Journal of Ethics and Legal Technologies – Volume 3(2) – November 2021

La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici

Gianluigi Fioriglio

Dipartimento di Giurisprudenza
Università degli studi di Modena e Reggio Emilia

This paper aims at discussing some crucial aspects of data protection in the Algorithmic society, taking into particular account health information, and starting from two shifts: from the Information Society to the Algorithmic Society, on the one hand, and from privacy to data protection, on the other hand. They both serve the purpose of identifying main issues of current laws and of presenting a possible solution to mitigate such issues.

Keywords: privacy, dati sanitari, dati personali, società algoritmica, algoritmi

1. Dalla Società dell'informazione alla Società algoritmica

Algoritmi, robot e agenti intelligenti effettuano, in totale o parziale autonomia, un numero sempre crescente di processi decisionali ed esecutivi, dando così vita e plasmando la contemporanea "Società algoritmica"[1] in cui alla centralità dell'informazione si accompagna quella degli algoritmi eseguiti dai software che, in qualsiasi modo, elaborano o comunque adoperano l'informazione medesima, per cui la società viene organizzata sulla base dei processi decisionali svolti da algoritmi, robot e agenti intelligenti[2]. Proprio gli algoritmi, così, costituiscono il principale intermediario per l'esercizio del potere[3].

Per quanto nessun ambito della società, a livello nazionale e internazionale, sia escluso da questa rivoluzione, ve ne sono alcuni – come quello sanitario e della salute – tanto delicati da richiedere, da un lato, un'ancor più attenta riflessione interdisciplinare[4], e, dall'altro, un intervento del legislatore che sia mirato e realmente efficace, poiché essa ha un impatto potenziale molto forte su ciascuna persona, in relazione alle ipotesi di vulnerabilità temporanea o permanente che conseguono all'insorgenza delle patologie più varie e che, oltre a colpire chi ne è affetto, incidono sulla relativa cerchia di affetti[5].

In linea generale, può sostenersi che un intervento legislativo realmente efficace implicherebbe che il legislatore fosse in grado di ascoltare le tante parti che sono in causa direttamente o indirettamente, mediando poi fra le medesime grazie alla ricerca e al mantenimento di un equilibrio sostenibile fra esse[6]. Ciò non è facile, perché nel settore della salute tali parti spaziano dai pazienti alle famiglie, dalle strutture sanitarie ai vari operatori sanitari, dalle aziende farmaceutiche alle università e ai centri di ricerca, da prestatori di servizi "generici" della Società dell'informazione a quelli specializzati nell'ambito biomedico, e così via.

---

[1] Balkin, 2017, 1219; cfr., inoltre, la relativa discussione di Pasquale 2017, nonché quanto osservato in Gorgoni 2020.

[2] Anche robot, automi e dispositivi "tangibili" richiedono comunque l'esecuzione di un software che ne consente il funzionamento.

[3] Cfr. in tal senso Schuilenburg – Peeters 2021.

[4] Con particolare riferimento alla problematica della responsabilità, ma con una metodologia applicabile anche al di fuori di essa, si può adottare una prospettiva "socio-tecnica" (Vermaas et al. 2011), che consideri artefatti tecnici (sistemi di supporto alle decisioni, robot chirurgici, ecc.), operatori umani e utenti (medici, pazienti, caregiver, ecc.) e artefatti sociali (dalle leggi alle procedure mediche, dalle strutture sanitarie alle agenzie regolatorie, e così via; Lagioia e Contissa 2020, 249).

[5] Sulla vulnerabilità cfr., in particolare: Pastore 2021; Zanetti 2019.

[6] Per un quadro generale, cfr. Barfield 2020.

Questo scenario, oltremodo complesso e variegato, si arricchisce di un ulteriore fattore di complessità in virtù dello sviluppo e della diffusione di agenti artificiali sempre più intelligenti, come si è accennato, e ciò implica necessariamente un aumento del già elevatissimo grado di difficoltà del compito affidato a ciascun legislatore. Difatti, i prodotti e i servizi della Società algoritmica sono caratterizzati da complessità, ubiquità e talvolta inafferrabilità oltre che dall'oscurità delle proprie logiche di funzionamento e dei ragionamenti prodromici allo svolgimento dei relativi compiti[7].

Non si può, tuttavia, pensare di bloccare l'evoluzione tecnologica, sia perché appare irrealizzabile da un punto di vista meramente pratico sia perché i benefici che una simile informatizzazione potrebbe apportare sono tanto grandi da suggerire di non mirare a una limitazione *tout court* bensì a orientare fattivamente la ricerca in tali ambiti, ricordando che sono interdisciplinari per loro stessa natura (e un ruolo cruciale è dunque rivestito dall'Informatica medica[8]).

Alla luce di quanto appena accennato, il presente contributo ha dunque lo scopo di presentare e discutere alcuni aspetti cruciali della corrente evoluzione informatico-giuridica della protezione dei dati sanitari così da delinearne i relativi rischi e opportunità, partendo da due passaggi fondamentali: il passaggio dalla Società dell'informazione alla Società algoritmica e dalla privacy alla protezione dei dati personali, per poi focalizzarsi specificatamente sull'ambito sanitario. Il parallelismo fra questi due passaggi è qui funzionale alla individuazione dei principali profili di criticità nell'attuale regolamentazione nonché di una proposta che consenta quanto meno di mitigarli.

Svolta questa doverosa premessa, si può quindi evidenziare come ancor oggi l'informazione costituisca un bene primario, ma mentre nella Società che viene così definita i sistemi informatici che la raccolgono e la elaborano sono caratterizzati da un'automazione che si potrebbe definire statica e basata sulla effettuazione di uno o più set di operazioni comunque predefiniti *ab origine* da chi ha sviluppato i relativi software, in quella algoritmica all'intelligenza umana del programmatore si affianca quella artificiale del programma o sistema informatico nel suo complesso. Come afferma Sadin, all'intelligenza artificiale si affida addirittura il compito di enunciare la verità[9], per cui, in una certa prospettiva, essa diventa ancor più

[7] Cfr. Fioriglio 2021.
[8] Fioriglio 2020.
[9] Sadin 2020, 10.

importante di quella umana (di cui è il frutto) in quanto novella depositaria della verità[10].

Sorgono, così, numerosi quesiti informatici, giuridici ed etici, di carattere sia generale, già in ordine alla definizione di intelligenza e quindi di intelligenza artificiale, sia particolare, legati alle applicazioni concrete di quest'ultima[11].

Proprio tali applicazioni sono tanto numerose da aver già pervaso la società contemporanea seguendo un percorso che può considerarsi evolutivo o involutivo in base alla considerazione delle loro conseguenze dirette o indirette, che purtroppo non sono sempre percepibili o comunque non lo sono, sovente, in modo adeguato.

Per meglio comprendere quanto appena affermato, basti pensare – senza pretesa di esaustività e a mero titolo esemplificativo – a numerosi prodotti, servizi e attività che vengono svolti adoperando, in modo più o meno marcato, sistemi "intelligenti" in ambito sia pubblico sia privato: la valutazione dell'affidabilità creditizia per la concessione di prestiti e mutui (grazie alla elaborazione di informazioni potenzialmente rilevanti), il supporto alla clientela (mediante chatbot), l'autenticazione degli utenti in sistemi informatici e in luoghi "fisici" (con l'impronta digitale, il volto, ecc.), la fornitura di informazioni in tempo reale sul traffico (grazie alla raccolta e alla elaborazione dei dati raccolti da milioni, se non miliardi, di dispositivi), il trattamento di informazioni online per la prestazione del servizio di motore di ricerca web (con i relativi spider e agenti software), il suggerimento alla fruizione di opere dell'ingegno (sulla base della profilazione dell'utente), la creazione e la gestione delle graduatorie nei concorsi (previe raccolta ed elaborazione dei dati), e così via. In ambito medico, un esempio concreto è fornito dallo strumento di IBM Watson for oncology, un sistema intelligente in grado di generare raccomandazioni e opzioni di trattamento[12].

Ad ogni buon conto, anche ove si dovesse effettuare una simile elencazione con pretesa di esaustività, se ne rischierebbe una obsolescenza già al momento della sua definizione, poiché l'incessante progresso della tecnica e della ricerca la potrebbe arricchire di giorno in giorno non solo mediante

[10] Si realizza così, surrettiziamente, una tendenza involutiva che contrasta con la consapevolezza centrale negli Stati costituzionali di essere destinati a una mera ricerca della verità poiché non si è in possesso di verità precostituite eterne. Essi, difatti, si fondano su verità provvisorie e rivedibili, assunte in linea di principio al plurale e non al singolare oltre che non imposte mediante l'emanazione di atti normativi (Häberle 2010, 85). Oggi, però, la verità rischia di essere imposta dai sistemi intelligenti in quanto enunciatori della verità costruita da essi stessi grazie alle proprie elaborazioni.

[11] Per un quadro generale, dal punto di vista "tecnico", sull'intelligenza artificiale cfr. Russell – Norvig 2021.

[12] Su questo sistema cfr. Lagioia – Contissa 2020.

nuove applicazioni, ma anche grazie alla combinazione di più applicazioni diverse (ad esempio, l'utilizzo di un sistema intelligente di autenticazione al proprio veicolo a guida autonoma che a sua volta, mediante ricorso a un servizio di terze parti, può profilare l'utente-passeggero suggerendogli determinate opere dell'ingegno di cui fruire durante il percorso, o, quanto il veicolo non è a guida completamente automatizzata, può verificare lo stato di salute del conducente, e dunque trattare i relativi dati personali, così da valutarne l'idoneità alla guida[13]). Ovviamente una mappatura, che non può essere svolta in questa sede, ha comunque una sua utilità, consentendo di cristallizzare a un determinato momento storico l'ampio ventaglio di possibilità concrete offerte dalla ricerca in questo ambito (e di ciò dovrebbe essere ben conscio qualsiasi legislatore, per regolamentarlo compiutamente).

A livello più generale, può osservarsi che le sfide che ne derivano per l'etica e per il diritto siano già oggi numerosissime e come il riferimento all'algoritmo sia oramai di prassi e, per certi versi, molto utile grazie alla sua forza evocativa che descrive un aspetto certamente caratterizzante la società contemporanea.

Del resto, al modello tradizionale in cui lo sviluppo di un sistema intelligente necessita della fornitura all'elaboratore di una completa rappresentazione formale della conoscenza nonché di algoritmi capaci di compiere inferenze e ragionamenti se ne è oggi sostituito un altro, in cui vengono applicati metodi di apprendimento automatico *(machine learning)* a grandi masse di dati. In tal modo si superano le problematiche consistenti nella potenziale incompletezza della base di dati, nella incapacità di considerare le specificità dei casi concreti, nell'onerosità di ampliamento e aggiornamento della base di conoscenza[14].

Il sistema intelligente, così, *impara facendo* ed elaborando la massa di dati cui può avere accesso (e in ipotesi può imparare a trovare nuovi metodi per avere accesso a ulteriori informazioni), ma ovviamente diviene quasi o del tutto impossibile prevedere le sue "azioni", così come le loro conseguenze[15]. Si realizza, così, un passaggio dalla Società dell'informazione alla Società algoritmica che è opportuno leggere in parallelo a un altro passaggio, quello dalla privacy alla protezione dei dati personali, per poi focalizzarsi specificatamente sull'ambito sanitario e della salute.

[13] In argomento cfr., ex multis, l'ampio quadro in Scagliarini 2019b.

[14] Sartor 2020, 66.

[15] Cfr. Sartor 2003 per una eccellente discussione su questo e altri aspetti degli agenti software. Per un'analisi della dimensione semantica del concetto di prevedibilità delle condotte di macchine intelligenti cfr., da ultimo, Salardi 2021.

2. Dalla privacy alla protezione dei dati personali

La prima compiuta concettualizzazione del diritto alla privacy si deve, com'è noto, a due giuristi statunitensi, Samuel D. Warren e Louis D. Brandeis, i quali lo hanno teorizzato quale *right to be let alone* nell'omonimo saggio sul finire dell'Ottocento[16], proponendo un'impostazione che tratteggia la sfera negativa della riservatezza, consistente nella pretesa di non subire ingerenze nel proprio ambito privato. Ad essa si è progressivamente affiancata la costruzione di una sfera positiva, consistente invece nella pretesa (e talvolta nella pia illusione) di controllo sui propri dati personali.

Se di primo acchito pare quasi di trovarsi dinanzi a una dicotomia (negativo e positivo, passivo e attivo) cui conseguirebbe l'obsolescenza della prima sfera sopracitata, a uno sguardo più approfondito si può invece argomentare che essi siano profili complementari e non coincidenti.

Per approfondire proficuamente quanto appena affermato è opportuno partire dalle parole di Stefano Rodotà, secondo cui la privacy "è stata costruita come un dispositivo «escludente», come uno strumento per allontanare lo sguardo indesiderato. Ma l'analisi delle sue definizioni mostra anche le sue progressive trasformazioni, che hanno fatto emergere un diritto sempre più finalizzato a rendere possibile la libera costruzione della personalità, l'autonomo strutturarsi dell'identità, la proiezione nella sfera privata dei principi fondamentali della democrazia"[17].

Di certo questa linea evolutiva trova un compiuto riscontro nella legislazione positiva che, nel bene e nel male, ha segnato gli ultimi decenni nella direzione di un potenziamento della sfera positiva a scapito, potrebbe dirsi, di quella negativa (che rimane sullo sfondo e viene sovente richiamata ma, nei fatti, poco tutelata): con precipuo riferimento all'ambito europeo, basti pensare alla direttiva 95/46/CE, seguita dal regolamento (UE) 679/2016 (*General Data Protection Regulation, GDPR*, o Regolamento Generale sulla Protezione dei Dati, RGPD) avente ad oggetto la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la loro libera circolazione all'interno dell'Unione Europea.

Per comprendere le motivazioni che hanno spinto i vari legislatori nel senso sopra citato è tuttavia opportuno ricordare che l'esigenza di una regolamentazione a tutela della summenzionata sfera positiva sia sostanzialmente sorta a partire dagli anni Settanta in seguito alla creazione e alla diffusione delle prime banche dati informatizzate, che hanno consentito operazioni di trattamento dei dati personali prima praticamente irrealizzabili

[16] Warren – Brandeis 1890.
[17] Rodotà 2012, 320.

dal punto di vista sia quantitativo (numero di dati) sia qualitativo (tipologia delle operazioni effettuate o effettuabili).

Appare dunque chiaro perché e come si sia giunti alla costruzione sia della sfera negativa che di quella positiva.

Nel primo senso, il diritto alla privacy è stato infatti configurato inizialmente come un baluardo a tutela della persona dai mass media che iniziavano a oltrepassare il confine che separa l'ambito pubblico da quello privato, da sottrarre agli indiscreti sguardi altrui (partendo da Warren e Brandeis).

Nel secondo senso, e seguendo una direttrice per certi versi analoga, il diritto alla protezione dei dati personali è stato pensato primariamente per difendere la persona dalle nuove modalità di raccolta ed elaborazione di informazioni non necessariamente private ma il cui trattamento possa comunque comportare rischi per la libertà, la dignità e altri diritti. Il diritto alla protezione dei dati personali, così, concretizza la risposta di numerosi legislatori alle istanze di regolamentazione della Società dell'informazione.

Pare, tuttavia, che l'evoluzione legislativa si sia qualitativamente arrestata, nonostante i proclami sulle prossime regolamentazioni[18] e nonostante l'approvazione del GDPR: già i richiami qui solo sommariamente e succintamente svolti consentono di dedurre che il diritto alla protezione dei dati personali, per come oggi concettualizzato o comunque regolamentato, si appalesi anacronistico. Rimane, infatti, un diritto che affonda le sue radici più profonde nella società degli anni Settanta che si apprestava a diventare la Società dell'informazione. Un mondo, quello, in cui effettivamente la pretesa al controllo pareva realizzabile e certamente utile.

È un mondo, però, che è profondamente mutato: in primo luogo, il dato è sempre meno controllabile, fra Big Data e sistemi in cloud (o comunque sostanzialmente inaccessibili a chi dovrebbe sorvegliare l'applicazione della normativa). Inoltre, nella Società algoritmica il dato è certamente centrale, ma il tratto caratterizzante è costituito dall'elaborazione automatizzata, soprattutto su larga scala, che consente altresì l'automazione dei processi decisionali. È qui che può emergere l'importanza di un recupero della concezione negativa del diritto alla privacy, quale diritto a non subire ingerenze nella propria sfera privata, recuperandone così la sua funzione primaria di baluardo a difesa della persona, più che dei soli (ancorché importanti) dati ad essa riferibili.

[18] Si pensi, in particolare, alla proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale del 21 aprile 2021 – COM(2021) 206 final.

In secondo luogo, si pone, a livello generale, il c.d. paradosso della privacy, per cui normalmente le persone pubblicamente dichiarano di attribuire una elevata importanza alla propria privacy, ma sono pronte a comunicare anche dati sensibili per piccoli sconti, minimi benefici, o anche in loro assenza. Come affermato in dottrina, gli studi in materia dimostrano la sussistenza di un divario fra l'attitudine a livello generale delle persone e la loro condotta concreta, ma esso non dovrebbe essere considerato un'anomalia in quanto la seconda dipende dal contesto in cui si svolge mentre la prima si pone a un livello astratto che trascende proprio contesti particolari[19].

In un simile scenario, l'impostazione burocratica e burocratizzata del GDPR sembra rivelarsi un retaggio del passato più che una normativa idonea a proteggere realmente i diritti e le libertà di ciascun interessato nella Società algoritmica, come si discuterà nel prosieguo sulla base della considerazione unitaria dei due passaggi sin qui citati: da un lato, dalla Società dell'informazione a quella algoritmica; dall'altro dalla privacy alla protezione dei dati personali.

Da uno sguardo d'insieme a entrambi, infatti, emerge una progressione a diverse velocità. Se le tecnologie che plasmano la società e che rendono sempre più cruciale la difesa della sfera privata di ciascuna persona (e di ciascun gruppo sociale) avanzano a un ritmo impressionante[20], gli strumenti di protezione effettiva diventano obsoleti senza tuttavia essere aggiornati o rimpiazzati, il che appare particolarmente grave nei settori a maggior rischio, come quello sanitario e, più in generale, della salute.

3. I dati personali nell'ambito della salute: dal diritto alla realtà

L'ambito della salute è, per sua natura, particolarmente delicato e ciò trova riscontro anche nella regolamentazione dei dati personali. Non a caso, già nella direttiva 95/46/CE è stato sancito, in linea generale, il divieto di trattare proprio i dati relativi alla salute (art. 8, par. 1), fatte salve le eccezioni di cui all'art. 8, par. 2; inoltre, la l. 675/96 ha annoverato i "dati personali idonei a rivelare lo stato di salute" fra i "dati sensibili" (art. 22).

Non è questa la sede per un compiuto approfondimento della normativa vigente[21], essendo qui sufficiente richiamare alcuni concetti chiave, ossia:

[19] Solove 2020, 51.

[20] Non a caso, "Sorge il sospetto[…] che, oltre a chiederci come si possa regolare il digitale e chi possa farlo, ci sia anche da chiedersi – una domanda che non può essere aggirata – come il digitale ci regola e come questo linguaggio stia trasformando la nostra esperienza e gli altri linguaggi" (Andronico – Casadei 2021, 8).

[21] La letteratura in materia è oramai sterminata, in riferimento al GDPR sia al novellato

dati relativi alla salute, divieto di trattamento di categorie particolari di dati, eccezioni a tale divieto.

Innanzi tutto, per "dati relativi alla salute", ai sensi dell'art. 4(15) GDPR, si intendono "i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute". Inoltre, l'art. 9, par. 1, GDPR dispone il divieto di " trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". Infine, l'art. 9, par. 2, GDPR prevede diverse eccezioni al divieto appena menzionato, fra cui possono qui ricordarsi [22]: il consenso; il rispetto della normativa in materia di diritto del lavoro e della sicurezza sociale e protezione sociale; l'interesse vitale dell'interessato o di altra persona fisica; i dati resi manifestamente pubblici dall'interessato; l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o l'esercizio di funzione giurisdizionale da parte di un'autorità giurisdizionale; i motivi di interesse pubblico se proporzionali rispetto alla finalità perseguita; la finalità di medicina preventiva o del lavoro o di valutazione della capacità lavorativa del dipendente, nonché la diagnosi, l'assistenza o terapia sanitaria o sociale, la gestione di sistemi e servizi sanitari o sociali (sulla base del diritto dell'Unione europea o nazionale o di un contratto con professionista della sanità); i motivi di interesse pubblico nel settore della sanità pubblica, come "la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici".

A un primo sguardo, avulso dalle considerazioni sulle specificità della Società algoritmica, ci si potrebbe illudere circa l'insussistenza di timori in ordine a una insufficiente protezione della privacy sanitaria, che si guardi alla sua sfera negativa o positiva: ciò grazie all'ampia nozione di dato relativo alla salute e alla regola generale del divieto dei relativi trattamenti, fatte salve le dovute eccezioni di cui si è brevemente detto, nonché – si potrebbe aggiungere – al severo regime sanzionatorio delineato dal GDPR (che prevede sanzioni sino a venti milioni di euro o sino al quattro per cento del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, *ex* art. 83 GDPR).

È una normativa tanto severa, del resto, da comportare anche taluni effetti indesiderati per la ricerca e la pratica clinica: un esempio concreto

D.lgs. 196/2003 per ciò che concerne l'ordinamento italiano. Ex multis, cfr. Pizzetti 2021; Riccio – Belisario – Scorza 2018; Scagliarini 2019a.

[22] Si rinvia all'art. 9, par. 2, GDPR, per ulteriori specificazioni.

ed emblematico è costituito dagli ostacoli all'utilizzo (e al riutilizzo) dei dati relativi alla salute nell'ambito dei trial clinici a causa del concorso delle disposizioni circa le finalità (che devono essere, ovviamente, esplicite, determinate e legittime) e il consenso, che in ultima analisi rendono estremamente difficoltoso, e talvolta impossibile, anche solo poter comunicare ai partecipanti a un trial clinico l'eventuale scoperta di una nuova cura per la loro patologia. Ciò in quanto i dati sono memorizzati in differenti banche dati o archivi che costituiscono, legalmente, dei compartimenti stagni[23].

Guardando in altro senso, poi, all'efficacia della normativa vigente, il quadro cambia, ove si guardi soprattutto a tre profili: la molteplicità di violazioni del diritto alla protezione dei dati sanitari (con particolare ma non esclusivo riferimento ai casi di *data breach*[24]); i trattamenti svolti al di fuori di una possibilità di reale controllo da parte dell'interessato; la "zona grigia" di prodotti e servizi che non sono commercializzati quali dispositivi medici o comunque forniti nell'ambito delle attività delle strutture sanitarie e dei professionisti della salute, ma che effettuano trattamenti di dati sanitari anche in cloud (come smartwatch e altri dispositivi indossabili).

I suddetti profili non sono un portato esclusivo della Società algoritmica, in quanto costituiscono una conseguenza dell'avvento della Società dell'informazione, ma è con la prima che assumono una importanza e una estensione prima impensabili. Come controllare, infatti, una molteplicità di informazioni, memorizzate nei formati più diversi, che viaggiano nel cyberspazio e che vengono elaborate da sistemi intelligenti che sovente costituiscono delle "scatole nere"[25] e che sono in grado di profilare le persone nonché di comprendere e mettere in relazione enormi quantitativi di dati? Queste riflessioni impongono, dunque, di soffermarsi su tali frontiere della tecnologia che, pur non essendo ormai più nuove (ancorché recenti), sono in costante evoluzione: si delinea sin d'ora, però, uno scenario in cui può ravvisarsi un ampio iato fra un diritto obsoleto, perché basato sui paradigmi della Società dell'informazione, e una tecnologia in progresso costante, che connota la Società algoritmica.

[23] Proprio tale questione è centrale nel progetto FACILITATE ("FrAmework for ClInicaL trIal participants daTA reutilization for a fully Transparent and Ethical ecosystem"), https://cordis.europa.eu/project/id/101034366, finalizzato a costruire un framework legale ed etico, oltre che tecnico, per risolverla.

[24] Il "data breach" è la "violazione dei dati personali", ossia "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" (art. 4(12) GDPR).

[25] Cfr. Pasquale 2015.

4. Profilazione e Big Data: dal mercato alla salute

La profilazione automatizzata delle persone fisiche svolta dai sistemi informatici costituisce al contempo una opportunità e un rischio.

Essa, infatti, consente di offrire prodotti e servizi sempre più personalizzati nell'ambito del mercato, trovando così applicazione nell'offerta di prodotti mediante siti di ecommerce, di servizi di social network o di motore di ricerca web, di applicazioni per il fitness, e così via. Vengono quindi costruiti i "classici" profili utente legati a ciascun account che consentono di accedere ai servizi di un sito o di un'applicazione, ma si corre il rischio che essi siano sostanzialmente il cavallo di Troia per la creazione di profili utente che costituiscono vere e proprie rappresentazioni digitali dell'identità non della persona in quanto tale bensì di essa quale mera consumatrice di prodotti e servizi, in una prospettiva di disumanizzazione che viene mascherata dalle modalità con cui il sistema intelligente si relaziona con l'utente (dagli assistenti vocali alle pagine che vengono strutturalmente personalizzate prevedendo dei campi dinamici che dovrebbero far percepire all'utente medesimo un ambiente "familiare", in cui sentirsi a suo agio).

Diviene così più facile fruire dei prodotti e dei servizi della Società algoritmica, sovente pagando coi propri dati personali quando essi sono apparentemente forniti a titolo gratuito. Può così osservarsi una tendenza al riduzionismo della persona a un complesso di dati e quindi il rischio del "dataismo"[26], anche per cercare di calcolare quegli aspetti emotivi ed imprevedibili che connotano la natura umana, da un lato, e che costituiscono tuttora un'ardua sfida per gli elaboratori elettronici, dall'altro; del resto, quest'ultimi sono costruiti proprio per "computare"[27].

La profilazione, che si lega senza esaurirla alla più ampia questione dell'identità digitale, tocca sempre più anche la sfera della salute sia per ciò che concerne la fornitura di servizi e prestazioni sanitarie in senso stretto, ivi inclusa la pratica clinica, sia in relazione a prodotti e servizi che, in un modo o nell'altro, incidono sull'ambito della salute ed effettuano trattamenti di dati sanitari, come diversi dispositivi indossabili fra cui gli ormai numerosi smartwatch dotati di pulsossimetro o in grado di effettuare

[26] Oltretutto si pone il rischio dell'affermazione di una nuova forma di riduzionismo: il "dataismo", in relazione a cui può osservarsi il "dato" è, necessariamente, una riduzione della realtà, una sua rappresentazione semplificata e parziale (oltre che decontestualizzata e ri-contestualizzata), in quanto è una descrizione elementare, o anche codificata, di una entità, di un fenomeno, di un avvenimento. Così, come i dati sono una riduzione della realtà, anche il loro uso rischia di essere una rappresentazione riduttiva del reale (in quanto il reale non può essere considerato quale mera somma delle sue parti). Cfr., in particolare, Palazzani 2020.

[27] Sul punto cfr. altresì l'inquadramento generale in Casadei – Pietropaoli 2021.

un elettrocardiogramma (i cui dati vengono poi sovente elaborati o memorizzati in cloud).

Il concetto alla base della profilazione, ossia la costruzione di una specifica identità digitale, va oggi ad evolversi in ambito sanitario, grazie non solo alla capillare diffusione, fra l'altro, degli *Electronic Health Records* (e nell'ordinamento italiano del Fascicolo Sanitario Elettronico), ma altresì alla effettuazione di ricerche e studi sulla medicina di precisione, finalizzati a personalizzare la terapia per ciascun paziente[28].

Tutte queste evoluzioni (e talvolta involuzioni) richiedono, però, una mole enorme di informazioni da trattarsi non solo e non tanto con le tecnologie proprie della Società dell'informazione ma soprattutto con quelle della Società algoritmica. È questa, infatti, la chiave di lettura dei nuovi processi evolutivi, in cui i sistemi intelligenti sono sempre più tali e riescono a compiere operazioni così complesse da essere sostanzialmente precluse alla mente umana, per quanto ciò possa affermarsi solo in relazione a domini e compiti estremamente specifici. Questi sistemi sono infatti in grado di trattare una mole enorme di dati, anche diversi in quanto a tipologia (dal testo alle immagini, dalle registrazioni sonore a quelle audiovisive) e a formato; e se la loro componente dedicata all'apprendimento automatico è stata ben programmata, più dati hanno a disposizione, più sono in grado di imparare e di perfezionarsi (e magari di imparare, ciascuno come "autodidatta", ulteriori metodologie di apprendimento: il sistema intelligente, novello educando, si educa da se).

Non v'è dubbio, pertanto, che i Big Data assumano oggi un'importanza fondamentale. Com'è noto, con tale locuzione si indica una ingente mole di dati informatici le cui caratteristiche principali sono facilmente riassumibili seguendo il modello delle tre "v": volume (grandi quantità), velocità (incremento esponenziale della velocità di generazione dei dati sino alla loro acquisizione ed elaborazione in tempo reale), varietà (diverse tipologie da diverse fonti, per cui si ha una forte eterogeneità)[29].

Il punto cruciale non sta, però, nell'elemento quantitativo richiamato dal riferimento alla quantità ("big"), bensì nella possibilità di estrarre correlazioni probabilistiche inattese dalle grandi masse di dati grazia alla Data analytics, che trova applicazione in numerosi ambiti sia pubblici sia privati, ad esempio per analizzare le dinamiche dei mercati e cercare di prevedere l'evoluzione di domanda e offerta; ciò consente di orientare

[28] È il caso, questo, della medicina di precisione; cfr. sul punto, Di Giandomenico – Fioriglio 2020.

[29] Questa è, ovviamente, la nota impostazione "tradizionale", anche se, a seconda dei casi, ne vengono proposte altre (in particolare, veridicità e valore).

l'andamento dei prezzi di prodotti e servizi nonché di comprendere, in un periodo specifico, quale potrebbe essere il target di riferimento.

Di certo, l'avvento della Società dell'informazione ha aperto la strada ai Big Data, comportando un aumento esponenziale delle informazioni digitali o digitalizzate. Tuttavia, avere accesso a un ingente quantitativo di dati è un elemento necessario ma non sufficiente: bisogna avere infatti a disposizione delle tecnologie molto sofisticate per poterle analizzare proficuamente (e in tempi estremamente rapidi). Come si è detto, del resto, è proprio la qualità dell'elaborazione dei dati a essere centrale nell'evoluzione della Società dell'informazione in Società algoritmica.

Questo passaggio ha tuttavia colto impreparati i vari legislatori, come dimostra la sostanziale assenza di normative specifiche che regolamentino, in particolare, l'intelligenza artificiale; a nulla valgono le proposte e i solenni proclami in assenza di interventi legislativi specifici, con la conseguenza che tale componente fondamentale della società contemporanea è governata dai nuovi poteri privati, ossia da quei soggetti che forniscono i maggiori servizi in materia e che hanno sia il know-how sia le strutture materiali su cui transitano i dati e nelle quali essi possono essere elaborati.

È pur vero che determinati limiti a siffatte operazioni, in riferimento a quelle che coinvolgono dati personali, sono comunque stabiliti dal GDPR, e dunque da una normativa cardine per l'Unione europea che fa altresì avvertire i propri effetti su un ambito più ampio in virtù della sempre crescente fornitura di servizi su scala globale. Questo profilo positivo è fortemente contemperato dalla considerazione per cui il suddetto Regolamento aggiorna ed evolve, senza rivoluzionarlo, l'approccio seguito dal legislatore della Direttiva 95/46/CE, basato sull'osservazione della Società dell'informazione e non di quella algoritmica (indipendentemente dal rafforzamento dei principi della privacy by design e by default, nonché dalla forte previsione del principio di accountability: i meccanismi di base, in fin dei conti, partono pur sempre dall'obiettivo cardine consistente nel diritto, in capo all'interessato, di controllare i propri dati personali).

Come conseguenza che potrebbe dirsi indesiderata, mediante tale intervento vengono legalmente posti dei limiti che appaiono più efficaci, loro malgrado, per le attività di ricerca in ambito medico e scientifico che in quello della fornitura al pubblico di prodotti e servizi.

Basti pensare, in tal senso, alle grandi aziende che detengono una posizione monopolistica o dominante in determinati settori, come Amazon fra le piattaforme di e-commerce e di fornitura di servizi informatici (Amazon Web Services), Google fra i prestatori del servizio di motore di ricerca, hosting video e di altri servizi (oggi nell'ambito di Google Workspace), Facebook fra le reti sociali, Microsoft per i sistemi operativi (Windows), e così via.

Essi, infatti, trattano un ingente quantitativo di dati al di fuori del controllo reale delle autorità pubbliche: non risultano, allo stato, controlli effettivi in tal senso (oltretutto estremamente difficoltosi, a causa delle enormi dimensioni e della dislocazione delle loro server farm) e ciò comporta, altresì, l'acquisizione di un enorme vantaggio competitivo che pone altresì barriere quasi insormontabili a nuovi concorrenti e che, in ultima analisi, consente loro di orientare l'evoluzione della società grazie al controllo di questi inafferrabili flussi informativi di cui i Big Data costituiscono forse l'espressione più emblematica[30].

Se a livello generale i problemi etici e giuridici che ne scaturiscono appaiono estremamente delicati, in riferimento all'ambito della salute lo sono ancor di più, in quanto aumenta il rischio di possibili violazioni del diritto alla privacy e di quello alla protezione dei dati personali (un ostacolo per chi vuole acquisire il maggior numero possibile di informazioni) e sullo sfondo si pone la questione del *bias* nella formulazione degli algoritmi, cui possono conseguire potenziali discriminazioni, che si accompagna all'opacità delle già citate "scatole nere" che effettuano le elaborazioni, nascondendo i ragionamenti effettuati per il compimento di determinate scelte[31].

Non si può, infatti, argomentare un'oggettività dei Big Data, in quanto la straordinaria potenza di calcolo e l'apprendimento automatico basato su dati statistici non consentono, di per sé, una reale comprensione del loro operare [32], per quanto quest'ultima sia comunque mediata – seppur *ab origine* – dalle scelte dei programmatori. Oltre a ciò, si consideri che l'affidabilità stessa delle elaborazioni compiute dai sistemi di Big Data Analytics richiede che i dati medesimi siano esatti e non errati, il che potrebbe viziare le elaborazioni svolte dai sistemi intelligenti (per quanto a livello statistico anche ciò potrebbe essere previsto).

Pertanto, lo scenario qui solo tratteggiato in alcuni elementi essenziali appare, al contempo, foriero di opportunità e di rischi, presenti o futuri: è comunque necessaria una riflessione interdisciplinare che metta al centro non solo l'evoluzione tecnologica ma altresì le questioni giuridiche ed etiche affinché la tecnologia sia incentrata sulla persona e non sia

[30] La letteratura in materia è molto ampia e in costante evoluzione. Un buon punto di partenza può essere costituito da Mayer-Schönberger – Cukier (2017); per una visione di insieme sulla Data society cfr. Faini 2019 e sulle sfide giuridiche dei Big Data Cannataci – Falce – Pollicino 2020.

[31] La questione della "spiegabilità" dei ragionamenti compiuti dai sistemi intelligenti sta diventando sempre più cruciale; sul punto sia consentito rinviare a quanto osservato in Fioriglio 2020, e cfr. altresì, fra gli altri, Pagallo 2020.

[32] "I dati non sono oggettivi e i modelli statistici rappresentano la realtà modificandola, e cioè orientando i comportamenti" (Amato Mangiameli 2019, 111).

autoreferenziale (o comunque finalizzata unicamente al raggiungimento di obiettivi finanziari).

5. Le criticità informatico-giuridiche della "zona grigia" dei servizi e dei dispositivi della Società algoritmica nell'ambito della salute

Come si è detto, l'ambito della salute, inteso nel suo complesso, non riguarda solo quello medico-sanitario in senso stretto, e dunque le attività svolte dai professionisti e dagli operatori sanitari individualmente e/o nelle strutture sanitarie. Diversi fattori, fra cui la crescente attenzione verso stili di vita salutistici o comunque orientati al wellness, nonché l'evoluzione delle pratiche e degli studi sulla telemedicina, hanno così alimentato l'offerta di servizi e prodotti, anche altamente tecnologici, prima riservati proprio agli operatori professionali. Inoltre, la grande diffusione di social network e di strumenti di comunicazione a distanza rende agevolmente possibile l'effettuazione di consulti anche esclusivamente online in tutte le loro fasi.

Convivono, così, dispositivi medici (rigidamente regolamentati, com'è giusto che sia) e servizi sanitari "tradizionali", ancorché resi con modalità innovative, con una nuova "zona grigia" in cui operano dispositivi e vengono resi servizi ai consumatori/pazienti nell'ambito della salute.

È, questa, un'altra sfida per ciascun legislatore, che si trova a dover regolamentare non solo le nuove modalità di erogazione delle prestazioni sanitarie, ma altresì a disciplinare o meno determinate fattispecie che si pongono al confine con le medesime – o che tale confine oltrepassano, ma che vengono rese sfruttando le potenzialità degli strumenti informatici e delle reti telematiche per tentare di sottrarsi a eventuali controlli o comunque a limitarne gli effetti operando, magari, da giurisdizioni diverse[33].

Il quadro è ampio e non comprende unicamente i dispositivi indossabili cui si è già accennato, ma altresì tutti quei servizi che hanno un impatto, anche indiretto, in fase preventiva o terapeutica, ivi inclusi i servizi che forniscono informazioni mediche online.

[33] Come evidenzia il Comitato Nazionale per la Bioetica, diversi soggetti tendono ad aggirare la normativa in materia presentando i propri prodotti e servizi come semplici modalità di controllo del benessere nonostante siano, in sostanza, dei veri e propri dispositivi medici, per cui è possibile riscontrare un'ambiguità nell'offerta di applicazioni sulla salute, che da un lato consentono ai produttori di tenersi a distanza dalle applicazioni medicali in senso stretto ma che dall'altro si pongono come vicine alla salute, distribuendo applicazioni sempre più connesse alla salute che non vengono però qualificate come mediche (Comitato Nazionale per la Bioetica 2015, 9).

Sembra dunque realizzarsi una sorta di telemedicina diffusa e non del tutto controllata. Per approfondire questo profilo è opportuno partire dalla sua definizione come "l'integrazione, monitoraggio e gestione dei pazienti, nonché l'educazione dei pazienti e del personale, usando sistemi che consentano un pronto accesso alla consulenza di esperti ed alle informazioni del paziente, indipendentemente da dove il paziente o le informazioni risiedano"[34]. Normalmente si distingue fra telediagnosi, teleassistenza, telesoccorso, teledidattica e in base all'attività svolta ed al fruitore della stessa (medici, infermieri, personale tecnico e amministrativo; pazienti e loro congiunti; studenti).

La telemedicina può agevolare l'esercizio delle attività cliniche, assistenziali e didattiche, anche grazie alla capillarità della rete Internet e alla pervasività di dispositivi di uso comune quali smartphone e computer, oltre, ovviamente, ai dispositivi medici veri e propri; si possono così trasmettere e condividere informazioni sanitarie di qualsiasi tipo ed a velocità sempre crescenti. La telemedicina, poi, appare particolarmente utile qualora sia necessario monitorare le condizioni di salute di persone che si trovano in isolamento domiciliare, così da ridurre il carico di lavoro delle strutture sanitarie garantendo, al tempo stesso, il loro diritto alla salute dal momento che si potrebbe intervenire solo in caso di bisogno, evitando un inutile dispendio di risorse.

Oltretutto, questo scenario si è oggi arricchito notevolmente grazie al progresso delle tecnologie, per cui anche app e sensori integrati in dispositivi indossabili di uso comune possono diventare strumenti preziosi nell'ambito della telemedicina. Ad esempio, è possibile effettuare esercizi di fisioterapia mediante applicazioni di realtà virtuale e aumentata, monitorare costantemente lo stato di salute di un paziente, coadiuvarlo nel controllo del rispetto delle terapie farmacologiche, ecc.

La diffusione delle tecnologie appena menzionate, nonché la raccolta e l'elaborazione di Big Data, fanno emergere la centralità di un nuovo concetto: quello di *Mobile Health* (*mHealth*), che può definirsi come "l'insieme di tecnologie "mobili", ossia l'uso di comunicazione wireless (cellulari e smartphone, tablet, dispositivi digitali, con o senza sensori indossabili), applicate in ambito medico-sanitario o in ambiti correlati alla salute"[35].

Tali tecnologie possono comportare nuove opportunità per la salute, essendo idonee a promuovere uno stile salutare di vita, facilitare e velocizzare la comunicazione medico/paziente, personalizzare i trattamenti, incrementare

[34] Questa definizione, del 1990, è del gruppo di lavoro creato dalla Commissione Europea su "Advanced Informatics in Medicine".

[35] Comitato Nazionale per la Bioetica 2015, 5.

l'autonomia e la sicurezza del paziente che può essere controllato e localizzato a distanza, migliorare l'efficienza del sistema sanitario (attraverso la riduzione dei costi di assistenza e ospedalizzazione, la telemedicina, la comunicazione di informazioni), contribuire alla ricerca (acquisendo dati soprattutto per ricerche epidemiologiche, studi della correlazione tra determinate condizioni mediche e ambientali, ecc.), ampliare l'accesso alle cure raggiungendo utenti che altrimenti non avrebbero avuto assistenza medica, stimolare il trasferimento di ricerca, la produzione e l'innovazione, condividere casi clinici e richiedere secondi pareri in tempo reale[36].

La diffusione di app, professionali e non, nell'ambito della salute che vengono sviluppate e rese disponibili e che riescono a sfruttare le potenzialità dei dispositivi adoperati pone, però, il problema della loro validazione e della loro regolamentazione[37], anche per evitare una diffusione incontrollata di app che potrebbero risultare dannose. Inoltre, è evidente che il loro utilizzo comporta necessariamente il trattamento di una enorme mole di dati personali, sovente al di fuori di qualsiasi possibilità di controllo effettivo da parte di ciascun utente (interessato), che non conosce effettivamente quali e quanti dati vengono effettivamente trattati (o che venga rispettato quanto affermato nella informativa sulla privacy, ove resa).

Oltretutto, la *mobile health* "fa emergere una nuova forma di vulnerabilità dell'era tecnologica" e gli utenti possono diventare vittime di "forme ossessive di salutismo individualistico e di medicalizzazione" mirando a "conformarsi ad uno standard 'normale' definito dagli sviluppatori sulla base di parametri statistici sociali: la standardizzazione porta alla creazione di 'norme di comportamento' che tendono ad imporsi (peraltro, spesso in modo arbitrario o meramente statistico), diminuendo la sfera personale di libertà"[38].

In un simile scenario emerge, ancora una volta, la centralità del diritto alla protezione dei dati personali, poiché, nel loro funzionamento, questi dispositivi e questi servizi richiedono necessariamente il trattamento di una ingente mole di dati relativi allo stato di salute, che possono essere raccolti su larga scala e dunque andare ad arricchire la galassia dei Big Data, come già discusso. Inoltre, l'eventuale mancanza di controllo sui relativi flussi informatici fa riemergere l'opportunità di richiamare nuovamente anche la sfera negativa del diritto alla privacy: quella di non subire ingerenze nella propria sfera privata, ingerenze che oggi sono magari impercettibili quando

[36] Ivi, 7.

[37] Si consideri, altresì, che il controllo sulle app non è svolto da enti pubblici, bensì da chi gestisce lo "store" da cui scaricare le app medesime (in primis, Apple per iOS e Google per la maggior parte dei sistemi Android). Un controllo, dunque, sul rispetto delle relative policy che ha chiaramente una finalità diversa da quella della tutela della salute.

[38] Palazzani 2017, 370.

vengono svolte ma le cui conseguenze, come nei casi di violazioni dei dati personali, possono essere anche assai gravi. Il confine fra le due sfere, in tal senso, appare quasi evanescente, ma è forse utile richiamare il concetto originario di privacy intesa quale baluardo a tutela della persona umana, in aggiunta alla pretesa di controllo sui dati personali che la riguardano. Sullo sfondo, in ogni caso, rimane il problema di una sua nuova concettualizzazione che tenga conto delle peculiarità della Società algoritmica.

6. Riflessioni conclusive: privacy, dati personali e nuove sfide dell'algoritmizzazione

Gli algoritmi non sono neutrali, né tecnicamente né eticamente[39] e stanno plasmando una società connotata dalla primazia di chi detiene il potere tecnologico. Esso è un potere esercitato pubblicamente i cui meccanismi di funzionamento sono oscuri, celati dal connubio fra la tecnica e il diritto; è, inoltre, un potere esercitato da pochi soggetti, per cui si realizza una sorta di coesistenza nel governo dei territori fisici e digitali fra democrazia, tecnocrazia e tecnoligarchia (quest'ultima a opera di quella che è, come si è osservato, una piccola frazione dell'umanità che progetta e sviluppa un set di tecnologie che stanno già trasformando la vita quotidiana di tutta la parte restante)[40].

Oltretutto, e in linea generale, "oggi non solo il giurista e il filosofo, che avvertono i rischi di una virtualità/realtà dominati da datacrazia e dromocrazia, dovrebbero sentire il dovere di un'apertura alla terzietà e all'universalità della ratio iuris, non unicamente per l'individuazione di nuovi diritti fondamentali, ma per non rischiare che lo spazio proprio dell'autonomia del diritto venga di fatto occupato da sedicenti algoritmi che, in realtà, nascondono la vecchia ambizione di dominio, tipica dell'assolutizzazione del potere 'oligarchico'"[41], il che può creare nuove forme di vulnerabilità e potenziare quelle esistenti[42].

Quale approccio si potrebbe seguire, dunque, per un ripensamento del diritto alla privacy e del diritto alla protezione dei dati personali? Appare chiaro che, in un villaggio globale in cui coesistono poteri diversi e i dati viaggiano in flussi sostanzialmente incontrollabili, la pretesa di un controllo effettivo paia irrealizzabile concretamente anche in ragione della complessità dei sistemi che trattano proprio i dati personali. Non si può, tuttavia, rifuggire dal porlo, quanto meno, come un obiettivo. Come trovare un bilanciamento

[39] Cfr., fra gli altri, Amato Mangiameli 2019; Fioriglio, 2015; Floridi – Taddeo 2016. Per una mappatura, cfr. Mittelstadt et al. 2016, nonché Tsamados et al., 2021.
[40] Floridi et al. 2017, 699.
[41] Avitabile 2019, 325.
[42] Sulla vulnerabilità nel cyberspazio cfr., fra gli altri, Brighi 2017.

che conduca a una strada percorribile che venga tracciata mediante una normativa valida ed efficace?

Per tentare di contribuire a fornire una risposta a una domanda tanto difficoltosa, cui difficilmente si potrà rispondere in modo univoco e "stabile" (stante l'incessante evoluzione tecnologica), sembra opportuno partire dal problema dei limiti che potrebbero essere imposti alla ricerca e del suo utilizzo nella fornitura di prodotti e servizi. Del resto, "la storia ci mostra la impossibilità o anche la inutilità di limitare la ricerca, ma ci mostra anche la necessità di aver chiara la differenza tra libertà della ricerca e utilizzo di strumenti ai fini della ricerca. Ci mostra l'importanza di una libertà della ricerca correlata ai fini che essa si pone. Ci mostra la necessità di distinguere tra ricerca e utilizzo delle sue scoperte o invenzioni"[43]; in tal senso, la logica della *privacy by design* e della *privacy by default* è un importante punto di partenza, che necessita però di una reale implementazione concreta. È questo, forse, un corto circuito della normativa vigente, che si basa sostanzialmente sull'*accountability* di titolare e responsabile, nonché sull'eventualità di un controllo successivo ad opera delle relative autorità: la complessità dei sistemi che effettivamente trattano su larga scala i dati, personali e non, comporta purtroppo elevatissimi rischi di elusione o violazione della normativa, in quanto diviene praticamente impossibile controllare effettivamente quanto avvenga nei sistemi medesimi.

Questa impossibilità pratica è dovuta al concorso mutevole di diversi fattori, fra cui giocano un ruolo primario la territorialità, gli oneri e la normativa sulla proprietà intellettuale. In modo molto succinto, può qui osservarsi che la prima impatta sulla giurisdizione delle autorità nonché sulla stessa possibilità di azione degli eventuali interessati; i secondi sono relativi alle risorse umane e patrimoniali necessarie per poter verificare sistemi normalmente distribuiti e molto complessi; la terza costituisce un ostacolo alla conoscibilità dei codici informatici che eseguono gli algoritmi e che elaborano realmente i dati personali, anche in relazione ai relativi spazi di archiviazione.

L'odierna tecno-regolazione[44], però, è oggi inidonea a orientare concretamente il percorso dell'intelligenza artificiale verso una società in cui gli algoritmi non siano al di sopra della legge: ma, a ben vedere, essi sono lo strumento che consentono ciò a quei soggetti che creano, controllano e adoperano proprio tali algoritmi su scala globale.

Queste brevi considerazioni evidenziano come la risposta di ciascuno Stato non possa essere né isolata né relativa unicamente all'ambito della

[43] Serra 2003, 135.

[44] Cfr. Amato Mangiameli 2017, nonché Lettieri 2020.

privacy[45], in quanto investe la più ampia galassia dei sistemi informatici su cui viene metaforicamente "eseguita" la Società algoritmica. In tal senso, può guardarsi con favore ad alcune scelte di politica legislativa effettuate nell'Unione europea, come quelle consistenti nella regolamentazione di ampi settori attraverso lo strumento del regolamento. Basti pensare, così, al più volte citato GDPR, ma altresì al regolamento n. 910/2014, eIDAS (electronic IDentification Authentication and Signature), nonché alle proposte di regolamentazione del mercato unico sui servizi digitali – COM/2020/825 final – e sull'intelligenza artificiale – COM/2021/206 final.

L'ambito della salute, in questo contesto più generale, appare però delicatissimo: è, come si è visto, al crocevia fra il pubblico e il privato, fra il rapporto medico/paziente e utente/dispositivo o servizio, fra la territorialità e la globalità della Società dell'informazione. Un eccesso di attenzione verso il solo profilo della protezione dei dati personali rischia, oltretutto, di accentuare la tendenza al dataismo, cui si è accennato.

In ogni caso, è necessario un cambio di passo da parte dei legislatori, in quanto anche normative quali il GDPR e le sopracitate proposte di regolamento (ove dovessero poi concretizzarsi) sono certamente tardive, come dimostra l'attuale configurazione del mercato, e richiedono di riflettere su un approccio "cucito su misura" sulle nuove tecnologie oltre che sulla comprensione delle esigenze di regolamentazione che sorgono in un'epoca così rivoluzionaria[46]. Inoltre, senza strumenti effettivi di controllo sul software realmente eseguito e sui dati realmente trattati, queste normative rischiano comunque di essere inefficaci ancorché formalmente valide, e oltretutto sarebbe necessario potenziare notevolmente gli strumenti che consentano a ciascun interessato di reagire rapidamente, anche mediante piattaforme telematiche: in caso contrario, continueranno a realizzarsi non solo macro-lesioni del diritto alla privacy e alla protezione dei dati personali, ma infinite micro-lesioni che rimangono e che rimarranno impunite poiché la relativa tutela sarebbe troppo onerosa, soprattutto in termini di tempo, per ciascun interessato.

[45] In riferimento a una più ampia considerazione del diritto alla salute cfr. in particolare Botrugno 2021.

[46] Oltretutto, e in una linea di riflessione più generale, "Diventano sempre più labili le linee di demarcazione tra naturale e artificiale, soggetto e oggetto, organico e inorganico, vita e morte. In fondo un essere umano è composto da 59 elementi: carbonio, idrogeno, ossigeno, azoto, calcio, fosforo e poi ancora un po' di molibdeno, vanadio, manganese, stagno, rame, cobalto, cromo 15. In che cosa saremmo allora diversi da Giove? Se la chimica ha prodotto la vita, perché il silicio non potrebbe produrre il pensiero? Queste domande sono esasperazioni concettuali, provocazioni o prospettive di ricerca? Un po' l'uno e un po' l'altro. Non sappiamo cosa ci riserva il futuro, ma certamente molte, troppe cose devono cambiare all'interno delle tradizionali categorie giuridiche" (Amato 2020, 7).

Bibliografia

Amato Mangiameli, A.C. (2017). *Tecno*-diritto e *tecno*-regolazione. Spunti di riflessione. *Rivista di filosofia del diritto,* speciale, 87-112.

(2019). Algoritmi e big data. Dalla carta sulla robotica. *Rivista di filosofia del diritto,* 1, 122-123.

Amato, S. (2020). *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino.

Andronico, A., Casadei, Th. (2021). "Introduzione. Algoritmi ed esperienza giuridica". *Ars interpretandi*, 1, 7-11.

Avitabile, L. (2017). Il diritto davanti all'algoritmo. *Rivista italiana per le scienze giuridiche*, 8, 313-325.

Balkin, J. (2017). "The Three Laws of Robotics in the Age of Big Data". *Ohio State Law Journal*, 78(5), 1217-1241.

Barfield, W., edited by (2020). *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, Cambridge.

Botrugno, C. (2021). "Information and Communication Technologies in Healthcare: A New Geography of Right to Health". *Rivista di filosofia del diritto*, 2021, 1, 163-188.

Brighi, R. (2017). La vulnerabilità nel cyberspazio. *Ars interpretandi*, 1, 81-94.

Cannataci, J., Falce, V., Pollicino, O., edited by (2020). *Legal Challenges of Big Data*. Edward Elgar, Cheltenham.

Casadei, Th., Pietropaoli, S. (2021). "Intelligenza artificiale: fine o confine del diritto?". *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali* (a cura di Th. Casadei, S. Pietropaoli), Wolters Kluwer, Milano, 219-232.

Comitato Nazionale per la Bioetica (2015). *"Mobile-health" e applicazioni per la salute: aspetti bioetici*. Roma.

Di Giandomenico A., Fioriglio, G. (2020). "Le prospettive della medicina di precisione e della medicina delle "scatole nere" fra bioetica e diritto, dentro e oltre l'Europa". P. Tincani (a cura di), *Diritto e futuro dell'Europa Contributi per gli workshop del XXXI Congresso della Società Italiana di Filosofia del Diritto* (Bergamo, 13-15 settembre 2018), L'Ornitorinco, Milano, 207-212.

Faini, F. (2019). *Data society. Governo dei dati e tutela nell'era digitale*. Giuffrè Francis Lefebvre, Milano.

Fioriglio, G. (2015). "Freedom, Authority and knowledge on line: the dictatorship of the algorithm". *Revista Internacional de Pensamiento Politico*, 10, 395-410.

(2020). *Informatica medica e diritto. Un'introduzione*. Mucchi, Modena.

(2021). "La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici". *Ars interpretandi*, 2021, 1, 53-67.

Floridi, L., Cowls, J., Beltrametti M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., Vayena, E. (2018). "AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations". *Minds and Machines*, 28, 689-707.

Floridi, L., Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A*.

Gorgoni, G. (2020). "Stay Human. The quest for Responsibility in the Algorithmic Society". *Journal of Ethics and Legal Technologies*, 2020, 2, pp. 31-47.

Häberle, P. (2010). *Diritto e verità*, tr. it.. Einaudi, Torino.

Lagioia, F., Contissa, G. (2020), "The Strange Case of Dr. Watson: Liability Implications of AI Evidence-Based Decision Support Systems in Health Care". *European Journal of Legal Studies*, 2, 245-289.

Lettieri, N. (2020). *Antigone e gli algoritmi. Appunti per un approccio giusfilosofico*. Mucchi, Modena.

Mayer-Schönberger, V., Cukier K. (2017). *Big Data. The Essential Guide to Work, Life and Learning in the Age of Insight*, New and expanded ed., John Murray, London.

Mittelstadt, B.T., Allo, P., Taddeo, M., Wachter, S., Floridi, L. (2016). "The ethics of algorithms. Mapping the debate". *Big Data & Society*, 1-21.

Pagallo, U. (2020) Algoritmi e conoscibilità. *Rivista di Filosofia del diritto*, 2020, 1, 93-106.

Palazzani, L. (2017). *Dalla bio-etica alla tecno-etica: nuove sfide al diritto*, Giappichelli, Torino.

(2020). *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*. Studium, Roma.

Pasquale F. (2015). *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge.

(2017). "Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society". *Ohio State Law Journal*, 78, 1243-1255.

Pastore, B. (2021). *Semantica della vulnerabilità, soggetto, cultura giuridica*. Giappichelli, Torino.

Pizzetti, F. (2021). *Protezione dei dati personali in Italia tra GDPR e codice novellato*. Giappichelli, Torino.

Riccio, G.M., Belisario, E., Scorza, G. (2018), a cura di. *GDPR e normativa privacy, Commentario*. Wolters-Kluwer, Milano.

Rodotà, S. (2012). *Il diritto di avere diritti*. Laterza, Roma-Bari.

Russell S., Norvig, P. (2021). *Artificial Intelligence. A Modern Approach*, 4th edition, Pearson, London.

Sadin, E. (2019). *Critica della Ragione Artificiale. Una difesa dell'umanità*, tr. it. LUISS University Press, Roma.

Salardi, S. (2021). "La dimensione semantica delle macchine intelligenti". *Notizie di Politeia*, 143, 156-161.

Sartor, G. (2003). Gli agenti software e la disciplina giuridica degli strumenti cognitivi. *Il diritto dell'informazione e dell'informatica*, (19)1, 55-87.

(2020). Introduzione. *Rivista di filosofia del diritto*, IX(1), 65-72.

Scagliarini, S., a cura di (2019a). *Il "nuovo" codice in materia di protezione dei dati personali. La normativa italiana dopo il d. lgs. 101/2018*. Giappichelli, Torino.

a cura di (2019b), *Smart roads e driverless cars: tra diritto, tecnologie, etica pubblica*. Giappichelli, Torino.

Serra, T. (2003). *L'uomo programmato*. Giappichelli, Torino.

Schuilenburg, M., Peeters, R., edited by (2021). *The Algorithmic Society. Technology, Power, and Knowledge*. Routledge, Abingdon-on-Thames.

Solove, D.J. (2021). "The Myth of the Privacy Paradox". *George Washington Law Review*, 1, 1-51.

Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Roberts, H., Taddeo, M., Floridi, L. (2021). The ethics of algorithms: key problems and solutions. *AI & Society*.

Vermaas P., Kroes, P., van de Poel, I., Franssen, M., Houkes, W. (2011) "A Philosophy of Technology: From Technical Artefacts to Sociotechnical Systems". *Synthesis Lectures on Engineers, Technology, and Society*, 6, 1-134.

Warren, S.D., Brandeis, L.D. (1890). "The right to privacy, in Harvard Law Review, 1890, 4, pp. 193-220.

Zanetti, Gf. (2019). *Filosofia della vulnerabilità. Percezione, discriminazione, diritto*. Carocci, Roma.