RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0131 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Simone Calzolaio

Vulnerabilità della società digitale e ordinamento costituzionale dei dati

La fine delle prospettive utopiche connesse all'avvento della rete Internet ha lasciato sul campo molteplici esigenze di regolazione, che si colgono osservando empiricamente le vulnerabilità che caratterizzano la persona ed il sistema democratico nella società digitale. In tale contesto, uno degli aspetti che rende più fragile e rischiosamente frammentato l'ordinamento giuridico di fronte alla evoluzione digitale consiste nella difficoltà di individuare in modo sistematico i caratteri emergenti del processo di datificazione. In questo contributo si tenta di identificare alcune caratteristiche ricorrenti dell'ordinamento dei dati e di verificare la possibilità, nell'ambito del sistema costituzionale dei valori e delle libertà, di continuare a garantire il primato della tutela della persona umana e del contesto sociale in cui si svolge la sua personalità, pur di fronte a nuove sfide epocali.

Internet – Ordinamento costituzionale – Ordinamento dei dati – Dati sintetici – Connessione sociale

The digital society vulnerabilities and constitutional data legal system

The end of the utopian perspectives connected to the advent of the Internet has left multiple needs in the field of regulation, which are captured by empirically observing the vulnerabilities that characterize the person and the democracy system in the digital society. Faced with digital evolution, the legal system needs to identify a legal data system that clarifies the characteristics of datafication and avoids the danger of legal fragmentation. In this contribution we attempt to identify some recurring characteristics of data system and to verify the possibility, within the constitutional system of values and freedoms, to continue to guarantee the primacy of the protection of the human person and the social context in which his personality unfolds, despite facing new epochal challenges.

Internet – Constitutional law – Data law – Synthetic data - Social connection

L'Autore è professore associato di Diritto costituzionale presso l'Università degli Studi di Macerata

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

"Addio", disse la volpe. "Ecco il mio segreto.
È molto semplice: non si vede bene che col cuore. L'essenziale è invisibile agli occhi".
"L'essenziale è invisibile agli occhi", ripeté il piccolo principe, per ricordarselo.
"È il tempo che tu hai perduto per la tua rosa che ha fatto la tua rosa così importante".

(Antoine de Saint-Exupéry, Il piccolo principe)

1. Oggetto del contributo

Scopo di questo lavoro – che prende spunto dal convegno ICON•S di Bologna su *Il Futuro dello Stato*[1] e dal panel che si è avuto l'opportunità di co-organizzare[2] – è contribuire a:

1) descrivere le vulnerabilità che l'avvento della società digitale sta mostrando in pressoché tutti gli ordinamenti costituzionali liberaldemocratici;
2) individuare alcuni punti fermi che l'analisi giuridica della società digitale, come società dei dati, evidenzia e che sono aspetti nodali per qualunque costruzione giuridica e regolatoria: si tratta dei primi aspetti di un ordinamento costituzionale dei dati (non più solo dei dati personali);
3) provare a identificare spunti di approfondimento che si scorgono come più pressanti all'orizzonte e che mettono alla prova la *vitalità* della nostra Costituzione e dell'ordinamento costituzionale italiano[3] ed europeo su aspetti classici del costituzionalismo liberaldemocratico.

2. Dall'utopia alle vulnerabilità: l'esigenza di un ordinamento costituzionale dei dati

Poco dopo la caduta del muro di Berlino e la sofferta – ma pacifica – conclusione della grande utopia del socialismo reale del secondo Novecento, v'era un clima euforico[4] nel mondo occidentale e nel rinato mondo orientale. Proprio agli albori di quella che si sarebbe chiamata "globalizzazione" faceva il suo ingresso nella storia una nuova rete: "Internet", nata per garantire le comunicazioni nel caso in cui la guerra fredda si fosse improvvisamente surriscaldata, finiva per venire divulgata

1. V. il sito del Convegno ICONS•S.
2. … sempre grazie alla cordialità degli organizzatori di ICON•S e alla vivacità intellettuale di colleghe e colleghi: v. il programma del Convegno.
3. Per ordinamento costituzionale intendiamo – come si vedrà – quanto autorevolmente individuato da Barbera 2010.
4. Si veda ancora oggi, ad esempio, Ash 2023, il quale descrive il periodo 1990-2007 della storia europea con il significativo titolo "Il trionfo". Qualcuno era meno utopico degli altri, qualcuno aveva intuito che il crollo del muro di Berlino avrebbe indotto, in Italia in particolare, altri crolli: cfr. Cossiga-Chessa 2007.

in tempo di pace come strumento di connessione mondiale, di collaborazione, di partecipazione da una parte all'altra del globo, da ovest ad est[5].

Un ottimismo utopico ha accolto l'avvento di Internet[6]: un ulteriore lascito della democrazia americana, che sembrava destinata a far crollare l'uno dopo l'altro tutti i muri che separavano gli esseri umani: libertà dell'est Europa (e dalla paura di una guerra nucleare), libertà dei commerci mondiali e con l'est del mondo, libertà di comunicazione e di informazione globale senza (possibilità di) censure, senza costi, per tutti.

Non tutti lo ricordano, ma alla base della tuttora vigente regola statunitense sulla responsabilità degli Internet service provider[7] – una regola materialmente costituzionale – vi era esattamente questo sentimento di ineluttabilità delle magnifiche sorti e progressive dell'umanità, che grazie al libero sviluppo di questa nuova tecnologia, e alla libera intelligenza collettiva che ne scaturiva, avrebbe trovato – attraverso la regia/supremazia americana[8] – progressivamente soluzione a tutti i suoi problemi.

In principio era Internet e lo immaginavamo diverso[9], in sintesi.

In quella prima fase, a farne le spese in ambito giuridico, furono principalmente il diritto della proprietà intellettuale, il diritto d'autore e la protezione dei dati personali.

Poi la Rete si è evoluta: l'avvento della banda larga, con lo sviluppo dei connessi servizi digitali, il web 2.0 interattivo, i servizi di messaggistica istantanea, l'i-phone e poi gli smartphone, i social media, la digitalizzazione pubblica, i motori – e poi, il motore – di ricerca e le piattaforme digitali, l'IOT, il cloud computing. Infine, quell'oggetto ancora largamente inesplorato e ignoto che chiamiamo convenzionalmente intelligenza artificiale.

Nel corso dell'ultimo decennio, accanto al progresso fulminante abbiamo cominciato a scorgere gli effetti, le incognite, i mutamenti indotti dalla evoluzione tecnologica (Pasquale, Cohen, Zuboff). L'ottimismo si è mutato in un più semplice arrendersi al dinamismo indotto dall'inesauribile sviluppo tecnologico. Distolto lo sguardo dal sole accecante dell'utopia, si intravedono ora i rischi (i danni, talvolta), le nuove divisioni sociali e geopolitiche, il ritorno di antichi poteri[10] per affrontare le vulnerabilità delle società (digitali)

5. Cfr. Elmer-Dewitt 1993; v. più di recente Amenta 2015.
6. … che doveva essere uno spazio statuale libero e libertario: «We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before», così Barlow 1996.
7. Come osserva Finocchiaro 2022, p. 815: «Gli Stati Uniti con il Communications Decency Act del 1996 [n.d.a., sez. 230: "Nessun provider o utente di un servizio informatico interattivo deve essere trattato come editore o creatore di qualsiasi informazione fornita da un altro provider di contenuti informativi"] e poi l'Europa con la Direttiva 2000/31/CE sul commercio elettronico statuirono una sostanziale esenzione di responsabilità del provider. Si era in un'epoca completamente diversa: eravamo all'inizio della diffusione del web e quindi occorreva lasciare che la comunicazione digitale seguisse il suo corso espansivo, senza onerarla di costi che inevitabilmente sarebbero stati riversati sugli utenti. Naturalmente questa è solo una delle prospettive di lettura – se ne potrebbero aggiungere molte altre – ma è probabilmente quella più accreditata dal punto di vista funzionale ed economico». V. anche Riccio 2002, p. 171 ss., in merito al DMCA (*Digital Millenium Copyright Act*) e al OCILLA (*Online Copyright Infringement Liability Limitation Act*).
8. … altra più recente grande disciplina – questa sì, materialmente costituzionale e intrinsecamente volta a rivendicare una forma di supremazia globale – è il CLOUD Act statunitense (acronimo che sta per *Clarifying Lawful Overseas Use of Data Act*), su cui, davvero interessante: Boncinelli 2021, spec. p. 36 ss.
9. Così Scorza 2022, p. 23 ss.
10. Davvero interessante: Morrone 2023, il quale giustamente si domanda – come pure faremo qui naturalmente – «La domanda vera, allora, non riguarda il "ritorno dello Stato" ma è: "quale Stato ritorna oggi?"» (p. 270) e poi sviluppa, anche in riferimento al governo del digitale, la tesi e l'auspicio della ri-politicizzazione dello Stato.

contemporanee[11]: «nessuno crede più alla retorica dello spazio digitale come luogo della libertà»[12].

Sta di fatto che ormai assistiamo al blocco sistematico e ricorrente, da parte di Stati (di norma autoritari), della rete Internet per evitare le comunicazioni e l'informazione delle persone in vista di avvenimenti importanti o di rilievo sociale[13] o per sedare rivolte o per placare gli animi social: l'ultimo caso è quello delle elezioni pakistane[14], ma altrettanto avviene in Israele e in Palestina, e in molte altre parti del mondo. Lo Stato, il potere nega internet alla sua gente[15] per affermare la sua supremazia (spesso autoritaria).

Ma altrettanto spesso, in diverse aree del mondo, quando lo Stato non nega (all'interno dei suoi confini) la Rete è perché si tratta di uno strumento inarrivabile per misurare, controllare, sorvegliare le persone: è il caso del *social scoring* cinese[16]. Che non è così isolato e lontano come vorremmo credere[17], ad esempio nel caso dell'ormai diffuso *credit scoring*[18]. Basta fare esperienza dei software di registro elettronico in uso presso le scuole pubbliche, per capire come sotto le specie della "trasparenza informativa" e della collaborazione scuola-famiglia, la dimensione digitale insinui quasi spontaneamente una forma pervasiva di "sorveglianza", e come questi modelli rischino di schiacciare i più deboli fra gli studenti (e fra i professori), in una apparente oggettivizzazione e, appunto, datificazione (intesa come riduzione alle informazioni che derivano dai dati) della vita scolastica. Eppure, anche questa è la rete Internet e non v'è nulla di più popolare fra genitori (ansiogeni) e professori (intimoriti e distanti) del controllo sistematico e immediato dei propri figli e studenti da remoto: liberi, ma mai di agire inosservati. Cioè: sorvegliati.

Ma pensiamo ancora alle capacità dei *Large Language Models* (LLM), all'intelligenza artificiale cd. generativa, che apprendono dalla rete (*web-scraping*[19] e altre modalità) e da altri data set e sono in grado di scrivere questo articolo[20] in

11. Questo rovesciamento dell'utopia, si sostanzia nella ritenuta progressiva frammentazione della rete Internet, in una molteplicità di reti nazionali e sovranazionali, in zone di influenza geopolitica, in piccoli spazi privati: cfr. Lemley 2021.
12. Bergonzini 2023, p. 99.
13. L'Internet society monitora il blocco di Internet nelle varie nazioni del mondo e le sue motivazioni. È una strana cartina geografica del mondo, che vale la pena osservare.
14. Cfr. Zorloni 2024.
15. Cfr. De Gregorio-Stremlau 2020, i quali ragionevolmente osservano: «we do not deny that Internet shutdowns constitute a highly intrusive form of censorship, there are reasons when these practices could be justified. This is not, in any way, to endorse or condone such actions, but we argue that in the context of a rising tide of incitement to violence on social media platforms (and an apparent inability of social media actors to curb such speech) there needs to be a more nuanced and transparent conversation about why some governments are taking the seemingly extreme actions they are, how they can be limited, or when they might be justified, and how concerns about widespread hate online can be better brought into debates around the protection of human rights».
16. Cfr. Cheung-Chen 2022; sul tema più generale del riconoscimento facciale, v. Mobilio 2021.
17. Cfr. Citino 2023, la quale riporta il famoso caso olandese Syri, ma altresì casi di *social scoring* sviluppati da istituzioni territoriali: non sono sempre e solo gli Stati ad adottare politiche di tal fatta, che peraltro in alcuni casi potrebbero perfino essere ragionevoli e utili, o comunque motivabili adeguatamente.
18. Si veda la recentissima CGUE, sentenza 7 dicembre 2023 in C-634/21, secondo cui l'attività di *credit scoring* può costituire un "processo decisionale automatizzato" ai sensi del GDPR laddove da tale punteggio dipenda, in modo decisivo, la stipula, l'esecuzione o la cessazione di un rapporto contrattuale tra l'interessato ed il soggetto terzo al quale è comunicato il predetto *score* probabilistico.
19. Cfr. Lobel 2021, spec. p. 185 ss.
20. Lo aveva capito prima, perché l'intelligenza è innanzitutto un dono, Caravita 2020, p. 470, par. 8, intitolato proprio "Questo testo non è stato scritto da una macchina di intelligenza artificiale, ma un domani…?". Quel domani è arrivato presto.

modo più puntuale, specifico, brillante, dotto, e soprattutto veloce e senza costi, di un misero e costoso essere umano, riproducendo tuttavia la visione, il modo di scrivere e di *interpretare* insito nelle modalità di apprendimento del sistema (è il caso *New York Times vs. ChatGpt*[21]), che altro non è poi che la vecchia tirannia della maggioranza (istituzionalizzata, in questo caso, dal design della tecnologia), di cui parlava un francese in viaggio negli States[22]. In genere, quando si ricorre a questo esempio la mente scorre verso il problema della sostituzione delle macchine ai colletti bianchi, ai professionisti, ai professori, ai giudici, ai medici, oltre che dei robot agli operai ed agli agricoltori. In realtà, è opportuno domandarsi[23]: quali capacità stiamo perdendo se non siamo più costretti a scrivere, ad apprendere questa o quella abilità seguendo una disciplina, e spesso qualcuno che ce la insegni, poiché c'è chi lo fa per noi, e meglio di noi, senza di noi? Come distingueremo un volto umano da un volto umano sintetico? Non si tratta di essere romantici, ma di affrontare il tema della libera formazione della personalità e, quindi, della libertà di formazione del pensiero[24] dopo l'avvento della società digitale.

Infine: la rete Internet, i suoi fantastici servizi gratuiti, le auto e le bici connesse con gli smartphone connessi con la domotica connessa e con gli acquisti online e il cibo a casa, con un bel libro digitale e la tv-online. Il problema della *iper-connessione* e della sua incidenza sulle relazioni sociali, sulla formazione dei minori, sulla edificazione del sistema dell'informazione e infine sulla impercettibile ma costante perdita di libertà cognitiva attraverso l'ineluttabile *engagement* con questo o quel social, app, game, di cui – solo per oggi – non possiamo fare a meno. Ormai la vita è digitale, senza una vera cittadinanza digitale[25], e con molte invisibili nuove forme di dipendenza, compresa la difficoltà pratica ed emotiva di disconnettersi dal lavoro[26].

Tutto questo significa che siamo perduti? No.

Il progresso indotto dalla società digitale è evidente e lo si potrebbe descrivere ancor più analiticamente di quanto non si siano – senza possibilità di essere esaustivi – descritte le vulnerabilità più marcate.

Peraltro, si sono tralasciati i temi posti dalle *big tech* private, dalle piattaforme digitali e l'altro grande tema delle libertà politiche e dei processi democratici, ma solo perché sono vicine alla tradizionale sensibilità costituzionalistica e già approfonditamente considerate[27].

Si è trattato però di lasciare sin qui emergere un po' brutalmente l'evidenza che l'utopia di Internet è ormai un ricordo e, ora, è necessario fare i conti con la datificazione e con le esigenze di governo dei dati, da cui dipende largamente la sopravvivenza e l'evoluzione del tessuto costituzionale e, con esso, delle democrazie[28].

Cerchiamo quindi di procedere ad individuare i caratteri di base dell'ordinamento costituzionale

21. Qui un atto giuridico di sicuro rilievo, l'atto di citazione del NYT a GPT e Microsoft. Ma l'aspetto interessante è che le modalità di addestramento della LLM non possono che tendere a rappresentare e riprodurre la mentalità – il capitale semantico, direbbe forse Floridi, cfr. Floridi 2018 – derivante dai dati con cui il LLM è addestrato: per intenderci, se i dati derivano dal principale quotidiano newyorkese, principalmente WASP. Pertanto, il rischio che la LLM diventi uno strumento di influenza culturale subliminale è reale, anche se gli studi più recenti di Microsoft ci dicono: a) che la IA generativa funziona meglio con "piccoli dati", cioè dati settoriali di qualità, come i classici manuali: cfr. Gunasekar et al. 2023; b) che la IA generativa può essere addestrata a dimenticare, a disapprendere quanto appreso, e quindi l'addestramento può diluire i pregiudizi di mentalità, gli eventuali danni generati, e può rispettare la proprietà intellettuale: cfr. Eldan-Russinovich 2023.
22. De Tocqueville 2005.
23. Freuler 2023.
24. Indispensabile la lettura di Richards 2015, e volendo Calzolaio 2018, pp. 366-369.
25. Ma v. su questo Costantino 2023.
26. Cuomo 2023.
27. Cfr., rispettivamente, Bergonzini 2023, Caruso 2023, Di Cosimo 2023, Manetti 2023.
28. Cfr. Manetti 2020.

dei dati[29] – procedendo nell'indagine si darà ragione dell'utilizzo dei tre termini (ordinamento, costituzionale, dati) –.

3. Alcuni punti fermi: dalla *data driven innovation* alla *data dependency*

In piena pandemia[30] fu semplice accorgersi del fatto che si era realizzato un passaggio netto in quegli anni: l'ottimismo intrinseco nell'idea retorica dell'intelligenza collettiva di Internet aveva una propaggine rilevante nella dimensione concettuale della *data-driven innovation*[31]. Tuttavia, quella fase è superata: ormai la dimensione di raccolta, disponibilità, sfruttamento, messa a disposizione, condivisione dei dati è coessenziale per garantire la vita ordinaria delle società contemporanee. L'innovazione passa per lo sfruttamento dei dati perché dipendiamo dai dati in tutti gli aspetti della nostra vita (compresa l'innovazione tecnologica).

Tre esempi. Abbiamo accennato alle ipotesi di *Internet shutdown*. Possiamo chiederci: come avrebbero agito gli stessi poteri pubblici che hanno bloccato Internet, 30 anni fa? Avrebbero censurato la radiotv e la stampa, vietato le manifestazioni, represso il dissenso con la forza. Può darsi lo facciano anche ora – ma è più semplice rimuovere la leva che aggrega e motiva le persone: bloccare Internet, bloccare la comunicazione, bloccare la diffusione di notizie, cioè bloccare la circolazione dei dati in particolare attraverso i social media, incide sulle modalità ordinarie con cui le persone ormai comunicano fra loro e acquisiscono informazioni e notizie. Le persone dipendono dalla circolazione dei dati e delle informazioni attraverso la Rete e i social media. Si tratta di una questione di diritto costituzionale.

Il Governo Conte I, con una certa disinvoltura (ma non isolatamente a livello europeo), stava concretamente vagliando, per il tramite di un membro del Governo vicino al governo cinese, la possibilità di affidare la costituzione della rete 5G a un noto operatore cinese[32]. In via ufficiale, l'ambasciata statunitense affermò che la Nato e gli Stati Uniti avrebbero, in tal caso, limitato la condivisione di informazioni con l'Italia[33]. Pochi mesi più tardi la vicenda assunse tutt'altra piega[34] e, come noto, poi l'esperienza di quel governo si concluse (il 4 settembre 2019). Le infrastrutture materiali e immateriali attinenti alla circolazione dei dati rappresentano una questione dirimente di interesse e sicurezza nazionale e di collocazione geopolitica. Gli Stati dipendono dalla circolazione dei dati e delle informazioni attraverso la rete Internet e dalle relative infrastrutture. Si tratta di una questione di diritto costituzionale[35].

Immaginiamo di privare un adolescente infratredicenne della possibilità di frequentare la sua comunità di pari con gli strumenti digitali che questa (lecitamente) utilizza: messagistica istantanea, social media, giochi online, Internet tv, ecc. Questo adolescente, di norma, avvertirà un senso percepibile di esclusione e di segregazione, molto simile a quello di un adolescente che fino agli anni Duemila fosse stato impedito stabilmente di frequentare personalmente la stessa comunità di suoi pari. La formazione della personalità passa attraverso gli strumenti che la contemporaneità offre e fra questi – seppure, come vedremo, rischiosissimi – ci sono gli strumenti digitali: un adolescente di oggi che ne fosse (totalmente e permanentemente) escluso, ne sarebbe menomato. Ma questo, se ci osserviamo un istante, vale per tutti noi.

29. Vi è una connessione fra l'identificazione di questi caratteri dell'ordinamento dei dati e la qualificazione privatistica della titolarità dei dati: cfr. Marinotti 2022.
30. Si veda Calzolaio 2021a.
31. Si veda a questo riguardo la descrizione di questo aspetto, volendo, in Calzolaio 2017, spec. p. 602, con relativi riferimenti.
32. Cfr. Bechis-Mieli 2019.
33. Cfr. Pierri 2019.
34. … con l'adozione di indirizzi governativi che di fatto rendevano impossibile la partecipazione delle aziende cinesi: cfr. Arnese-Walsingham 2020; ora il Piano Italia 5G è confluito nel PNRR, ma non sembra stia avanzando con sufficiente rapidità.
35. Su questo aspetto, v. Salerno 2018, spec. p. 765 ss.

La formazione e lo sviluppo delle nostre personalità sono incisi dalla presenza e dal rilievo dei servizi digitali che si alimentano sistematicamente di dati: la dipendenza dai dati che è una caratteristica propria delle macchine (*data dependency*[36]), si risolve ormai nella nostra dipendenza dalle macchine e quindi dallo sfruttamento dei dati in nostro favore (*data dependencies*).

Le persone dipendono dalla circolazione di dati e informazioni per l'ordinario svolgimento della propria personalità, sia come singoli, sia nelle formazioni sociali. Le implicazioni costituzionali di questa osservazione sono molteplici e rappresentano il passaggio dall'irenica – si direbbe[37] – *data-driven innovation*, alla ben più stringente dipendenza sistematica e strutturale dalla datificazione. Si tratta di una questione di diritto costituzionale[38].

Gli esempi potrebbero moltiplicarsi: ma se questa è la descrizione del contesto, si comprende perché è giuridicamente necessario rinvenire un ordine nel sistema della datificazione[39] e, progressivamente, un ordinamento costituzionale dei dati.

4. Dati e informazioni[40]

La seconda osservazione descrittiva è che esiste una grande differenza oggettiva – non sempre adeguatamente colta né dal legislatore, né dagli osservatori[41] – fra dati e informazioni.

Procediamo ancora con esempi, per introdurci al tema.

E partiamo dalla Cina[42]. Nel 2021 il legislatore cinese ha adottato due leggi molto significative: la c.d. "Data security law" (di seguito, DSL) e la c.d. "Personal information protection law" (di seguito, PIPL)[43]. Leggendo le rispettive disposizioni di legge, sembra di poter affermare che il legislatore cinese ha voluto distinguere, in modo necessariamente non casuale, tra "informazioni" (PIPL) e "dati" (DSL), e su queste due distinte nozioni ha costruito i due corpi normativi.

Si potrebbe presumere che ciò che conta, ai fini del PIPL, sia l'aspetto funzionale – l'informazione – più che il profilo strutturale – i dati –, poiché l'interesse primario del PIPL è quello di proteggere i diritti e gli interessi delle persone fisiche (artt. 1 e 3). Al contrario, quando l'interesse principale è l'interesse pubblico (la sicurezza dello Stato, che – va notato – include anche «i legittimi diritti e interessi di individui o organizzazioni», come specificato nell'art. 21 DSL), allora emerge la prospettiva della sovranità digitale dello Stato, che si basa sul riferimento alla nozione di "dati", indipendentemente dalle informazioni che incorporano. I dati intesi come entità fisica sono e devono essere sotto il controllo dello Stato (ubicazione, disponibilità, conservazione, utilizzo).

Infatti, ai fini della tutela della privacy della persona, ciò che conta non sono i "dati" intesi come entità fisica, ovvero i dati informatici, ma l'uso che se ne può fare nel contesto sociale, e quindi il significato, le informazioni che il titolare/responsabile

36. Wenfei-Geerts 2012, p. 8: «Dependencies as data quality rules. A central question concerns how we can tell whether our data have semantic errors, i.e., whether the data are dirty or clean. To this end, we need data quality rules to detect semantic errors in our data, and better still, fix those errors by using the rules. But what data quality rules should we adopt? A natural idea is to use data dependencies (integrity constraints). Dependency theory is almost as old as relational databases themselves. Since Codd [1972] introduced functional dependencies, a variety of dependency languages, defined as various classes of first-order logic sentences, have been proposed and studied. There are good reasons to believe that dependencies should play an important role in data quality management systems. Indeed, dependencies specify a fundamental part of the semantics of data, in a declarative way, such that errors emerge as violations of the dependencies».
37. Cfr. Luciani 2006.
38. Barbera 1975.
39. Cfr. Durante-Pagallo 2022.
40. Cfr., acutamente e preliminarmente, Durante 2022.
41. Si veda il contributo fondamentale di Orlando 2022, p. 14 ss.; Finocchiaro 2012.
42. Si riprende qui quanto si è potuto osservare in Calzolaio 2023, p. 197 ss., cui si rinvia per più specifici riferimenti.
43. Le norme cinesi sono reperibili in https://digichina.stanford.edu/ (traduzione non ufficiale, ma affidabile).

del trattamento può o intende estrarre dai dati nell'ambito del trattamento effettuato.

In questo senso, la "informazione personale" corrisponde alla nozione europea di "dati personali" a seconda dell'uso che ne viene fatto[44]: ma ai fini della protezione personale, la nozione di "informazioni personali" è più utile di quella di "dati personali", poiché tende a declinare l'applicazione della disciplina in materia in considerazione dei caratteri del trattamento concretamente svolto dal titolare e, contemporaneamente, del rischio effettivo per l'interessato.

La questione si fa ancora più interessante – nel diritto cinese – perché il termine "informazione" viene abbandonato e sostituito dal concetto di "dato" quando entra in gioco l'interesse pubblico per la sicurezza e la sovranità digitale dello Stato.

In questo caso, infatti, lo Stato (cinese) intende tutelarsi proprio dalla possibilità che altri soggetti, anche altri Stati, possano avvalersi di mezzi computazionali che vanno oltre quanto prevedibile o ragionevole (in termini di tempi, costi, competenze professionali, numero di persone dedicate)[45] al fine di ricavare informazioni (strategiche) dai dati (informatici): le informazioni che uno Stato o una entità straniera possono ricavare dalla analisi dei dati "cinesi" possono infatti anche essere ulteriori e diverse da quelle di cui lo Stato cinese stesso è in possesso attraverso l'ordinario sfruttamento di quei dati.

In altri termini, l'utilizzo della nozione di "dato" al fine di proteggere gli interessi nazionali cinesi rappresenta una forma di principio di precauzione dalla estrazione di informazioni dai dati "cinesi", con tecnologie presenti o future non necessariamente conosciute dall'ordinamento cinese, svolta da soggetti estranei alla Cina e con tempi, modi, esiti che possono generare una asimmetria informativa fra Cina e soggetti stranieri. Le norme cinesi si concentrano sul "dato" perché il processo di *data mining*, sviluppato in modo non controllato dalle autorità nazionali cinesi, può condurre a informazioni inedite, imprevedibili e strategiche per (e contro) l'ordinamento cinese.

In questo caso, quindi, è più che comprensibile che la disciplina dello Stato tuteli i "dati", e non le "informazioni": si tratta di una forma di tutela anticipata del rischio[46], fondata su una valutazione assiologica (cinese) di carattere giuridico-costituzionale.

In conclusione, l'ordinamento dei dati cinese ci dimostra plasticamente il primo profilo della distinzione tra dati e informazioni (che peraltro è piuttosto familiare al costituzionalista che può ricorrere all'analogia con i concetti di disposizione e norma).

Ma un esempio ancora più interessante, e a me familiare[47], è stato rappresentato in un recente contributo, facendo leva su consolidati studi ed evidenze scientifiche. In sostanza, tutto il meccanismo tecnologico della blockchain, i suoi profili di sicurezza e di progressione dei blocchi, si basa sulla (dispendiosissima, sul piano strettamente energetico) capacità computazionale delle macchine, volta a decodificare dati sempre più complessi per raggiungere informazioni significative per la

44. Cfr. OECD 2014, pp. 14-16; Abrams 2014.

45. … quelli qui citati sono i criteri in base ai quali è possibile ritenere che dei dati sono stati anonimizzati (perdendo quindi l'attributo di "personali"): si tratta per l'appunto di un criterio di tipo stipulativo e non oggettivo. Cfr. considerando n. 26, GDPR: «Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato». Comunque sul tema v. sempre D'Acquisto-Naldi 2017 e volendo anche Calzolaio 2017, p. 605, ove si lega il tema alla previgente dir. 95/46/CE, cons. 26, ed alla intepretazione dei concetti di anonimizzazione e pseudonimizzazione dell'allora Gruppo art. 29.

46. Sul tema, ora, acutamente, Longo 2024; per connessione, v. anche Longo 2024a.

47. Autorevolmente: E-Calzolaio 2023. Il saggio affronta il tema della qualificazione dei dati come beni e del rapporto sussistente fra persona e dati, ma a tal fine sviluppa inizialmente una descrizione pregevole e chiarissima dei caratteri delle blockchain, che nel testo si è sintetizzata.

catena digitale e per i suoi utenti. Il passaggio fra dato e informazione, e l'intermediazione di una chiave, determina la sicurezza strutturale dell'informazione (conosciuta dal solo titolare della chiave), mentre il dato può circolare liberamente (poiché non può essere decodificato).

Questo esempio conferma la distinzione proposta fra dato e informazione, ma aggiunge un tassello importante: affinché il dato sia tradotto in informazione è necessaria – in ambiente digitale – l'intermediazione della macchina e della sua capacità computazionale (hardware e software).

Nel passaggio fra dato e informazione, quindi, c'è un consumo di energia, che pone – come nel caso della blockchain – un tema di sostenibilità ambientale della evoluzione digitale[48], almeno per quanto concerne il modello di sicurezza della blockchain.

Inoltre, il fatto dell'inevitabile intermediazione della macchina pone il problema del titolo di appartenenza del dato e dell'informazione alla persona, alla macchina (e al suo titolare, se la macchina non ha – come per ora non ha – soggettività giuridica) e al fornitore di servizi, delle relative responsabilità e della configurazione del rapporto giuridico intercorrente fra questi "soggetti", in modo che ancora non appare risolto[49].

Infine, passiamo alla più pedestre realtà della attuazione del PNRR e quindi del PSN (Polo strategico nazionale[50]), cioè del cloud nazionale dei dati: la localizzazione dei cloud è nazionale, la tecnologia di base è americana, la criptografia delle informazioni è sviluppata a livello nazionale a seconda della tipologia di dati e servizi coinvolti (ordinari, critici, strategici)[51]. Quindi, in ipotesi, le aziende americane fornitrici della tecnologia su cui si fonda il cloud nazionale potrebbero venire in possesso dei "dati" contenuti nel cloud, ma ciò non implicherebbe la conoscenza delle "informazioni" portate dai dati, ché sono crittografate e dovrebbero essere conoscibili solo dai titolari italiani delle relative chiavi crittografiche esclusive. Si può pertanto porre una cesura nel rapporto fra dato e informazione, tale da escludere la capacità delle macchine di risalire dal dato all'informazione.

Possiamo quindi sintetizzare tre passaggi, in merito al rapporto fra dati e informazioni:

1) il dato è la base materiale ("la rappresentazione digitale"[52]) del suo significato, che chiamiamo informazione: a seconda di quanto sia rilevante (sul piano del valore giuridico-costituzionale) l'informazione che si può trarre dal dato, ovvero di quanto sia prezioso il dato e rischiosa la sua circolazione, è possibile anticipare la tutela al dato oppure si può consentire al dato di circolare e proteggere l'informazione che se ne ricava, oppure ancora non proteggere né l'uno né l'altra, perché è un bene che il dato e l'informazione circolino – quest'ultima dovrebbe essere la logica dei dati pubblici sul modello del cd. FOIA;
2) per ottenere una informazione dal dato è necessaria l'intermediazione della macchina; ciò comporta un dispendio di energia e, quindi, si lega il tema della evoluzione digitale alla sostenibilità ambientale[53], che può divenire un legittimo criterio di orientamento normativo, di rilievo costituzionale, dello sviluppo delle tecnologie;
3) nel rapporto fra dato e informazione, intermediato dalle macchine, esistono una molteplicità di strumenti tecnici volti a garantire l'improbabilità (e stipulativa impossibilità) che dal dato la macchina riesca a risalire all'informazione (crittografia) e strumenti organizzativi volti ad impedire che macchine non autorizzate possano analizzare dati protetti (obblighi di localizzazione, ad esempio). L'utilizzo di tali strumenti può essere combinato, ma soprattutto deve essere disciplinato in modo ordinato.

Nel contesto della dipendenza dai dati, la distinzione fra dati e informazioni assume un rilievo indiscutibile sia nei rapporti fra persone fisiche, sia nei rapporti di servizio e di consumo e cioè fra consumatore/utente e impresa, sia nei rapporti fra

48. Come puntualmente documenta E-Calzolaio 2023, spec. p. 92 e nota 15.

49. Ma su questo appunto si esercita la dottrina civilistica: E-Calzolaio 2023, p. 287 ss.

50. V. il sito ufficiale.

51. La disciplina e le vicende del PSN sono ben spiegate da Macrì 2022.

52. Cfr. *Data governance act*, art. 2, par. 1, n. 1), v. Iannuzzi 2024.

53. Cfr. Orofino 2023.

privati e soggetti pubblici, sia nei rapporti fra soggetti pubblici, ivi compresi i rapporti fra ordinamenti statuali.

Questa distinzione è un architrave ordinamentale di tutta la regolazione del diritto dei dati, anche se le difficoltà e incertezze definitorie non sempre riescono a farla emergere chiaramente, e in ciascun ambito sarà declinata seguendo gli equilibri e la tradizione giuridica dei diversi settori (diritto privato in senso stretto e diritto dei consumatori, diritto pubblico, diritto della concorrenza, diritto amministrativo e delle amministrazioni pubbliche, diritto delle telecomunicazioni, ecc.).

Per essere più chiari, le disposizioni in materia di trasparenza amministrativa (d.lgs. 33/2013) implicano di norma che, nell'adempimento degli obblighi di pubblicazione, dati e informazioni coincidano: il dato deve essere conoscibile a tutti e quindi non può essere pubblicato nella sezione amministrazione trasparente in una modalità o in un formato che renda non conoscibile l'informazione che il dato porta, ad esempio, richiedendo all'utente di dotarsi di un software proprietario per poter essere conosciuto.

In pressoché tutti gli altri casi è, invece, esattamente il contrario (o comunque ciascun soggetto può regolarsi, in assenza di norme specifiche, come meglio ritiene). Se invece l'informazione deve restare riservata o segreta, poiché l'ordinamento lo impone o l'interesse tutelato del soggetto che ne ha la disponibilità lo richiede, allora si utilizzeranno i metodi tipici per garantire riservatezza e segretezza: sul versante del dato, la localizzazione, la limitazione all'accesso o al trasferimento, il controllo da parte delle autorità preposte della circolazione del dato come tale; sul versante dell'informazione (i.e., del rapporto fra dato e informazione), la crittografia o strumenti di anonimizzazione o strumenti di pseudonimizzazione, o altri modelli organizzativi, a seconda dei casi.

In conclusione, possiamo distinguere un piano ordinamentale e un piano costituzionale.

Sul piano ordinamentale – cioè delle nozioni di base per qualsiasi forma di regolazione, pubblica o privata o pubblico-privata – la distinzione fra dato e informazione è basilare. In questo ambito occorre uno sforzo di osservazione e descrizione delle fattispecie concrete, da utilizzare per una corretta regolazione.

Sul piano costituzionale, nel rapporto fra dati e informazioni vale quel che affermava Norberto Bobbio nel noto saggio *La democrazia e il potere invisibile* del 1980: in democrazia, il governo si esprime attraverso un "potere visibile" e, pertanto, nello stato costituzionale, per quanto concerne i poteri pubblici, «la pubblicità è la regola, il segreto è l'eccezione». Qualche anno dopo, Paolo Barile apriva il proprio saggio *Democrazia e segreto* del 1987 affermando che «valgono regole opposte circa il segreto nel pubblico ed il segreto nel privato. L'apparato della democrazia ha per regola la trasparenza, ed il segreto costituisce una eccezione. I diritti costituzionalmente garantiti al soggetto privato in democrazia (la libertà nella comunità [n.d.a., *da tenere a mente: la libertà nella comunità*]) hanno per regola la privacy, e per eccezione la pubblicità».

5. Informazioni (dati) personali, informazioni (dati) non personali, dati importanti/critici, dati strategici

Una volta specificato il contesto ("dipendenza dai dati" e distinzione "genetica" fra dati e informazioni), possiamo addentriamoci allora nella tipologia, in senso oggettivo, dei dati e delle informazioni.

I dati sono – essenzialmente – la rappresentazione digitale di fatti e atti. Le informazioni che se ne traggono possono riguardare una persona fisica, identificata o identificabile, e allora sono dati personali, ovvero possono non riguardare una persona fisica, ed essere dati non personali.

Ma questa distinzione binaria (di cui siamo debitori innanzitutto del diritto europeo, poiché ci ha introdotto alla comprensione, alla regolazione e alla ricerca nel settore del diritto dei dati e del digitale), ben presto si è rivelata insufficiente a descrivere la tipologia in senso oggettivo dei dati, poiché l'ambiente digitale non si esaurisce nel discrimine fra dati personali e non personali.

E non è sufficiente affermare – come pure sembrerebbero voler dire il GDPR e il Regolamento sui dati non personali[54] – che un dato non personale può circolare liberamente, perché semplicemente non è così.

54. Torregiani 2020.

Nell'ordinamento dei dati cinese, ad esempio, è adottata una specifica tripartizione dei dati (nel DSL): dati, dati importanti, dati di interesse nazionale strategico[55].

La nozione di "dati importanti" appare davvero molto rilevante e cambia la prospettiva della regolazione, poiché identifica una specifica categoria della materia del diritto dei dati.

La legge cinese ci rivela che il regime dei dati non è determinato unicamente dal fatto di essere qualificati come "dati personali" (quindi protetti) o "dati non personali" (quindi soggetti a libera circolazione) secondo quanto sembrava prevedere – nella consueta prospettiva limitante del mercato unico digitale – l'ordinamento europeo.

La legge cinese afferma chiaramente che i dati e gli insiemi di dati, anche non personali, possono assumere valore strategico e possono avere diversi livelli di importanza per lo sviluppo economico e sociale e per la sicurezza dello Stato e dei diritti delle persone – a prescindere dalla loro qualificazione come dati personali o non personali. Le categorie cinesi sono tre, non due: informazioni personali, dati, dati importanti e quest'ultima è una categoria *autonoma e trasversale* rispetto alle altre (all'interno della quale si collocano anche i *core national data*, ovvero dati di interesse strategico nazionale).

A pochi mesi di distanza dalla adozione di queste leggi cinesi (rispettivamente settembre, DSL, e novembre, PIPL, del 2021), in Italia, la costituzione del Cloud nazionale[56] poneva esattamente gli stessi problemi di classificazione di dati e servizi pubblici e l'Agid, con proprio regolamento[57], richiedeva alle amministrazioni pubbliche di classificare i propri dati e servizi «sulla base della loro caratterizzazione, nelle seguenti tre classi:

a. *strategici*, se la loro compromissione può determinare un pregiudizio alla sicurezza nazionale;
b. *critici*, se la loro compromissione può determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese;
c. *ordinari*, qualora la loro compromissione non determini i pregiudizi di cui alle lettere a) e b)»

(così art. 3, c. 3, Regolamento Agid cd. *Servizi Cloud*).

Solo per completezza si ricorda – rinviando ancora al testo prezioso di Indra Macrì[58], che spiega con chiarezza procedure che altrimenti sarebbe estremamente faticoso ricostruire, da parte di un giurista, sulla base dei soli atti, normativi e non, delle diverse autorità implicate – che a partire da questa *classificazione di dati e servizi* si realizza, in parallelo, una *qualificazione dei servizi cloud* (cloud pubblico qualificato e non qualificato, cloud pubblico criptato, cloud privato/ibrido su licenza e privato qualificato), in forza della quale al livello di "sensibilità" dei dati corrisponde la possibilità di valersi di cloud recanti maggiori garanzie in termini di localizzazione, vigilanza esterna, crittografia dei dati[59]. Il Polo strategico nazionale (PSN) che è in fase di realizzazione viene utilizzato proprio per consentire la migrazione dei dati delle pubbliche amministrazioni in cloud qualificati e sicuri e, per i dati strategici, localizzati in Italia[60].

Vi sono alcuni profili da rimarcare in merito alla classificazione in senso oggettivo dei dati.

Il primo aspetto è che alcuni principi e indirizzi normativi – come quello dell'altruismo dei dati (su cui, in questa sezione monografica, v. il contributo di Elia Cremona[61]), o del più generale favore per la condivisione dei dati per finalità di sviluppo,

55. Sia consentito rinviare a Calzolaio 2023, p. 209 ss.

56. Su cui v. ancora Macrì 2022, p. 293 ss.

57. AGID, determinazione n. 628, 15 dicembre 2021, recante Adozione del "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione".

58. Macrì 2022, pp. 319-325.

59. Cfr. art. 33-*septies*, d.l. 179/2012.

60. Ci eravamo per l'appunto posti il problema della localizzazione dei dati, qualche tempo fa, in questa Rivista: cfr. Calzolaio 2021.

61. Cremona 2023.

ricerca ecc.[62] – si possono applicare, di norma, *in via residuale* alle categorie di dati non personali, non critici, non strategici. Che senso avrebbe, altrimenti, far classificare i dati alle amministrazioni pubbliche come critici e/o strategici e di conseguenza adottare modelli di cloud qualificati per mantenere i dati (e i servizi) sicuri, per poi consentirne la condivisione o la diffusione sistematica?

D'altra parte, proprio il regime di sicurezza che consegue alla classificazione dei dati delle amministrazioni come critici o strategici impone che i criteri regolamentari siano applicati in modo uniforme sull'intero territorio nazionale[63], per evitare che le amministrazioni classifichino in modo diverso dati e servizi analoghi (o viceversa), ingenerando una evitabile confusione e rischi per la sicurezza.

La quadripartizione classificatoria qui proposta si pone al punto di confluenza fra l'ordinamento (europeo) dei dati personali e l'ordinamento costituzionale dei dati e, in questo ambito, il diritto (europeo) alla protezione dei dati personali si incontra con le esigenze nazionali attinenti alla cd. sovranità digitale[64] (su cui si veda, in questa sezione monografica, il contributo di Stefano Torregiani[65]), sotto il profilo della organizzazione delle pubbliche amministrazioni e della tutela dei diritti dei cittadini italiani.

6. Dati, dati sintetici e sistema dell'informazione ibrido: l'essenziale è invisibile agli occhi?

«… my Administration will help develop effective labeling and content provenance mechanisms, so that Americans are able to determine when content is generated using AI and when it is not. These actions will provide a vital foundation for an approach that addresses AI's risks without unduly reducing its benefits»[66].

Questa è una delle preoccupazioni principali che esprime il presidente Biden nel suo ordine esecutivo Executive Order (E.O.) *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* del 30 ottobre del 2023.

Questo aspetto interessa specificamente l'ordinamento dei dati e, più specificamente, lo arricchisce ormai strutturalmente di una categoria ulteriore, che è in grado di rivoluzionare il nostro ambiente umano: i dati sintetici.

Ma procediamo per gradi.

Che cos'è l'intelligenza artificiale generativa? Secondo l'E.O. «The term "generative AI" means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content».

E cosa sono questi contenuti sintetici? Ancora secondo l'E.O. «The term "synthetic content" means information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI».

Ciò significa che l'IA generativa produce per definizione contenuti sintetici – i.e., dati sintetici, informazioni sintetiche – di qualsiasi tipo (immagini, video, testi e altri contenuti digitali).

E perché mai questi contenuti sintetici dovrebbero preoccuparci, così come preoccupano il presidente Biden che vi dedica l'intero titolo 4.5 (*Reducing the Risks Posed by Synthetic Content*) del suo E.O.?

Perché sono contenuti prodotti e messi in circolazione nello spazio digitale senza che, attualmente, gli esseri umani possano distinguerli dai contenuti non sintetici – cioè dai contenuti aventi una origine effettivamente umana.

E perché questo aspetto è così rilevante? Facciamo un esempio.

Immaginiamo che un gruppo di informatici addestri un sistema di intelligenza artificiale per produrre immagini di ambienti interni ed esterni di chiese, palazzi storici, beni culturali in genere. Il sistema viene alimentato da immagini reali, le

62. Cfr. Iannuzzi 2024.

63. Si tratta di applicare i principi del coordinamento digitale unitario e di standardizzazione, indicati in Calzolaio 2016, spec. p. 196.

64. Finocchiaro 2022, pp. 809 ss.; Simoncini 2017.

65. Torregiani 2023.

66. U.S. Executive Order 14110 of October 30, 2023, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

immagazzina, le elabora, e poi comincia a produrne autonomamente a milioni – si pensi a quanta elegante creatività a basso costo per architetti, designer, mobilifici ecc.!

Queste immagini verosimili riproducono anche ambienti e beni reali: piazza San Pietro, la basilica di San Francesco di Assisi, la Tour Eiffel e così via. Queste immagini cominciano ad abitare, o ad invadere, lo spazio digitale e poi il Web.

Un giovane studente svolge una ricerca scolastica su uno di questi monumenti, quindi osserva e scarica queste immagini: sono verosimili, ma non riproducono esattamente quel monumento. Ci sono delle differenze, più o meno percettibili. Lo studente descrive l'immagine, che crede reale, e invece è verosimile, quindi contiene delle differenze con la foto reale del monumento. Lo studente, tuttavia, è certo di conoscere quel monumento sulla base delle immagini reperite e quando il professore gli fa osservare che, invece, quel monumento non ha questa o quella caratteristica che lo studente ha descritto, lo studente reagisce come se il professore negasse una realtà evidente, oggettiva. Ne nasce una discussione: entrambi sanno di avere ragione[67].

Immaginiamo ora che sia trascorso del tempo: 100 anni. E che in questi 100 anni si siano accumulate una miriade di immagini che riproducono in tutti i modi quel certo monumento in diversi momenti di tempo e altrettante ricerche: potremmo ricostruire la storia del monumento, se potessimo essere (ragionevolmente) certi che sono vere le immagini e le ricerche che ritraggono e raccontano effettivamente quel monumento così com'era tempo per tempo. Ma non possiamo più esserlo: la maggior parte delle immagini e delle ricerche sono contenuti sintetici, o ibridi, e non ritraggono e non raccontano i luoghi, ma sono prodotto – verosimile, indistinguibile immediatamente – di intelligenza artificiale generativa[68]. Non solo: i racconti delle persone viventi sullo stato dei luoghi e sulle vicende del monumento non coincidono con le immagini e le ricerche, talvolta sono contraddittori. Ne nasce una grande incertezza: nessuno si può fidare della narrazione storica.

Il primo aspetto rilevante dell'avvento pervasivo della categoria dei dati sintetici è che essi sono in grado di modificare, impercettibilmente, *l'asse terrestre della cognizione umana*[69]. Con conseguenze imprevedibili, ma certamente rischiose, nel breve, medio e lungo termine.

Per questo, l'E.O. adotta politiche immediate di *watermarking*[70] e di etichettatura di questi dati sintetici e delle relative informazioni immesse nel circuito digitale[71].

Tuttavia – e questo è il secondo aspetto – non possiamo illuderci: il sistema dell'informazione in cui siamo immersi e da cui traiamo la cognizione della realtà che ci circonda è già da tempo ibrido, cioè abitato e popolato da persone verosimili e comunicative, ma che non sono persone pur presentandosi come tali, in modo occulto (bot)[72], o in modo palese (co-pilot). L'IA generativa rappresenta un salto di qualità, in questo senso: ma

67. C'è anche un analogo esempio divertente nella filmografia di 007, *Il domani non muore mai*, 1997, in cui un miliardario del settore delle telecomunicazioni sviluppa un sistema in grado di modificare il segnale GPS, e quindi la cognizione della posizione in mare, ricevuto da una nave da guerra inglese e la fa sconfinare – ignara – nelle acque territoriali cinesi, con tutte le conseguenze del caso.

68. Cfr. Wagner-de Clippele 2023.

69. … in qualche modo l'E.O. del presidente Biden rappresenta una prima forma di disciplina della IA generativa, che appare seguire l'orientamento del giudice Thomas richiamato puntualmente da Niro 2021.

70. … secondo l'E.O.: «The term "watermarking" means the act of embedding information, which is typically difficult to remove, into outputs created by AI—including into outputs such as photos, videos, audio clips, or text—for the purposes of verifying the authenticity of the output or the identity or characteristics of its provenance, modifications, or conveyance».

71. L'E.O., titolo 4.5. *Reducing the Risks Posed by Synthetic Content*, fissa tappe precise per garantire l'identificazione, la rilevazione, la provenienza e l'etichettatura dei contenuti sintetici, e lo sviluppo di tecniche e standard per l'autenticazione dei contenuti. Si rinvia al testo dell'E.O. per maggior dettaglio, delle incisive misure presidenziali in merito.

72. Cfr. Tedeschi Toschi-Berni Ferretti 2023.

dobbiamo riconoscere che abitiamo in una realtà cognitivamente ibrida, fatta di relazioni con soggetti e oggetti digitali che influiscono sulla nostra percezione della realtà (si vedano i contributi in questa sezione monografica di Angela Cossiri e Arturo Di Corinto[73]), in modo ancor più incisivo se riteniamo che non sia così e di non accorgercene.

È a questo livello che si pone il problema, peraltro acutamente affrontato in dottrina, della c.d. "riserva di umanità"[74]. La realtà ibrida non consente "riserve", perché incide ineluttabilmente proprio su ciò che intendiamo per "umanità", cioè sulla nostra sfera cognitiva, sulla formazione del pensiero e della personalità[75]: lo studente del nostro precedente esempio potrebbe essere un giudice, un chirurgo, un generale, un autista, un dirigente d'azienda, una persona comunque convinta di basare le proprie azioni su una visione *oggettiva* – ma in realtà solo *oggettivizzata* – della realtà, e di essere nel giusto, di rappresentare il vero. Quindi, più che difendersi, bisogna apprendere rapidamente ad affrontare la realtà ibrida con tutti i suoi rischi epocali – come intuito rapidamente dall'E.O.

Il primo passo in tal senso è aggiornare la classificazione dei dati e delle informazioni con il riferimento esplicito agli inevitabili contenuti sintetici, ed alla pressante esigenza di determinare le modalità per renderli il più possibile sistematicamente visibili e riconoscibili agli esseri umani (e, soprattutto, ai minori).

7. Una (apparente) sosta: dati epidemiologici del Surgeon General

Nel 2023 il Surgeon General (S.G.) statunitense ha pubblicato solo due Avvisi[76].

Raccontano due distinte, ma connesse, emergenze epidemiologiche che investono la società statunitense e che – per dovere istituzionale – spetta proprio al S.G. identificare e denunciare, per tutelare e proteggere la salute pubblica degli americani.

A ormai oltre 25 anni dall'avvento della rete Internet e a oltre 15 dall'avvento dei social media, come fenomeni di massa, la società americana è investita da due fenomeni che minacciano – dati alla mano – la speranza di vita e la salute degli americani: la solitudine e l'isolamento sociale delle persone; la salute mentale dei giovani. Come si potrà verificare, si tratta di due studi seriamente documentati.

Per quanto qui interessa, in entrambi – molto più esplicitamente in quello concernente i minori, che davvero non lascia nulla di implicito (negli Stati Uniti è in atto «una crisi nazionale di salute mentale giovanile»: p. 13, righe 9-10) – si identifica un ruolo specifico dell'avvento della società digitale nel mutamento esistenziale e nel peggioramento delle condizioni socio-sanitarie che colpisce gli americani e i giovani americani.

Le azioni che sono suggerite per contrastare queste problematiche coinvolgono esplicitamente i famosi "poteri privati" della tecnologia. Ma a mio avviso vi è un profilo ancor più rilevante in questi Avvisi: essi cercano di enucleare modalità operative di azione dei poteri pubblici (e privati) americani per contrastare la solitudine e l'isolamento sociale, da un lato, e le minacce alla salute mentale dei giovani, dall'altro: queste sembrano essere le vulnerabilità della società americana più pressanti.

Sul primo versante, il S.G. suggerisce l'adozione di politiche pubbliche che favoriscano le relazioni sociali e, in particolare, il *"Connection-in-All-Policies" approach*.

È peculiare che nella patria dell'individualismo si proponga esplicitamente e come misura in grado di contrastare la diminuzione della speranza di vita delle persone sole o isolate, l'adozione sistematica di politiche pubbliche attive, in tutti i settori, volte a favorire la partecipazione delle persone ai rispettivi ambienti comunitari.

Questo aspetto colpisce, in quanto si tratta un profilo che la Costituzione italiana – forse più di quella americana – conosce e valorizza, a partire proprio dalla formula dell'art. 2 Cost.: «la "persona", per non scadere ad "individuo", va considerata non solo nella sua "immanenza" [n.d.a., *ove oggi sarebbe vittima di una realtà ibrida, che lo relega alla solitudine ed allo sbandamento cognitivo*] ma anche nella sua "apertura sociale", non solo "nell'isolamento dell'uomo dall'uomo", ma anche "nel

73. Cossiri 2023; Di Corinto 2023.

74. Cfr. Gallone 2023; Cerri 2023.

75. Richards 2015.

76. Cfr. U.S. Surgeon General 2023; U.S. Surgeon General 2023A.

legame dell'uomo con l'uomo"»[77] e i doveri di solidarietà «sono da vedere non in funzione restrittiva della libertà della persona (non come eccezioni rispetto a regole) ma in una prospettiva tale da consentirne il pieno ed armonico sviluppo»[78]; e ancora: «le formazioni sociali vengono riconosciute e garantite a livello costituzionale non come tali ma nella misura in cui consentano e favoriscano il libero sviluppo della persona (…) o nella misura in cui garantiscano la tutela di "interessi diffusi" rilevanti costituzionalmente»[79].

Sorprende quindi che, senza negare l'esigenza di modificare i modelli fatti propri dai poteri privati delle *big tech*, il S.G. muova dalla esigenza di riscoprire la dimensione ed il valore sociale dei rapporti personali (fra) privati, come rimedio a malattie e morte precoce, fra l'altro.

Sul versante della tutela della salute mentale dei minori dai social media – e come si comprende, non deve essere stato particolarmente popolare l'intitolazione stessa dell'Avviso presso le *big tech* – il S.G. rileva che, in assenza di protezioni adeguate, i bambini statunitensi sono divenuti partecipanti inconsapevoli di un esperimento decennale. Pertanto è molto più netto, stanti anche le gravi conseguenze di questa esposizione, e si richiama all'esigenza di applicare il *Safety-first approach*: «According to this principle, a basic threshold for safety must be met, and until safety is demonstrated with rigorous evidence and independent evaluation, protections are put in place to minimize the risk of harm from products, services, or goods»[80].

Vorrei osservare che fra i molteplici interventi normativi dell'Unione europea in materia di diritto dei dati e di società digitale – come emerge dalla tabella curata da Camilla Lobascio[81] – non v'è specifica attenzione a nessuno di questi due aspetti, di cui onestamente il più originale è senz'altro il primo: il recupero e la promozione delle relazioni sociali come strumento di lotta all'isolamento ed alla solitudine largamente indotti, o almeno accelerati, dall'avvento della società digitale e della datificazione.

8. Spunti conclusivi per un ordinamento costituzionale dei dati

In conclusione, si desidera sommessamente individuare, a mo' di elenco, una serie di temi di stretta, e anche classica, attinenza costituzionale che rappresentano altrettanti capitoli da scrivere per fondare un effettivo ordinamento costituzionale dei dati, che limiti e orienti il processo di datificazione: la tutela della libertà di pensiero e del libero sviluppo della personalità; l'esigenza positiva di concepire un nuovo modello di pluralismo informativo; il rischio di una regolazione eccessiva e di un accentramento di competenze tecniche in organi sostanzialmente di governo.

Il primo fra questi è stato sviluppato negli Stati Uniti da Neil Richards, con il suo volume del 2015, sulla *Intellectual privacy*: sin da allora – e sul piano tecnologico è già cambiata un'epoca – egli osservava che la protezione dei dati personali non era più solo una questione di autodeterminazione informativa, ma ormai appariva come un presidio della libera formazione del pensiero e, con esso, della personalità. La datificazione e l'asseto ibrido del sistema dell'informazione e, ormai si può affermare, della realtà, mettono davvero a rischio le funzioni cognitive dell'essere umano. La rete di relazioni sociali e la sua sistematica promozione sono un buon antidoto: ma cos'altro può proteggere la sfera di libertà della persona di fronte alle macchine intelligenti che la circondano?

Un secondo aspetto – connesso – concerne la riscoperta del significato attuale del principio del pluralismo informativo[82]. Il principio in parola[83] nasce per garantire che il sistema dell'informazione più pervasivo del tempo, quello radio-televisivo,

77. Cosi Barbera 1975, p. 106, citando Karl Marx, nella nota 14.

78. *Ibidem*, p. 106.

79. *Ibidem*, p. 109.

80. Ivi compresa l'azione di «Pursue policies that further limit access – in ways that minimize the risk of harm – to social media for all children, including strengthening and enforcing age minimums».

81. Lobascio 2023.

82. Cfr. Caterina 2023, p. 19 ss.

83. Albanesi-Valastro-Zaccaria 2023, pp. 35-37.

vedesse protagonisti una pluralità di soggetti, nessuno dei quali in posizione dominante (pluralismo esterno) in modo che vi fossero più voci diverse ad operare nel sistema dell'informazione. D'altra parte, seppure rivolto principalmente alla radio-tv pubblica, si è anche affermato il principio del pluralismo interno, inteso nel senso di offrire, all'interno della medesima emittente, il più largo spazio a opinioni, tendenze e culture diverse e rappresentative del pluralismo sociale. Nell'era dell'iperconnessione ibrida e delle piattaforme digitali, cosa si intende per pluralismo informativo? Come si possono coniugare (o limitare reciprocamente) datificazione, iperconnessione e esigenze personali, sociali e democratiche di pluralismo informativo (o, se si preferisce, di libertà passiva di informazione)? Il nemico di un tempo (la tradizionale scarsità di risorse informative, frequenze ed editori) appare superato, ed anzi oggi appare l'eccesso e la velocità di informazione un ostacolo al pluralismo informativo: forse un aiuto potrebbe arrivare proprio da una limitazione della velocità delle informazioni e da un design orientato al pluralismo informativo di strumenti di intelligenza artificiale che ci supportino? Si possono applicare modelli di valutazione del rischio anche a questo ambito, per suggerire un quadro plurale qualitativamente e sostenibile quantitativamente di informazioni?

Il terzo aspetto – come emerge dalla citata Tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme – concerne i rischi di coordinamento e integrazione della cospicua regolazione europea sopravvenuta nell'ultimo biennio, sia rispetto all'esperienza – positiva! – maturata nella applicazione del GDPR, sia rispetto alla effettiva capacità regolatoria dei nuovi fronti aperti, dal DGA/DA, al delicato e rimaneggiato IA Act. Un focus particolare concerne poi l'esigenza di una efficace allocazione delle funzioni, anche di carattere tecnico, strettamente connesse, se non proprio assimilabili in questo campo, con quelle regolatorie[84]. Come osserva bene Federico Serini[85], la regolazione della società digitale si sviluppa innanzitutto attraverso la fissazione degli standard internazionali che governano i diversi aspetti alla base della produzione delle tecnologie, che spesso sfuggono anche al livello europeo.

In ogni caso, come si avvertiva già qualche tempo fa, siamo ormai lontani dalla regolazione della società digitale come ordine spontaneo[86].

This work has been funded by the European Union - NextGenerationEU under the Italian Ministry of University and Research (MUR) National Innovation Ecosystem grant ECS00000041 - VITALITY - CUP E13C22001060006

Riferimenti bibliografici

L. Abba, A. Lazzaroni, M. Pietrangelo (2022) (a cura di), *La internet governance e le sfide della trasformazione digitale*, Editoriale scientifica, 2022

M. Abrams (2014), *The Origins of Personal Data and its Implications for Governance*, The Information Accountability Foundation, March 2014

E. Albanesi, A. Valastro, R. Zaccaria (2023), *Diritto dell'informazione e della comunicazione*, Cedam, 2023

M.R. Allegri (2018), *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, FrancoAngeli, 2018

V. Amenta (2015), *Internet governance eco-system: un'utopia globale? Dal modello multi-stakeholders al modello multi-equal-stakeholders*, Giuffrè, 2015

84. Sia consentito rinviare, a questo riguardo, a Calzolaio 2024.

85. Serini 2023.

86. Cfr. Bifulco 2018, spec. p. 394 ss.

C. Anderson (2008), *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, in "Wired", 23 June 2008

M. Arnese, F. Walsingham (2020), *Perché Ericsson, Nokia, Cisco e Microsoft brinderanno in Italia col 5G,* in "Start Magazine", 16 luglio 2020

T.G. Ash (2023), *Patrie*, Garzanti, 2023

A. Barbera (2020), *Prefazione*, in U. Ruffolo (a cura di), "Intelligenza artificiale. Il diritto, i diritti, l'etica", Giuffré, 2020

A. Barbera (2015), *Costituzione della Repubblica italiana*, in "Enciclopedia del Diritto", Giuffrè, 2015

A. Barbera (2010), *Ordinamento costituzionale e carte costituzionali*, in "Quaderni costituzionali", 2010, n. 2

A. Barbera (1975), *Articolo 2 Cost.*, in G. Branca (a cura di), "Commentario della Costituzione. Artt. 1-12. Principi fondamentali", Zanichelli, 1975

E. Bassi (2022), *Dati, sovranità, nuovi modelli di governance*, in M. Durante, U. Pagallo (a cura di), "La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società", Mimesis, 2022

M. Bassini (2019), *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali*, Aracne 2019

F. Bechis, R. Mieli (2019), *La nuova via della seta e il 5G. Gli obiettivi della Cina e i rischi per l'Italia*, Dossier del Machiavelli, n. 14, 21 marzo 2019

C. Bergonzini (2023), *"Prova a prendermi". Ecosistema digitale e consapevolezza degli utenti: uno spazio per la regolazione nazionale?*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

R. Bifulco (2018), *Intelligenza artificiale, internet e ordine spontaneo*, in F. Pizzetti, "Intelligenza artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018

V. Boncinelli (2021), *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, in "Rivista italiana di informatica e diritto", 2021, n. 1

E. Bruti Liberati (2023), *Poteri privati e nuova regolazione pubblica*, in "Diritto pubblico", 2023, n. 1

E. Calzolaio (2023), *Beni digitali e proprietà fra civil law e common law*, in "Rivista critica di diritto privato", 2023, n. 3

S. Calzolaio (2024), *Autorità indipendenti e di governo della società digitale*, in corso di pubblicazione, Giappichelli, 2024

S. Calzolaio (2023), *Dalla protezione dei dati personali all'ordinamento dei dati (l'evoluzione del diritto cinese e del diritto europeo dei dati)*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

S. Calzolaio (2021), *Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in "Rivista italiana di informatica e diritto", 2021, n. 1

S. Calzolaio (2021a) (a cura di), *Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in "Rivista italiana di informatica e diritto", 2021, n. 1

S. Calzolaio (2018), *Recensione a: "Neil Richards, Intellectual privacy. Rethinking civil liberties in the digital age, Oxford University Press, 2017"*, in "Giornale di storia costituzionale", 2018, n. 36

S. Calzolaio (2017), voce *Protezione dei dati personali*, in "Digesto delle Discipline pubblicistiche", Aggiornamento, Utet Giuridica, 2017

S. Calzolaio (2016), *Digital (and privacy) by default. L'identità costituzionale dell'amministrazione digitale*, in "Giornale di storia costituzionale", 2016, n. 1

B. Caravita (2020), *Principi costituzionali e intelligenza artificiale*, in U. Ruffolo (a cura di), "Intelligenza artificiale. Il diritto, i diritti, l'etica", Giuffrè, 2020

C. Caruso (2023), *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in "Quaderni costituzionali", 2023, n. 3

M. Castells (2009), *Comunicazione e potere*, UBE, 2009

E. Caterina (2023), *La comunicazione elettorale sui social media tra autoregolazione e profili di diritto costituzionale*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

A. Cerri (2023), *Spunti e riflessioni sull'impiego dell'Intelligenza Artificiale nei procedimenti giuridici*, in "Diritto pubblico", 2023, n. 1

A.S.Y. Cheung, Y. Chen (2022), *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, in "Law & Social Inquiry", 2022, n. 11

Y.M. Citino (2023), *Social scoring e città distopica: la profilazione del cittadino con finalità di policy urbana alla prova dei valori costituzionali*, in G. Allegri, L. Frosina, A. Guerra, A. Longo (a cura di), "La città come istituzione, entro e oltre lo Stato", Sapienza editrice, 2023

J. Cohen (2019), *Between Truth and Power. The Legal Construction of Informational Capitalism*, Oxford University Press, 2019

G.L. Conti (2022), *Contratto sociale e Grundnorm al tempo degli unicorni*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La internet governance e le sfide della trasformazione digitale", Editoriale scientifica, 2022

F. Cossiga, P. Chessa (2007), *Italiani sono sempre gli altri, Controstoria d'Italia da Cavour a Berlusconi*, Mondadori, 2007

A. Cossiri (2023), *Le campagne di disinformazione nell'arsenale di guerra: strumenti giuridici per contrastare la minaccia alla prova del bilanciamento*, in "Rivista italiana di informatica e diritto", 2023, n. 2

F. Costantino (2023), *La c.d. cittadinanza digitale,* in "Diritto pubblico", 2023, n. 1

E. Cremona (2023), *Quando i dati diventano beni comuni: modelli di* data sharing *e prospettive di riuso*, in "Rivista italiana di informatica e diritto", 2023, n. 2

M. Cuomo (2023), *La tutela del diritto alla disconnessione. Fonti, limiti e prospettive*, in "Lavoro Diritti Europa", 2023, n. 3

G. D'Acquisto (2021), *Intelligenza artificiale. Elementi*, Giappichelli, 2021

G. D'Acquisto, M. Naldi (2017), *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli, 2017

G. De Gregorio (2022), *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022

G. De Gregorio, N. Stremlau (2020), *Internet Shutdowns and the Limits of Law*, in "International Journal of Communication", vol. 14, 2020

A. de Tocqueville (2005), *La democrazia in America*, (a cura di) G. Candeloro, RCS libri, 2005

A. Di Corinto (2023), *Netwar, come cambia l'hacktivismo nella guerra cibernetica*, in "Rivista italiana di informatica e diritto", 2023, n. 2

G. Di Cosimo (2023) (a cura di), *Processi democratici e tecnologie digitali*, Giappichelli, 2023

V. Dubal (2023), *On algorithmic wage discrimination*, in "Columbia Law Review", vol. 123, 2023, n. 7

M. Durante (2022), *Il Potere computazionale: dalle informazioni ai dati*, in M. Durante, U. Pagallo (a cura di), "La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società", Mimesis, 2022

M. Durante, U. Pagallo (2022) (a cura di), *La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società*, Mimesis, 2022

R. Eldan, M. Russinovich (2023), *Who's Harry Potter? Approximate Unlearning in LLMs*, in arXiv, 2023

P. Elmer-Dewitt (1993), *First Nation in Cyberspace*, in "Time", 6 December 1993

G. Finocchiaro (2022), *La sovranità digitale*, in "Diritto pubblico", 2022, n. 3

G. Finocchiaro (2012), *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012

L. Floridi (2018), *The Semantic Capital: Its Nature, Value, and Curation*, in "Philosophy & Technology", vol. 31, 2018, n. 4

J.O. Freuler (2023), *Datafication, identity, and the reorganization of the category individual*, in "Temple Law Review", vol. 95, 2023, n. 4

G. Gallone (2023), *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Cedam, 2023

K. Geddes (2023), *The Death of the Legal Subject*, in "Vanderbilt Journal of Entertainment & Technology Law", vol. 25, 2023, n. 1

Y. Guerra (2023), *Il fenomeno delle smart city come esempio di co-regolazione delle nuove tecnologie. La democrazia locale di fronte alle sfide globali*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

S. Gunasekar et al. (2023), *Textbooks Are All You Need*, in arXiv, 2023

W. Hartzog, N. Richards (2022), *The surprising virtues of data loyalty*, in "Emory Law Journal", vol. 71, 2022, n. 5

A. Iannuzzi (2024), *I regolamenti intersettoriali per l'istituzione dei «data spaces»: Data Governance Act e Data Act*, in corso di pubblicazione, Giappichelli, 2024

A. Iannuzzi (2024a), *Le fonti del diritto per la disciplina della società digitale come affermazione della sovranità digitale europea*, in corso di pubblicazione, Giappichelli, 2024

P. Khanna (2016), *Connectography. Le mappe del futuro mondiale*, ed. it. Fazi, 2016

M.A. Lemley (2021), *The splinternet*, in "Duke Law Journal", vol. 70, 2021

C. Lobascio (2023), *Tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme,* in "Rivista italiana di informatica e diritto", 2023, n. 2

O. Lobel (2021), *Biopolitical opportunities between datafication and governance*, in "Notre Dame Law Review Reflection", vol. 96, 2021

E. Longo (2024), *La disciplina del rischio digitale*, in corso di pubblicazione, Giappichelli, 2024

E. Longo (2024a), *La sicurezza nel ciberspazio. La disciplina della cybersecurity nell'Unione europea e in Italia*, in corso di pubblicazione, Giappichelli, 2024

M. Luciani (2006), *Costituzionalismo irenico e costituzionalismo polemico*, in "Giurisprudenza costituzionale", 2006, n. 4

I. Macrì (2022), *Digitalizzazione, innovazione e sicurezza nella P.A.*, Wolters Kluwer, 2022

M. Manetti (2023), *Internet e i nuovi pericoli per la libertà di informazione*, in "Quaderni costituzionali", 2023, n. 3

M. Manetti (2020), *Regolare Internet*, in "Media Laws", 2020, n. 2

J. Marinotti (2022), *Data Types, Data Doubts & Data Trusts*, in "New York University Law Review Online", vol. 97, 2022

M. Micheli, M. Ponti, M. Craglia, A. Berti Suman (2020), *Emerging models of data governance in the age of datafication*, in "Big data & society", 2020, n. 2

G. Mobilio (2021), *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, 2021

A. Morrone (2023), *Sul «ritorno dello Stato» nell'economia e nella società*, in "Quaderni costituzionali", 2023, n. 2

R. Niro (2021), *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolazione: note ricostruttive*, in "Osservatorio sulle fonti", 2021, n. 3

OECD (2014), *Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, 21 March 2014

S. Orlando (2022), *Data vs capta: intorno alla definizione di dati*, in "Nuovo diritto civile", 2022, n. 4

M. Orofino (2023), *Le due transizioni, digitale e verde, nel c.d. pacchetto digitale europeo*, in "Astrid Rassegna", 2023, n. 10

J. Perry Barlow (1996), *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation, 8 February 1996

M. Pierri (2019), *Con il 5G cinese a rischio la condivisione di informazioni con gli Usa. L'avvertimento di Eisenberg*, 1 aprile 2019

F. Pizzetti (2018), *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in Id., "Intelligenza artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018

G.M. Riccio (2002), *La responsabilità civile degli internet providers*, Giappichelli, 2002

N. Richards (2015), *Intellectual Privacy. Rethinking civil liberties in the digital age*, Oxford University Press, 2015

G.M. Salerno (2018), *Le garanzie della democrazia*, in "Rivista AIC", 2018, n. 3

G. Scorza (2022), *In principio era internet e lo immaginavamo diverso*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La internet governance e le sfide della trasformazione digitale", Editoriale scientifica, 2022

F. Serini (2023), *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in "Rivista italiana di informatica e diritto", 2023, n. 2

F. Serini (2022), *La protezione dei dati personali tra Giappone e Unione europea*, Aracne, 2022

A. Simoncini (2021), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di stato e forma di governo*, in "Osservatorio sulle fonti", 2021, n. 2

A. Simoncini (2020), *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin, D.U. Galetta (a cura di), "Il Diritto dell'ammnistrazione pubblica digitale", 2020

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "Bio-Law Journal – Rivista di BioDiritto", 2019, n. 1

A. Simoncini (2017), *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), "Diritti e libertà in Internet", Mondadori Education, 2017

A. Simoncini, S. Suweis (2019), *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in "Rivista di filosofia del diritto", 2019, n. 1

C.P. Sundquist (2023), *Surveillance Normalization*, in "Harvard Civil Rights-Civil Liberties Law Review", vol. 58, 2023

A. Tedeschi Toschi, G. Berni Ferretti (2023), *Il contrasto legislativo ai socialbot. Alcuni spunti per una riforma in Italia*, in "Rivista italiana di informatica e diritto", 2023, n. 1

L. Torchia (2023), *Lo Stato digitale*, il Mulino, 2023

S. Torregiani (2023), *Il* Data Act*: una versione europea del* Data Nationalism*?*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Torregiani (2020), *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in "federalismi.it", 2020, n. 18

U.S. Surgeon General (2023), *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*, 2023

U.S. Surgeon General (2023a), *Social Media and Youth Mental Health. The U.S. Surgeon General's Advisory*, 2023

G.E. Vigevani (2023), *Piattaforme digitali private, potere pubblico e libertà di espressione*, in "Diritto costituzionale", 2023, n. 1

A. Wagner, M.-S. de Clippele (2023), *Safeguarding Cultural Heritage in the Digital Era – A Critical Challenge*, in "International Journal of Semiotic Law", 2023, n. 36

F. Wenfei, F. Geerts (2012), *Foundations of data quality management*, Springer Nature, 2012

L. Zorloni (2024), *I blackout di internet minacciano le elezioni 2024,* in "Wired", 10 febbraio 2024

S. Zuboff (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019