essenzialmente, le libertà di espressione, di pensiero, di scelta, di associazione, di assemblea?

Come ha puntualizzato il Segretario Generale del Consiglio d'Europa alla pubblicazione delle Linee Guida menzionate[55], il riconoscimento facciale può rappresentare un modo per rendere determinate azioni della nostra vita quotidiana più semplici. Tuttavia, dà anche il potere di monitorare e controllare tali aspetti senza che gli individui ne

---

[50] Sul punto, *ex multis*, S. Rodotà, *La società della sorveglianza, in Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Roma-Bari, 2004.

[51] S. D. Warren - L. Brandeis, *The Right to Privacy*, cit.

[52] Tale interpretazione è suggerita da R. Panetta, in *Privacy it's not dead. It's hiring!*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, 2019.

[53] Autorevole lettura interpretativa fornita dalla Corte di giustizia dell'Unione europea nei casi C-92/09 e C-93/09, *Volker und Markus Schecke and Eifert GbR and Hartmut Eifert* (2010), § 71.

[54] Nel gergo legale di common law significa la refrattarietà ad esercitare un proprio diritto per paura di ripercussioni: un fenomeno amplificato dagli algoritmi, come spiegato da M. Büchi in *Chilling Effects of Profiling Activities: Mapping the Issues,* in *Computer Law & Security Review*, 36, 2020.

[55] *Infra,* nota 46.

siano a conoscenza o vi abbiano acconsentito[56]. Ed è proprio sul piano del consenso che si è soffermato il CoE: un aspetto problematico che era già venuto in risalto in un caso deciso lo scorso anno dal Tribunale Amministrativo di Marsiglia[57]. L'Ufficio Scolastico delle Provincie di Marsiglia e Nizza aveva firmato alla fine del 2018 una partnership con Cisco International Limited per consentire l'installazione in una scuola superiore di telecamere che effettuavano riconoscimento facciale sugli studenti[58]. A seguito del ricorso presentato dall'associazione dei genitori, il Tribunale è stato chiamato a pronunciarsi e sono emersi due aspetti. Anzitutto, la violazione del GDPR da parte dell'ufficio scolastico tramite l'installazione di dispositivi FRT, in quanto lesivi dell'art. 9[59] del Regolamento: gli studenti, difatti, non potevano in alcun modo fornire un libero consenso al trattamento dei loro dati biometrici trattandosi di una decisione dell'autorità scolastica che si trova in una posizione di potere nei loro confronti. In secondo luogo, in mancanza tra l'altro di necessità e proporzionalità, un tale sistema di sorveglianza rappresenterebbe un'adesione di tipo *opt-out*, senza possibilità di negare il proprio consenso in quanto, nel caso in cui non volesse essere sottoposto ad un siffatto trattamento, lo studente non potrebbe correttamente accedere all'edificio scolastico, patendo un detrimento ad uno dei diritti fondamentali dei fanciulli: quello all'istruzione[60].

È, dunque, chiaro che non si può accettare lo stabilirsi di un sistema che impone la scelta tra istruzione, espressione, associazione – tutti quei diritti cardine di una qualsiasi società democratica – e tecnologia a causa della sorveglianza di cui talvolta quest'ultima si macchia. L'obiettivo, ci si augura, non utopico dovrebbe essere una corretta commistione di questi elementi che sia scevra di invasività e opacità. L'aspetto allarmante che emerge con riferimento al riconoscimento facciale, e che, nonostante tutto, non ne blocca la commercializzazione, è relativo al fatto incontrovertibile che la stessa produce numerosi *bias*[61], errori, nel riconoscere efficacemente alcuni volti: in particolare,

---

[56] *«At its best, facial recognition can be convenient, helping us to navigate obstacles in our everyday lives. At its worst, it threatens our essential human rights, including privacy, equal treatment and non-discrimination, empowering state authorities and others to monitor and control important aspects of our lives – often without our knowledge or consent»,* M. Pejčinović Burić in *Facial Recognition: Strict Regulation Is Needed to Prevent Human Rights Violations*, CoE, 28 gennaio 2021.

[57] Trib. Adm. de Marseille, n. 1901249, 3 febbraio 2020.

[58] Si trattava di un progetto sperimentale che avrebbero dovuto passare il vaglio del CNIL, garante per la privacy francese. L'autorità, tuttavia, diede parere negativo dichiarando l'installazione di dispositivi di riconoscimento facciale illegali, come si legge in L. Kayali in *French privacy watchdog says facial recognition trial in high schools is illegal,* in *politico.com*, 29 ottobre 2019.

[59] L'art. 9, regolamento (UE) 2016/679 si riferisce al "trattamento di categorie particolari di dati personali", cui rientrano anche i dati biometrici ricadendo perfettamente nell'inquadramento effettuato dal par. 1. Inoltre, l'iniziativa dell'Ufficio Scolastico non ricade in alcun modo nelle categorie delle eccezioni enucleate, invece, al par. 2.

[60] Si veda artt. 28 e 29 della Convenzione internazionale sui diritti dell'infanzia e dell'adolescenza (1989).

[61] I *bias* sono errori cognitivi che l'intelligenza artificiale commette riproducendo sostanzialmente gli stessi deficit che la mente umana compie. Tuttavia, la macchina compie suddetti errori, in particolare, sulla base degli esempi che sono stati ad essa forniti. Sebbene Turing sottolineasse che "dobbiamo accettare che le macchine commettono errori", non possiamo affermare questa frase in un'epoca in cui i processi decisionali divengono sempre più automatizzati, in quanto un errore significa esporre una o più categorie discriminate dalla macchina e, dunque, sottoposte ad una grave lesione dei diritti fondamentali. Per un approfondimento dei concetti ivi richiamati, si veda A. Turing, *Intelligenza meccanica,* Torino, 1994;

quelli pertinenti a donne e persone di colore. Un recentissimo caso di arresto nei confronti di un uomo afroamericano in New Jersey dimostra quanto appena affermato: questi è stato vittima di un errore causato dall'impiego da parte della polizia dell'app di riconoscimento facciale Clearview, come riportato dal New York Times[62]. Medesimo problema identificativo mostrato da Rekognition, il sistema di FRT sviluppato da Amazon[63], che, in una sua fase di sperimentazione su alcuni membri del Congresso Americano, ha erroneamente identificato 28 di essi, ancora una volta afroamericani, ricollegandoli ad alcune foto segnaletiche presenti nel database. Uno spiacevole episodio che testimonia la fallacità di questa tecnologia, in un periodo storico fortemente scosso dalle violenze commesse, tra gli altri, ai danni di George Floyd nell'estate del 2020: la punta dell'iceberg che è stata colta da varie organizzazioni internazionali, quali Amnesty International[64], per sottolineare una volta per tutte i rischi connessi con tale sistema di sorveglianza qualora venisse massivamente applicato.

Dati gli errori e le problematiche relative ai menzionati diritto alla privacy, al principio di non discriminazione e alla libertà di espressione, IBM[65] ha deciso, seguita poi da altre[66], di sospendere la commercializzazione del proprio sistema di FRT. Ed ecco, dunque, in tutta evidenza il paradosso di cui si diceva, provocato dal vuoto non colmato dall'indecisione legislativa: mentre gli Stati stanno discutendo attorno a poche ed inefficaci misure, le maggiori *corporation* globali si trovano a dover prendere delle decisioni, auto-limitandosi. Sono loro che, assumendo un ruolo quasi-pubblicistico all'interno della dinamica regolatrice, stanno attivamente favorendo il processo di «privatizzazione dei diritti fondamentali»[67] assicurando quello che dovrebbe essere, viceversa, il primario ruolo dello Stato: la salvaguardia dei diritti fondamentali. Un fenomeno che può essere osservato sotto molti punti di vista, ma che si presta efficacemente anche in tema di riconoscimento facciale, in quanto, come abbiamo potuto vedere, il potere pubblicistico sta mancando di una chiara visione garantista tanto delle nostre libertà quanto del futuro, non solo digitale, dell'umanità tutta.

J. Robinson et al., *Face Recognition: Too Bias, or Not Too Bias?,* in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops,* 2020.

62 *Flawed Facial Recognition Leads to Arrest and Jail for New Jersey Man,* in *The New York Times*, 6 gennaio 2021.

63 Si veda sul punto M. DeGeurin, *Amazon's Facial-Recognition Software Mistakes 28 Congressmen for Criminals*, in *Intelligencer*, 27 luglio 2018.

64 V. *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance*, 11 giugno 2020.

65 Circa la protesta di IBM, si veda *IBM Quits Facial-Recognition Market over Police Racial-Profiling Concerns,* in *The Guardian*, 9 giugno 2020; *IBM's facial recognition protest, explained*, in *Vox,* 10 giugno 2020.

66 IBM ha sollevato un'onda di opposizione all'uso di tale tecnologia, cui si sono unite molte delle maggiori compagnie digitali, quali, ad esempio, Amazon e Microsoft, come spiega T. Simonite, *Amazon Joins Microsoft's Call for Rules on Facial Recognition*, in *Wired*, 2 luglio 2019.

67 Tale concetto è suggerito da M. Bassini in *Fundamental Rights and Private Enforcement in the Digital Age* in *European Law Journal,* 25(2), 182 ss., ove l'A. sottolinea il ruolo preponderante dei *private actors* nell'assicurare la tutela dei diritti fondamentali, venendo sempre più esposti ad una posizione di necessari intermediari.

4. Conclusioni

Non pubblicare più *selfie,* o cancellare account e farsi risucchiare dal vortice del *social dilemma*[68]*,* non sembra essere una soluzione prospettabile. Negare il valore della tecnologia sarebbe un atteggiamento luddista che porterebbe a ben poco sotto il profilo economico, sociale e, persino, giuridico. Tuttavia, i dati ci stanno insegnando una preziosa lezione: ogni passaggio online lascia una profonda traccia. I nostri *like*, le nostre interazioni, pensieri, gusti, corpi: tutto può essere sottoposto al processo di raccolta, analisi e conservazione di immensi database.

Le nuove forme di sorveglianza appena descritte sono sempre più precise e intrusive, favorendo una nuova allocazione della conoscenza nelle mani di coloro che possono efficacemente controllare, raccogliere e ricavare informazioni da suddetti dati. Non vale più il sillogismo per cui «se è gratis tu sei il prodotto», come sottolinea Zuboff[69]. Noi, in questo meccanismo, non siamo il prodotto, bensì l'oggetto di questo scrutinare senza fine, partecipi e protagonisti di un'euforia digitalizzante che sta sconvolgendo i meccanismi della nostra società, a partire da un sostanziale sbilanciamento dei rapporti tra pubblico e privato, che stanno minando l'esercizio del potere degli uni, a scapito di una preponderanza degli altri.

In conclusione, occorre domandarsi, fino a che punto si possono lanciare sul mercato nuovi *devices* senza effettuare una riflessione relativa ai rischi? Dove finisce la datacrazia o governance del dato ed inizia la tirannia di questo? La riallocazione del potere e della conoscenza gli ha affidato un compito sempre più preponderante, investendolo non solo del ruolo di oracolo[70] della politica, della socialità, dell'economia, ma anche del diritto, assorgendolo ad intermediario tra Stato e cittadino, tra pubblico e privato. Come suggerisce il filosofo Giorello[71] è urgente la ridefinizione di sistemi di governo e forme legislative che non siano incastonate in posizioni pietrificate dal passato ma che si dimostrino, piuttosto, robuste e adattabili alle scoperte scientifiche e tecnologiche del nostro tempo.

[68] Titolo dell'omonimo e discusso documentario diretto da Orlowski e distribuito da Netflix.

[69] S. Zuboff, *The Age of Surveillance Capitalism,* cit.

[70] Il riferimento è ad A. Vespignani - R. Rijtano, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo,* Milano, 2019.

[71] G. Giorello, *Di nessuna chiesa: La libertà del laico,* Milano, 2020.