2024 NUMERO 67

Coscienza e Libertà

SEMESTRALE DI LIBERTÀ RELIGIOSA, LAICITÀ, DIRITTI DAL 1978

S. Amato

Religione e sicurezza integrata

ISSN 0394-2732

D. Romano - M. Ventura - G. Fattori - D. Curtotti - P. Annicchino - V. Ricciuto - T.F. Giupponi
E. Gianfrancesco - G. Tropea - A. Vedaschi - I. Ruggiu - A. Pin - G. Corso - N. Marchei - F. Alicino
D. Milani - A. Casiere - I.A. Caggiano - P.B. Helzel - S. Amato - A. Benzo - S. Baldassarre

Libertà religiosa e *privacy* informazionale*

Salvatore Amato

Professore Ordinario di Filosofia del diritto, Dipartimento di Giurisprudenza, Università di Catania

ABSTRACT

Gli effetti cumulativi e rafforzativi delle tecnologie di IA potrebbero rendere la nostra esistenza integralmente trasparente. Questo rapido mutamento della nostra società può essere sintetizzato da due aggettivi: incommensurabile e opaco. L'incommensurabilità non è solo quantitativa, per l'enormità dei dati e per le straordinarie capacità di calcolo, ma anche qualitativa per i meccanismi con cui si autoproduce e autoprogramma. Per la prima volta nella nostra storia abbiamo macchine (e avremo sempre più macchine) *human out of the loop* che dialogano autonomamente tra di loro e sviluppano autonomamente i propri percorsi di apprendimento. L'incommensurabilità e l'opacità sono difficilmente compatibili con l'esperienza giuridica e con quella morale. Non si può regolare quello che non si può delimitare e non si può valutare quello che non si conosce. Le recenti linee guida dell'IBM sull'Intelligenza artificiale si fondano su un'affermazione netta: *Imperceptible AI is not ethical AI*. In questo contesto la *privacy* rischia di diventare un'illusione magica, una fata Morgana, con pericolose ripercussioni sulla libertà di coscienza religiosa.

1. L'opacità degli algoritmi

Già alla fine degli anni '60 del secolo scorso Reyner Banham, noto per le ardite tesi sul rinnovamento dell'architettura esposte in *Theory and Design in*

* Elaborato nell'ambito delle ricerche del progetto PRA-HE 2021 "Re.co.se - Religion and Comprehensive Security" finanziato dall'Università degli Studi di Foggia (bando PRA_HE 2021 UNIFG finanziato dall'Unione europea mediante il programma Next Generation EU e dal programma MUR-Fondo Promozione e Sviluppo-DM 737 del 2021).

the First Machine Age, aveva provato ad anticipare il futuro, chiudendosi con la sua famiglia dentro una bolla trasparente circondato da tutti gli strumenti di telecomunicazione disponibili in quel periodo. Il messaggio era abbastanza evidente: muri e porte sono solo un'illusione perché (e ora ce ne rendiamo sempre più conto) nell'era delle macchine ogni pretesa di isolamento è divenuta impossibile. Non ha senso progettare le case come se fossero un mondo chiuso in se stesso e tendenzialmente impenetrabile. Saranno, piuttosto, un centro privilegiato di raccolta e diffusione delle informazioni su chi è presente, sulle attività che svolge, sulle sue interazioni, sui suoi gusti.

Sono passati 60 anni e la provocazione di Banham trova, ormai, integrale attuazione negli sviluppi tecnologici di case sempre più *smart* dove sono intelligenti i muri, i frigoriferi, la cucina, i cestini assieme agli orologi, ai vestiti, ai sensori e ai biosensori. Intelligenza, per questi dispositivi, significa essere idonei a captare, memorizzare, classificare, utilizzare ogni traccia della nostra esistenza. Ci stiamo rannicchiando dentro una bolla virtuale perché vogliamo/dobbiamo essere sempre visibili, per essere protetti ed assistiti da quella rete comunicativa che va oltre le mura, oltre la nostra stessa volontà, per fondersi con la nuova dimensione, reale per quanto immateriale, del *cloud*, dei *big data*, dell'infosfera.

Non sono solo le cose che ci circondano a immergerci in questo flusso comunicativo, ma anche l'impiego sistematico di *smartphone*, *ipad*, computer. La pressione dei *social network* spinge ciascuno a divenire creatore/fruitore di contenuti. Attraverso *post*, *blog*, *tweet*, *mail*, *like*, *screenshot* siamo sempre disponibili a rendere conto di noi stessi, a proiettare *on line* i momenti salienti della nostra vita.

Secondo le previsioni nel 2025 si dovrebbero produrre intorno ai mille triliardi di byte, ma non sapremmo cosa farcene di tutto questo continuo e in contino aumento *digital data stream* se non avessimo supercomputer la cui capacità di elaborazione non è neppure immaginabile da una mente umana: 200 milioni di miliardi di calcoli al secondo; quanto potrebbero fare tutte le persone sulla terra se eseguissero un calcolo ogni istante di ogni giorno per 305 giorni. Calcolare non significa soltanto accumulare dati, ma presuppone la selezione, la memorizzazione, la classificazione, l'utilizzazione. All'acquisizione grezza e non strutturata dei singoli elementi si aggiungono, quindi, i metadati (dati sui dati) che ridefiniscono le informazioni (*machine readable*) in base ai contesti in

cui sono formate, ai contenuti che veicolano o agli scopi per cui sono acquisite. I dati *storici* assunti dalla vita reale producono i dati *sintetici* costitutivi della realtà virtuale. Gli uni e gli altri alimentano quel mondo dell'infosfera, della *digital society*, che ha le sue regole (gli algoritmi), le sue connessioni (il *cloud*), la sua incommensurabilità (i *Big data*) e i suoi effetti (l'internet delle cose).

È una tecnologia basata ormai prevalentemente su algoritmi di apprendimento automatico, strutturati sul modello di reti di neuroni artificiali, che riescono a trattare le correlazioni statistiche in dimensioni e per funzioni finora impensabili. I *learner*, gli algoritmi di addestramento e insieme i nuclei di apprendimento di questi sistemi informatici, "capiscono" dagli stessi dati ciò che devono fare attraverso l'architettura di svariati "trasformatori generativi pre-addestrati" che sono in grado, con un programma di apprendimento lungo poche centinaia di righe, di generare automaticamente milioni di stringhe di codice. Il rapporto tra dati e metadati diventa, così, sempre più labile perché la loro fusione determina sviluppi ed esiti che non sono prevedibili neppure dagli stessi programmatori *(black box effect*).

Ci possiamo affidare a un'entità che ci sfugge? È il problema che affronta la proposta, ancora in via di definizione, di regolamentazione europea dell'intelligenza artificiale. L'art. 14 pone il principio dell'*Human oversight* per cui, al momento della raccolta dei dati (*designed and developed*), i codici di funzionamento dovrebbero vincolare l'intelligenza artificiale a specifici parametri di azione, a definiti funzioni e obiettivi, a un rigido rapporto tra *input* e *output* attraverso "schemi esecutivi", accessibili e trasparenti, che indichino i singoli passaggi, le loro connessioni e gli esiti. Tuttavia questo modello *white box* che produce algoritmi deterministici copre solo una parte, per quanto rilevante, dei processi digitali. Sempre più spesso la tecnologia di apprendimento automatico non è in grado di spiegare come e perché un dato diviene metadato, come e perché i metadati filtrano i dati, segnando il passaggio dalla "realtà aumentata" alla "realtà virtuale". Non siamo neppure in grado di capire quando gli algoritmi deterministici di un *white box model* mutino negli algoritmi stocastici di un *black box model*.

Uno dei casi più sconcertanti è stato il famoso "colpo 37" con cui il computer *AlphaGo* ha sconfitto il campione del mondo, Lee Sedol, in una partita di *Go*: il gioco più difficile per la sua complessità da inserire in un sistema informa-

tico. Una mossa apparentemente sbagliata, anzi assurda per tutti gli esperti, eppure decisiva per la vittoria fino ad apparire «il primo barlume di una vera intelligenza artificiale»[1]. Come può un algoritmo, scritto da esseri umani, fare quello che gli esseri umano non sono in grado concepire?

La *Big Data Revolution* si fonda su un continuo accrescimento incrementale: se aumentano i processori, si moltiplicano le connessioni; se si moltiplicano le connessioni, diventano più numerose e complesse le interazione; se diventano più numerose e complesse le interazione, cresce la quantità delle informazioni assimilate e gestite; se cresce la quantità delle informazioni assimilate e gestite, sono milioni, e forse addirittura miliardi, i parametri non previsti e non identificabili dai programmatori. Tutto questo determina una sempre più estesa capacità di autoapprendimento e quindi di registrazione e rielaborazione dei più minuti risvolti dell'esistenza umana (datificazione).

L'internet delle cose, quella infrastruttura globale che consente un'interazione continua tra gli esseri umani e gli oggetti (*it from bit*), tende a trasformarsi *nell'internet di tutte le cose*, che si affida incondizionatamente alla onnipotenza e all'onnivalenza dei "learner". Emerge una sorta di nuova religione, il "datismo"[2], che fonda una nuova forma di potere, la datacrazia. Il datismo è una religione i cui sacerdoti sono le *Big Six* o GAFAIM (Google, Apple, Facebook, Amazon, IBM, Microsoft), soggetti privati più potenti dei singoli Stati, se non della comunità internazionale nel suo complesso. La datacrazia è una forma di potere costruita sulla «governamentalità algoritmica»[3] che consente attraverso i dati di controllare e condizionare tendenzialmente qualsiasi aspetto della società, riducendo gli esseri umani a un insieme di tracce digitali da acquisire, selezionare e sfruttare.

[1] B. Labatut, nell'opera di finzione "basata sulla realtà" in cui narra questa vicenda, osserva che «era diversa da qualunque altra cosa un computer avesse mai fatto prima. Ed era anche diversa da qualunque cosa un essere umano avesse mai preso in considerazione. Era qualcosa di nuovo, una totale rottura con la tradizione, una deviazione radicale da migliaia di anni di esperienza accumulata», B. Labatut, *Maniac*, Adelphi, Milano, 2023, p. 314.

[2] Y.N. Harari, *Homo Deus. Breve storia del futuro*, Giunti-Bompiani, Firenze-Milano, 2017, p. 535.

[3] M. Benasayag, *La tirannia dell'algoritmo. Conversazione con Régis Meyran*, Vita e pensiero, Milano, 2020, cap. III.

2. *I from bit*

Ci troviamo, quindi, di fronte a un meccanismo estremamente efficace di cui possiamo sintetizzare gli sviluppi attraverso due aggettivi: incommensurabile e opaco. Incommensurabile proprio perché opaco e opaco proprio perché incommensurabile. L'incommensurabilità, infatti, non è solo quantitativa, per l'enormità dei dati e per le straordinarie capacità di calcolo, ma anche qualitativa per i meccanismi con cui si autoproduce e autoprogramma. Per la prima volta nella nostra storia abbiamo macchine (e avremo sempre più macchine) "human out of the loop" che dialogano autonomamente tra di loro e sviluppano autonomamente i propri percorsi di apprendimento.

L'incommensurabilità e l'opacità sono difficilmente compatibili con l'esperienza giuridica e con quella morale. Non si può regolare quello che non si può delimitare e non si può valutare quello che non si conosce. Ne prendono atto le recenti linee guida dell'IBM sull'Intelligenza artificiale che si fondano su un'affermazione netta: «Imperceptible AI is not ethical AI»[4]. È difficile non esserne consapevoli, ma non conosciamo il rimedio. Ci troviamo di fronte a un limite tecnico, intrinseco allo sviluppo scientifico. Gli straordinari successi dell'intelligenza artificiale in tutti i campi dell'esperienza umana si devono proprio alla capacità dei "trasformatori generativi pre-addestrati" di andare oltre i limiti della logica umana, spingendo verso una *General Purpose AI* (GPAI) con programmi flessibili che sviluppano applicazioni non solo diverse da quelle per cui erano state inizialmente progettate, ma spesso neppure ipotizzabili.

È proprio il modello "black box" che ha consentito, ad esempio, ai sistemi GPT di superare le barriere linguistiche, elaborando traduzioni sempre più efficaci, oppure ad AlphaFold2, l'applicazione di DeepMind, di individuare uno schema per la comprensione (fino a quel momento impossibile) del ripiegamento delle proteine. L'elemento cruciale è che non siamo (ancora?) in grado di aprire la "scatola nera" che abbiamo creato e di cui ci avvaliamo sistematicamente. Dobbiamo limitarci a prendere atto del fatto che gli attuali limiti tecnologici rendono irrealistico aspettarsi che i sistemi di supporto decisionale

[4] www.ibm.com/design/ai/ethics/explainability/#:~:text=Explainability%20is%20key%20for%20users%20interacting%20with%20AI,seamless%20experience.%20Imperceptible%20AI%20is%20not%20ethical%20AI

di apprendimento automatico siano in grado di generare, in tutte le circostanze, spiegazioni complete per le previsioni che fanno o per i risultati che ottengono[5].

L'intelligenza artificiale sta quindi, in quanto tale e in quanto sistematica produttrice di opacità, incidendo su tanti aspetti dell'esperienza giuridica: dai profili della responsabilità per danni alle negoziazioni algoritmiche ad alta frequenza, dai nuovi aspetti del rapporto di lavoro ai *robot-board*, dalla proprietà intellettuale all'eredità digitale, fino all'impiego degli algoritmi predittivi per vari aspetti della valutazione delle persone, compresa la pericolosità sociale.

Stiamo assistendo a un progressivo logoramento dei tradizionali orizzonti istituzionali. Fino a che punto potremo continuare ad andare avanti con questa difficile opera di adattamento? Mi pare estremamente significativo che nel 2019 la International Commercial Court di Singapore non abbia escluso che alcuni elementi basilari della teoria del contratto vadano ripensati: «turning to knowledge of the mistake, the law in relation to the way in which ascertainment of knowledge in cases where computers have replaced human actions is to be determined will, no doubt, develop as legal disputes arise as a result of such actions. This will particularly be the case where the computer in question is creating artificial intelligence and could therefore be said to have a mind of its own»[6].

L'impossibilità di mantenere gli attuali modelli giuridici è particolarmente evidente con la *privacy*[7]. L'Alto Commissario ONU per i Diritti Umani lo ha sottolineato nel Rapporto del 13.09.2021, su *Il diritto alla privacy nell'era digitale*[8]. Fra le varie considerazioni ha rimarcato con forza che l'opacità rende difficile valutare in modo significativo gli effetti dei sistemi di intelligenza artificiale sulla tutela dei diritti fondamentali e in particolare su quel nucleo essenziale di rispetto della riservatezza che dovrebbe costituire la base intangibile dell'integrità personale.

Se i margini di opacità non sono eliminabili e neppure prevedibili, è im-

[5] Non siamo ancora in grado di aprire la scatola nera: A. Adadi, M. Berrada, *Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)*, in *IEEE Access*, 2018-6.

[6] www.sicc.gov.sg/docs/default-source/modules-document/judgments/b2c2-ltd-v-quoine-pte-ltd pdf § 206.

[7] A. M. Froomkin, *The Death of Privacy?*, in "Stanford Law Review" 52/2000, p. 1461 ss.

[8] www.ai4business.it/intelligenza-artificiale/ai-e-diritti-umani-le raccomandazioni-dellalto-commissario-dellonu/

possibile individuare in che termini e fino a che punto significhi ancora qualcosa quel diritto a "let to be alone" che ha caratterizzato tutto il secolo scorso, erigendo una barriera intangibile per le immagini, i sentimenti, le opinioni, per tutto quello che è mio e deve restare solo mio perché costituisce una parte essenziale e indisponibile dell'identità. La *privacy* doveva proteggere la "casa" dagli sguardi e dagli ascolti indiscreti; il corpo dalle invasioni delle terapie e delle indagini cliniche; il *self* dalle discriminazioni per le scelte di vita.

Ora la casa è il punto di partenza del flusso di informazioni alimentato dall'*internet of things*, mentre il corpo è sempre più spesso la *password* per accedere a prestazioni e servizi. La casa e il corpo sono il tramite del passaggio dall'*it from bit*, dalla connessione uomo-macchina, all'*I from bit*, all'assimilazione dell'uomo alla macchina. Un elemento fondamentale di questo passaggio sono i processi di identificazione biometrica che consentono la rilevazione digitale di specifiche caratteristiche fisiche, fisiologiche o comportamentali come la voce, il volto, la topografia e geometria della mano, le vene della mano e del polso, i solchi delle nocche, l'iride, la retina, le emissioni otoacustiche, il microbioma: insomma, qualsiasi parte del corpo sia rilevabile da un sensore con i caratteri dell'universalità, della permanenza e dell'unicità. Attraverso la biometria, esisto solo se sono classificato e omologato dentro l'imperscrutabile mondo dell'infosfera. Imperscrutabile per me, che ignoro chi e perché mi classifica in un certo modo, ma non per il sistema informatico in cui tutte le tracce della mia esistenza si collegano e ridefiniscono per essere, poi, sintetizzate in una stringa numerica. Il *self* è tale se è *quantified*, se è riconducibile all'insieme dei dati che lo riguardano. Se io sono i miei *bit*, l'identità personale evapora nell'identità digitale. Le *networked persons* escludono l'idea stessa di un *privus*, di qualcuno che pretenda di sottrarsi al flusso comunicativo.

Nei limiti in cui "*life is going digital*", nulla è "chiuso in sé", nulla è "privato": tutto diviene scomponibile, osservabile, manipolabile. Come ho già detto, gran parte di quello che vediamo, che facciamo, che scriviamo passa da un computer, è dentro la nostra casa, ma intanto è già fuori, è in rete. Gran parte di quello che siamo, dai componenti biochimici del nostro organismo al suono della nostra voce, può essere registrato e archiviato su un supporto informatico. Non c'è più nulla che sia "nostro" nel senso che inizia, finisce con noi e resta nel nostro controllo; come un qualsiasi oggetto queste svariate tracce della nostra esistenza

ci possono essere sottratte in ogni momento, quando non siamo noi stessi a cederle o a disinteressarci della loro sorte.

Anche se non ce ne interessiamo, i dispositivi che ci circondano restano sempre attivi. Il dataismo alimenta quel "capitalismo della sorveglianza"[9] per cui questi continui e minuti nostri *surplus* comportamentali, captati dai biosensori, decifrati dalla biometria ed eventualmente collegati ai processi di *affective computing*, vengono trasformati in prodotti predittivi in grado di ipotizzare cosa faremo, cosa vorremo oppure cosa dovremmo fare e volere. Si prevede per condizionare e si condiziona per prevedere, alimentando un nuovo mercato estremamente redditizio: il mercato dei comportamenti futuri.

Questo mercato è strettamente collegato alla datacrazia, perché rende possibili i primi passi di una polizia del pensiero. La biometria, infatti, si prolunga nella psicometria che, attraverso le tecnologie di *emotion Ai* o *affective computing*, pretende di decifrare e valutare i nostri sentimenti attraverso le inflessioni vocali e le espressioni del volto. Si stanno imponendo sistemi di *social scoring* in cui la profilazione attraverso queste tecniche di rilevazione biometrica consente di attribuire a ciascun cittadino un "punteggio sociale" che facilita o condiziona l'accesso ai servizi, al credito, al mondo del lavoro o allo stesso esercizio dei diritti fondamentali. Dobbiamo credere a Morozov? «Le aziende della Silicon Valley stanno piazzando un filo spinato invisibile intorno alle nostre vite»[10]? In Cina questo filo spinato non è poi tanto invisibile se nel 2018 il governo ha annunciato che avrebbe imposto il divieto di viaggiare in aereo ai cittadini che non avessero raggiunto un determinato "punteggio sociale".

Alcuni esempi. La Zhongheng Electric fornisce ai lavoratori che si alternano alla catena di montaggio un caschetto che al suo interno ha dei sensori *wireless* che monitorano in continuazione le onde cerebrali dei lavoratori e comunicano questi dati ai computer, che grazie all'intelligenza artificiale individuano picchi emotivi legati ad ansia, stanchezza, distrazione o rabbia. La Clearview AI, una startup che si occupa di riconoscimento facciale, afferma di possedere oltre tre miliardi di volti di persone, cioè un po' meno della metà dell'intera popolazione

[9] S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2019, § 1.3.

[10] E. Morozov, *Silicon Valley: i signori del silicio*, Codice ed., 2018, p. 56.

umana. Sari Real Time è un sistema, che consente il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza: attraverso una serie di telecamere installate in una determinata area geografica, è in grado di analizzare in tempo reale i volti dei soggetti ripresi, confrontandoli con una banca dati predefinita (denominata "watch-list")[11]. Questa società ha già stipulato contratti con la polizia di Detroit e di Miami, con lo Stato della Georgia e con altre 2.200 agenzie pubbliche negli Stati Uniti e con numerose imprese private in tutto il mondo.

Questi nuovi orizzonti del mercato ci fanno capire in che modo stiamo sommando al corpo *password*, che rivela le nostre azioni, il corpo *scanner*, che rivela le nostre emozioni. Le azioni non sono nostre nei limiti in cui sono registrabili. Le emozioni non sono nostre nei limiti in cui sono osservabili. Se la tecnologia cancella il "mio", come continuare a segnare i confini del "proprio" attraverso la *privacy*?

3. Un robot santo

La tecnologia impone la trasparenza[12], ma si nasconde dietro l'opacità. L'enorme quantità di tracce dell'esistenza che vengono profilate sfugge ad ogni possibilità di controllo individuale. Non sappiamo, chi controlla e perché; come profila e perché. Chi guarda e conserva non è un'entità unica e riconosciuta, come lo Stato, ma può essere una qualsiasi applicazione offerta da *App store*, che si avvale di qualsiasi informazione fornita da *Google* o immagine affidata a *Instagram* o pensiero espresso su *Facebook* o pulsazione rilevata da un *Apple Watch* o emozione captata da un algoritmo affettivo. Tracce di tracce su tracce in una costellazione indecifrabile di entità (in molti documenti si usa l'orribile espressione "terzisti") che gestiscono un pezzetto di noi per i fini più vari. Se consideriamo che tutto questo può sfuggire alla previsione degli stessi programmatori, ci rendiamo conto di quanto la *privacy* stia divenendo una sorta di fata Morgana di cui evochiamo il concetto, ma lo vediamo svanire non appena

[11] È opportuno tenere presente che gli attuali *software* sono in grado di riconoscere le facce non solo quando sono di fronte e isolate al centro di una foto, ma anche quando il soggetto è tra la folla.

[12] «Ecco la massima trasparenza. Vedere tutto. Sempre», D. Eggers, *Il cerchio*, Mondadori, Milano, 2014, p. 56.

cerchiamo di dargli un minimo di consistenza.

In apparenza potrebbe sembrare il contrario. È impossibile trovare una dichiarazione sull'Intelligenza artificiale che non faccia riferimento al problema della *privacy* e non invochi un "ecosistema di fiducia" o un "costituzionalismo digitale". Il Regolamento (UE) 2016/679 del Parlamento europeo (GDPR) offre un quadro estremamente articolato e, sotto molti punti vista innovativo, sulla protezione dei dati personali. Altrettanto rilievo assume la tutela della *privacy* nella proposta di Regolamento del Parlamento europeo sull'intelligenza artificiale con una tutela significativamente costruita attorno ai livelli di rischio per il rispetto dei diritti fondamentali.

Di riflesso si è imposto, anche per effetto dell'elaborazione giurisprudenziale, il concetto di *privacy* informazionale[13], che adombra l'esigenza di un *impact assessment* per tutti i rapporti tra la *privacy* e le nuove tecnologie dell'informazione e della comunicazione, determinando l'emergere di nuovi diritti e di ulteriori garanzie. Nuovi diritti come il diritto al controllo umano, il diritto di esplicabilità, il diritto di accesso, il diritto di disconnessione, il diritto all'oblio, il diritto all'eredità digitale. Nuove garanzie come la *differential privacy* per limitare l'acquisizione dei dati; la *privacy by design* per inglobarne la tutela nei progetti informatici; la *privacy* by *default* per definire precisi limiti operativi; la *privacy* neuronale per preservare almeno l'intimità dei nostri pensieri.

Proprio il ricorso a questo continuo puntellamento normativo conferma, a mio avviso, l'immagine di un edificio che si sta progressivamente sgretolando. La riprova è offerta anche dal fenomeno religioso. All'interno dello Stato di diritto non vi dovrebbe essere nulla di più intangibile del rispetto della libertà di coscienza. Ogni forma di schedatura delle dimensioni interiori dell'esistenza, al di là delle esigenze di sicurezza nei casi più gravi, è in sé un atto intollerabile che impedisce la compiuta realizzazione di sé. Tuttavia l'accesso ai servizi dell'intelligenza artificiale impone un progressivo e costante disvelamento proprio di questo mondo interiore. Un disvelamento che non distingue tra la preghiera e i video-giochi. Tanto l'una quanto gli altri sono riconducili a una stringa numerica che può rifluire in uno dei tanti percorsi di profilazione.

[13] Sugli sviluppi e le implicazioni della *privacy* informazionale rinvio al quinto capitolo di L. Floridi, *Infosfera. Etica e filosofia nell'età dell'informazione*, Giappichelli, Torino, 2009.

Penso al progetto di un robot SanTO[14] che contiene un sistema di dialogo integrato alla comunicazione multimodale, composto da visione, tocco, voce e luci, per gestire l'interazione con gli utenti. È, infatti, dotato di un microfono, sensori e una fotocamera abilitata al riconoscimento facciale, per l'acquisizione dell'identità e per la rilevazione delle emozioni. «Come ti chiami, figliolo?» è la prima domanda del robot, posta con voce profonda e dolce. Poi inizia un dialogo in cui la rete prende il posto del confessionale. Questa innovazione tecnologica è descritta come l'occasione per offrire nuovi spunti al raccoglimento interiore. E che dire dell'app "*confession*" che possiamo scaricare al modico prezzo di € 1,99?

Non possiamo, certo, affermare che anche il sacro stia divenendo (o possa divenire) digitale. La Chiesa continua a ritenere fondamentale per la validità dei sacramenti la dimensione "*in praesentem directa*". Tuttavia è stato presentato al Papa il primo progetto di "Pastorale mediata dalla robotica" dove un piccolo robottino coadiuva nell'assistenza ai fedeli. Questo robottino, magari affiancato dal "collega" SanTO, sarà il futuro sacerdote di una nuova spiritualità? Una spiritualità in cui anche il raccoglimento interiore fornirà i suoi *input* all'infosfera?

Sotto questo punto di vista il *Freedom of Religion or Belief and Security. Policy Guidance* dell'Office for Democratic Institutions and Human Rights dell'OSCE è tanto il segno di un invito a rafforzare la tutela della libertà di coscienza quanto uno dei tanti sintomi della crisi in atto. La preoccupazione, espressa nel documento per i sistemi di profilazione biometrica e di videosorveglianza, mette in luce quanto stia divenendo capillare il controllo politico degli atti di culto. Il fondamentalismo religioso offre l'occasione per giustificate forme estremamente sofisticate di polizia digitale. Non solo la difesa dell'ordine pubblico può arrivare a pesanti limitazioni della tutela della *privacy*, ma ha a disposizione lo sconfinato mondo dei *big data* in cui è difficile individuare una linea di separazione tra le esigenze del mercato dei dati e la loro utilizzazione politica.

Zhongheng Electric, *Clearview AI*, *Sari Real Time* sono imprese commerciali che offrono i propri servizi a qualsiasi acquirente, comprese le forze dell'ordine. Una commistione tra privato e pubblico in cui un qualsiasi ignoto algoritmo ci

[14] G. Trovato, *Il robot SanTO: il nuovo con uno sguardo al passato* in *Filosofia*, 2020/ LXV, p. 34 ss.

può trasformare da consumatori a sospetti terroristi nello spazio di un "clic". Non dobbiamo dimenticare che per la profilazione politica c'è un interlocutore, lo Stato, che, per quanto potente, è individuabile e contestabile, almeno nei sistemi democratici su cui fa affidamento il *Freedom of Religion or Belief and Security*. Per la profilazione economica abbiamo, invece, di fronte la barriera invalicabile di un eterogeno insieme di disparate applicazioni, spesso protette dal segreto industriale e/o coperte dall'opacità tecnologica. Se si saldano profilazione politica e profilazione commerciale, quali spazi restano al rispetto della *privacy*?

Nel 1964 Gunther Anders, riflettendo sulla tendenza alla "macchinizzazione" aveva rilevato che ogni macchina è "imperialistica" o "espansionistica"[15] perché si procura un proprio regno coloniale di servizi. Oggi ci rendiamo conto di quanto sia esteso e frammentato questo regno coloniale. Ognuna delle sei GAFAIM impone le sue regole e sviluppa le sue articolazioni senza che sia possibile individuare soluzioni di continuità tra pubblico e privato, tra il capitalismo della sorveglianza e la sorveglianza attraverso il capitalismo. Se in nome dell'ordine pubblico è stato possibile sospendere le garanzie costituzionali, anche il rispetto dell'ordine economico tende a prevaricare i diritti fondamentali. La tutela della *privacy* costituisce, infatti, un'evidente limitazione all'accrescimento e alla circolazione dei flussi digitali, che sono ormai lo strumento fondamentale degli sviluppi economici. Se analizziamo l'evoluzione giurisprudenziale, ci rendiamo conto di quanto l'inviolabilità del segreto industriale, presidio dell'economia digitale[16], riceva una tutela maggiore del sigillo sacramentale, presidio della libertà religiosa[17].

Da una parte la situazione internazionale giustifica le continue eccezioni

[15] G. Anders, *Noi figli di Eichmann*, Giunti, Firenze, 1995, pp. 53-55.

[16] Penso alla decisione (*State v. Loomis* 881 N.\V.2d 749 - Wis. 2016) con cui la Corte Suprema del Wisconsin, legittimando l'affidamento integrale a un algoritmo della valutazione della pericolosità sociale di un soggetto, sostiene che non è possibile violare il segreto industriale.

[17] A. Licastro, *Facoltà di astensione dalla testimonianza e «sacramentale sigillum»: verso una ridefinizione dei confini del segreto ministeriale?*, in *Quaderni di diritto e politica ecclesiastica*, 2016-3, p. 901 ss.

che consentono allo Stato di acquisire dati sensibili[18]. Dall'altra le pressioni del mercato rendono estremamente difficile, ai singoli cittadini, pretendere di conoscere e limitare le combinazioni algoritmiche che entrano sistematicamente nell'intimità della loro esistenza per vendere loro un prodotto o per venderli come un prodotto. Un'intelligenza artificiale "umano centrica" non può prescindere dalla tutela della *privacy*, ma l'economia digitale tende a renderla solo un vago ricordo del passato. Nella fase di transizione che stiamo vivendo, questa contraddizione ci appare insolubile: possiamo solo prendere atto degli interessi in gioco. Già questa consapevolezza è importante, perché ci consente di non cedere alle suggestioni delle dichiarazioni di facciata. Nessuno esclude esplicitamente la tutela dei valori fondamentali, ma «senza limitare od ostacolare indebitamente lo sviluppo tecnologico o altrimenti aumentare in modo sproporzionato il costo dell'immissione sul mercato di soluzioni di IA»[19]. Quindi…

[18] Gli Stati Uniti, ad esempio, hanno più volte dichiarato di essere pronti a «mettere in atto qualunque azione sia considerata necessaria per la protezione dei propri interessi essenziali nell'ambito della sicurezza», cfr. E. Morozov, *Silicon Valley: i signori del silicio,* cit., p. 47.

[19] Analogamente a quanto previsto anche dall'art. 23 e dal "considerando" 123 del GDPR.