

GIANLUIGI FIORIGLIO\*

## La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici

### ENGLISH TITLE

The Algorithmic Society between Opacity and Explainability: Legal and Informatics Profiles

### ABSTRACT

Information Society has evolved to Algorithmic Society, where decision-making processes are done not only by humans but also by artificial agents. However, opacity usually characterizes algorithms, and it means that machine reasoning could be understood only looking at each output, while keeping their manufacturers substantially unaccountable.

Starting from the perspective of legal informatics, this paper aims at investigating the dichotomy between opacity and confidentiality, on the one hand, and explainability and transparency, on the other hand, taking into account the current debate. Eventually, challenges and possible solutions for a fair Algorithmic society are discussed.

### KEYWORDS

Algorithmic Society – Artificial Intelligence – Explainability – Opacity – Transparency.

### 1. SOCIETÀ ALGORITMICA

La Società dell'informazione pare oggi trasformarsi progressivamente in una Società algoritmica, a causa della pervasiva affermazione di sistemi sempre più intelligenti, autonomi e dinamici, che dapprima si affiancano a quelli tradizionali, meramente automatici e statici, per poi giungere a superarli qualitativamente e a imporre questioni giuridiche inedite, trasversali ed estremamente delicate.

\* Ricercatore a tempo determinato (di tipo B) di Filosofia del diritto presso il Dipartimento di Giurisprudenza dell'Università di Modena e Reggio Emilia.

Il presente contributo è finalizzato a discutere la suddetta evoluzione in prospettiva informatico-giuridica, presentando le principali problematiche che toccano l'ambito giuridico e approfondendo poi la dicotomia fra opacità/segretezza e trasparenza/spiegabilità. Saranno, infine, trattate le principali sfide poste dall'avvento della Società algoritmica e proposte alcune soluzioni per renderla più equa.

Tanto premesso, si può evidenziare come il riferimento, oramai di prassi, all'algoritmo abbia certamente il pregio di evidenziare in modo fortemente evocativo e dirompente il passaggio epocale dalla mera automazione nell'acquisizione e nel trattamento delle informazioni a una automazione "intelligente", grazie all'evoluzione dell'intelligenza artificiale che, nonostante la ben nota alternanza di illusioni e disillusioni, di sogni e di fallimenti, di "inverni" ed "estati", è diventata – quasi bruscamente – un elemento caratterizzante la società contemporanea (nonché le piattaforme e i sistemi informatici che caratterizzano proprio la Società algoritmica).

Sono infatti numerosissime le sue applicazioni divenute di uso comune, adoperate, a titolo esemplificativo, per automatizzare totalmente o parzialmente il reperimento, l'archiviazione e la diffusione di informazioni (motori di ricerca, social network), la redazione di graduatorie (concorsi), la valutazione dell'affidabilità creditizia (per la concessione di prestiti e mutui), la guida di veicoli (automobili, aeroplani, imbarcazioni), la visione di un filmato o l'ascolto di un brano musicale (piattaforme di streaming), l'assistenza clienti (chatbot), la pulizia (robot), il riconoscimento facciale e vocale (sistemi di autenticazione, interfacce utente ecc.). Inoltre, molti servizi sono resi combinando più applicazioni di intelligenza artificiale (oltre che più sistemi e basi di dati): basti pensare, in tal senso, alla semplice interrogazione di un motore di ricerca web utilizzando la propria voce, per cui l'input vocale viene acquisito ed elaborato da un dispositivo affinché divenga una *query* (e in altri casi per conoscere le previsioni metereologiche, l'orario ecc.).

Afferma, non a caso, che ci si sta muovendo rapidamente dall'era di Internet e dall'era digitale alla Società algoritmica, in cui i processi decisionali, e talvolta quelli esecutivi, sono svolti da algoritmi, robot e agenti intelligenti<sup>1</sup>.

Non v'è dubbio, del resto, che i dispositivi e i sistemi che fanno uso di tecniche di intelligenza artificiale, in modo più o meno sofisticato a seconda dei casi, la abbiano resa ubiqua: gli effetti della rivoluzione informatica sono sempre più marcati, da un lato, e sovente impercettibili, dall'altro. Due aspetti, questi, che appaiono paradossali, di primo acchito, ma che sono, invero, due facce della stessa medaglia.

In relazione al primo aspetto, i sistemi summenzionati possono incidere su diritti fondamentali (vita, salute, eguaglianza, riservatezza, manifestazione del

1. Balkin, 2017, p. 1219.

pensiero, istruzione, libertà di movimento, diritto di difesa ecc.). Basti pensare, in tal senso, agli utilizzi nelle strutture sanitarie (ad esempio, per coadiuvare il personale medico, infermieristico, socio-sanitario e amministrativo), nella prestazione dei servizi di ricerca web (il cui *ranking* ha un fortissimo impatto sui siti indicizzati e nella circolazione delle informazioni, indipendentemente dalla loro liceità) e di social network (sino all'*extrema ratio* della cancellazione di contenuti o della disabilitazione di account), nel reclutamento presso le pubbliche amministrazioni (per redigere automaticamente le graduatorie), nello svolgimento di attività di polizia (per individuare potenziali delinquenti), nella guida autonoma, così via. Questa sintetica ricognizione, pur senza pretesa di esaustività, sottolinea quanto siano ampi e delicati gli ambiti delle applicazioni dell'intelligenza artificiale.

In relazione al secondo profilo, quest'ultime sono così diffuse nella vita quotidiana e così ben incorporate in servizi e prodotti complessi, già "metabolizzati" (come smartphone, televisori, computer ecc.), da rendere talvolta impossibile o estremamente arduo comprendere che il loro output sia il frutto di complesse elaborazioni svolte da sistemi intelligenti (connesse in rete: non a caso, le reti telematiche costituiscono una sfida di enormi proporzioni per la scienza giuridica e la riflessione giusfilosofica, imponendo al contempo una revisione critica di alcune categorie tradizionali<sup>2</sup>).

Come ricorda Giovanni Sartor, questo enorme successo è anche dovuto al cambiamento del paradigma di ricerca e sviluppo in materia, che si è avuto andando oltre 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. Esso incontra, infatti, due limiti principali: potenziali incompletezza e incapacità di considerare le specificità dei casi concreti; onerosità nell'ampliamento e nell'aggiornamento della base di conoscenza. Per risolvere questi problemi si è quindi cercato di applicare metodi di apprendimento automatico (*machine learning*) a grandi masse di dati, per cui all'elaboratore viene fornito un metodo di apprendimento da applicare automaticamente ai dati cui ha accesso, in modo da poter svolgere il compito che gli viene assegnato, anche se ciò comporta l'imprevedibilità teorica e pratica della condotta della macchina (non a caso, questi modelli possono essere combinati per contemperare i relativi pregi e difetti)<sup>3</sup>.

Gli algoritmi, però, non sono neutrali, né tecnicamente né eticamente<sup>4</sup> e nel quadro sin qui appena tratteggiato emerge, intuitivamente, il ruolo predo-

2. Su questo profilo cfr. Casadei, 2017.

3. Sartor, 2020, p. 66.

4. Cfr., fra gli altri, Amato Mangiameli, 2019; Fioriglio, 2015a; Floridi, Taddeo, 2016. Per una mappatura, cfr. Mittelstadt *et al.*, 2016, nonché Tsamados *et al.*, 2021.

minante di un numero relativamente basso di soggetti privati i quali forniscono servizi sia ad altri privati sia a pubbliche amministrazioni, per cui gli Stati si trovano ad essere contraenti di soggetti che forniscono servizi e prodotti informatici estremamente complessi (e normalmente progettati tenendo presenti le legittime finalità di esercizio dell'attività economica privata ma non i principi e i valori dello Stato costituzionale che dovrebbero connotare proprio l'azione pubblica) e che vengono altresì a conoscenza di informazioni riservate in numerosi settori di fondamentale importanza (istruzione, giustizia, sanità, pubblica sicurezza ecc.).

Tuttavia, gli Stati non sono – ovviamente – meri contraenti: devono altresì regolamentare un settore difficilissimo a causa di diversi fattori, fra cui assumono un ruolo primario l'estremo tecnicismo della tematica, la rapida obsolescenza di prodotti e servizi, nonché la loro fornitura su scala globale da parte di aziende che si pongono quali poteri privati in grado di tenere testa a quegli stessi poteri pubblici che hanno consentito loro di prosperare e, in numerosi casi, di acquisire posizioni dominanti o di monopolio.

La Società algoritmica, pertanto, si caratterizza per il ruolo primario di chi detiene il potere tecnologico, potere che si cela, tecnicamente e giuridicamente, dietro all'opacità degli algoritmi e dei codici informatici: moderni *arcana imperii* grazie ai quali i poteri tecnologici hanno prosperato e hanno assunto un ruolo cruciale nella società contemporanea grazie a un tecnicismo estremo e a delle tempistiche ben più rapide di quelle dei vari legislatori.

Così, come osservato in dottrina, una piccola frazione dell'umanità progettata e sviluppa un set di tecnologie che stanno già trasformando la vita quotidiana di tutta la parte restante<sup>5</sup>.

Questa nuova oligarchia, inoltre, non è composta dai saggi filosofi di cui ha scritto Platone, ma soprattutto da pochi soggetti privati che operano per legittime finalità di impresa sfruttando sia le proprie conoscenze e competenze sia gli amplissimi vuoti legislativi, fornendo comunque servizi utili alla collettività<sup>6</sup>.

Anche in ragione di ciò è necessaria una regolamentazione che, pur difendendo l'iniziativa economica privata, la temperi con gli interessi dei singoli e delle collettività, in uno sforzo di riflessione che coinvolga non solo gli operatori e le operatrici del diritto, ma tutte e tutti, vista la trasversalità di questioni che toccano la società nel suo complesso.

Del resto, "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

5. Floridi *et al.*, 2018, p. 699.

6. Oltre ai casi già citati, si pensi anche alle inedite opportunità per la libertà delle persone con disabilità fisiche: su questo profilo cfr. Vantin, 2019.

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'<sup>7</sup>. Si pongono, così, sfide delicatissime dovute a questa "nuova ondata tecnologica"<sup>8</sup>, che può potenzialmente creare nuove forme di vulnerabilità e potenziare quelle esistenti<sup>9</sup>.

Proseguendo ed evolvendo una linea di ricerca già intrapresa<sup>10</sup> e ferma restando la necessità di costruire un *framework* legislativo ponendo dei limiti chiari e invalicabili, così da garantire effettivamente la dignità umana pur promuovendo lo sviluppo di nuove tecnologie che potrebbero avere un impatto benefico, sarà così argomentata una nozione di opacità variabile applicabile ai sistemi intelligenti per contemperare le diverse esigenze che possono sorgere di volta in volta, tenendo comunque presenti i potenziali limiti del diritto nella loro regolamentazione.

## 2. OPACITÀ (E SEGRETEZZA)

La Società algoritmica è caratterizzata, come si è detto, dalla diffusione capillare di sistemi intelligenti che, in modo più o meno silente ma comunque efficace, coadiuvano l'essere umano nel prendere decisioni, sino al punto di sostituirlo in determinati casi.

Pertanto, come osservato da Stefano Rodotà<sup>11</sup>, ci si trova dinanzi a una nuova forma di *arcana imperii* che appare quasi paradossale: le tecnologie dell'informazione e della comunicazione rendono la società più trasparente poiché permettono controlli diffusi su qualsiasi potere, ma gli algoritmi che fondano a loro volta il potere dei soggetti che prestano i relativi servizi tecnologici è totalmente segreto. Appare sempre più attuale, dunque, il riferimento alla "Società delle scatole nere"<sup>12</sup>, in cui i flussi informativi viaggiano sovente all'insaputa dei (trasparenti) consociati grazie ad algoritmi segreti, mentre chi gestisce tali flussi (e crea gli algoritmi) acquisisce un notevole potere economico che può prosperare grazie alla confidenzialità degli algoritmi e dei codici informatici, che a loro volta sono protetti dalle normative in materia di proprietà intellettuale e industriale (che impedisce accessi e utilizzi non autorizzati), da un lato, e dalla stessa complessità dei sistemi informatici (che rende arduo comprenderne in modo preciso e accurato i "comportamenti"), dall'altro.

7. Avitabile, 2017, p. 325.

8. Palazzani, 2020.

9. Cfr. Brighi, 2017; Pastore, 2021; Zanetti, 2019.

10. Fioriglio, 2016.

11. Rodotà, 2012, p. 402.

12. Pasquale, 2015.

In un simile quadro, l'opacità è pressoché assoluta: non è normalmente possibile sapere quali e quante informazioni siano effettivamente acquisite ed elaborate, né come lo siano o controllarne realmente la circolazione (nonostante stringenti normative come il Regolamento UE 679/2016, il Regolamento Generale sulla Protezione dei Dati – di seguito GDPR, che hanno però un impatto settoriale e limitato: v. *infra*). Si crea, ovviamente, un circolo vizioso in assenza di una reale regolamentazione dell'intelligenza artificiale e delle sue applicazioni, cui consegue un potenziamento dell'opacità: negli ultimi anni, fortunatamente, il dibattito in materia e la pervasività di tali applicazioni stanno finalmente, ma tardivamente, destando l'attenzione di inerti legislatori (cfr. parr. 3 e 4).

In linea generale, pare quasi che quest'ultimi abbiano timore di approcciare una tematica aliena, che tuttavia tale non è in quanto caratterizzante quella stessa società che il diritto è chiamato a regolare: forse ciò deriva anche dalla circostanza per cui nella medesima società globalizzata il potere si esplica in un reticolo in cui i nodi principali sono strutturati dal potere economico che, in simili casi, trae la sua linfa vitale dalla tecnologia e dal mercato che quest'ultima alimenta (e che a sua volta sostiene la prima e la fa sviluppare, in un *loop* infinito in cui terzi difficilmente possono inserirsi scardinando posizioni dominanti o di monopolio).

La riflessione su questo aspetto può giovare di quanto argomentato in relazione alle norme opache, che vengono applicate dal giudice senza poterle realmente comprendere ma facendo invece riferimento a ciò che viene detto dagli esperti. In simili ipotesi, l'opacità non è dovuta al tecnicismo in sé, bensì all'asimmetria cognitiva fra i legislatori e i giudici, da un lato, e gli esperti, dall'altro, poiché quando il linguaggio tecnico non giuridico è comprensibile dai primi, il diritto non è opaco ed essi operano nell'ambito dei propri ruoli. Qualora ciò non avvenga, essi non possono compiere una serie di attività intellettuali, di scelte pratiche e di ragionamenti<sup>13</sup>.

Nel caso dei sistemi intelligenti, l'asimmetria cognitiva è massima e riguarda tutti i loro utilizzatori, siano essi diretti (chi si fa coadiuvare da un sistema) o indiretti (chi subisce gli effetti dell'utilizzo del sistema): essi sono opachi perché non comprensibili al di fuori della cerchia di chi li ha creati e li gestisce. Solo il loro output e/o le conseguenze delle loro azioni (materiali o immateriali) vengono inoltre percepite, ma operando in ambienti complessi in cui avvengono infinite interazioni diviene estremamente difficile, e talvolta impossibile, comprendere se in essi vi siano anomalie o se essi compiano azioni riferibili ai propri produttori od utilizzatori; in ipotesi, tali informazioni potrebbero essere ricavate soprattutto dallo studio dei rispettivi codici e dei file di log.

13. Canale, 2015, pp. 94 ss.

Invero, anche chi detiene il potere sui sistemi medesimi può faticare nel comprenderli realmente e renderli trasparenti, a causa di diversi fattori fra cui assumono un ruolo centrale la loro complessità e la loro autonomia.

In relazione al primo profilo, è ovvio che sistemi tanto evoluti siano complessi, in quanto ad essi è demandato lo svolgimento di compiti che richiedono intelligenza. Per quanto concerne il secondo, non v'è dubbio che la loro condotta si realizzi applicando le conoscenze apprese anche automaticamente sulla base degli algoritmi di apprendimento automatico: il che comporta l'imprevedibilità teorica e pratica delle loro azioni<sup>14</sup>, anche grazie alla loro crescente 'intelligenza'<sup>15</sup>.

Sembra dunque necessario, più che opportuno, contrastare la predetta opacità e ciò, auspicabilmente, mediante una regolamentazione che non sia solo formalmente valida, ma anche efficace.

La suddetta necessità deriva, innanzi tutto, dalla considerazione per cui un ambito della società tanto trasversale e importante non possa continuare a essere lasciato a una tecno-regolazione autoreferenziale, in cui la legge è il codice informatico (per usare la celebre espressione di Lawrence Lessig<sup>16</sup> e andando verso la c.d. *lex informatica*<sup>17</sup>) e il legislatore chi lo crea e lo gestisce (con prerogative più ampie di un legislatore nazionale, avendo un dominio sostanzialmente assoluto sullo spazio cibernetico che va a creare e gestire). Inoltre, determinati sistemi intelligenti possono compiere azioni che hanno rilevanza giuridica nella società, il tutto in modo autonomo e al di fuori del diretto controllo del loro produttore, proprietario o utilizzatore (a seconda dei casi e con i diversi privilegi, per utilizzare un termine adoperato in ambito informatico).

È vero che in determinati casi anche il potere economico deve cedere e adeguarsi alle decisioni di quello giudiziario, come nei celebri casi Google Spagna<sup>18</sup> e Schrems I e II<sup>19</sup>, senza che però si abbia, ad oggi, una incidenza concreta sulla riduzione del grado di opacità: il dominio degli spazi cibernetici e dei sistemi intelligenti rimane, ancora, saldamente in capo al primo in relazione a tale, cruciale, aspetto.

Eppure, le azioni dell'agente di un sistema sono percepibili esternamente, al più, solo dopo essere state compiute e talvolta non sono percepibili, come nel caso di "sguardi" indiscreti che non lasciano tracce<sup>20</sup> e quindi il suo ragionamento è ricostruibile, potenzialmente, solo *ex post*. Ciò è essenziale per chi

14. Cfr. Sartor, 2003; Fioriglio, 2015b, 2016.

15. Cfr. però Salardi, Saporiti, 2016, sul "divenire antropomorfo delle macchine".

16. Lessig, 2006.

17. Su cui cfr. Maestri, 2017.

18. Cfr., fra gli altri, Pietropaoli, 2017.

19. Cfr., fra gli altri, Nino, 2020.

20. Sulla sorveglianza cfr. Fioriglio, 2015a; Ziccardi, 2015; Zuboff, 2019.

lo ha creato e lo gestisce, così da poter pianificare e svolgere le operazioni di manutenzione correttiva, adattiva ed evolutiva. È altresì fondamentale, in altra prospettiva, anche per chi lo utilizza e per chi ne subisce gli effetti (tali soggetti non sono necessariamente coincidenti, come nel caso della pubblica amministrazione che adoperi un sistema intelligente per la redazione delle graduatorie; utili spunti possono qui trarsi dalla sentenza del Consiglio di Stato 13 dicembre 2019, n. 8472) ove si verifichino degli illeciti o per comprendere se e come si siano realizzati.

Ciò non è tuttavia agevole, in ragione della complessità dei sistemi informatici e del sempre più frequente ricorso a servizi di cloud computing che rende talvolta praticamente impossibile esercitare un controllo effettivo anche dinanzi a un ipotetico ordine di un giudice. Come dimostra la prassi, comunque, ben difficilmente un giudice imporrà di verificare il codice utilizzato da uno dei poteri informatici dominanti nella prestazione dei propri servizi, perché segreto industriale utilizzato per fornire servizi a milioni o addirittura a miliardi di utenti; e ciò magari per la sproporzione fra il valore della causa (e del diritto tutelato), da un lato, e della proprietà industriale e intellettuale, dall'altro, oltre che per la possibilità di raggiungere un risultato accettabile (dal punto di vista probatorio) con minor sforzo e rischi per tali diritti. Così facendo, però, il potere economico prevale su quello giudiziario e un ambito cruciale della società contemporanea è celato allo sguardo di terzi, incluso il legislatore.

L'opacità potrebbe dunque costituire uno schermo dietro cui celare eventuali anomalie del software, discriminazioni, trattamenti illeciti di dati personali, falle di sicurezza, e così via, non essendo praticamente possibile (o quanto meno estremamente difficoltoso) ricostruire le tracce effettive di ciò che sia realmente accaduto in un determinato sistema (ad esempio, in un assistente vocale, un autoveicolo a guida autonoma o un motore di ricerca). Bisogna però considerare che l'assoluta trasparenza del codice potrebbe agevolare operazioni di plagio del software o il compimento di attacchi informatici (grazie alla possibilità di studiarlo "in chiaro"), riprendendo sul punto la dicotomia fra codice aperto e codice proprietario. In una società complessa come quella contemporanea, tuttavia, pare oramai improcrastinabile il momento di concentrarsi non tanto e non solo sugli estremi, quanto su soluzioni intermedie che permettano di mediare fra essi.

### 3. SPIEGABILITÀ (E TRASPARENZA)

Quanto esposto suggerisce l'adozione di un approccio prudente, finalizzato non a eliminare l'opacità dei sistemi intelligenti, ma piuttosto a renderla variabile nella sua intensità e proporzionale ai rischi che essi pongono, mediante una regolamentazione che preveda una estensione e delle modalità consone alle specifiche tipologie di tali sistemi e al loro ambito di applicazione.



Una opacità relativa, dunque, che è più o meno intensa in base alle posizioni soggettive individuali e collettive in potenziale conflitto così da evitare impostazioni estremistiche, tese verso una trasparenza o una segretezza assolute.

L'imposizione della prima, tra l'altro, comporterebbe una sostanziale revisione delle varie normative nazionali e internazionali che regolamentano la proprietà industriale e intellettuale; avrebbe, inoltre, un impatto devastante su gran parte del settore informatico (che si basa, parzialmente, proprio sulla confidenzialità degli algoritmi e dei codici informatici) e non appare, quindi, una soluzione realmente percorribile. L'attuale *favor* per la seconda, però, dovrebbe trovare dei limiti, dovendosi comunque rendere possibile la c.d. spiegabilità degli output dei sistemi intelligenti quanto meno in casi specifici.

Del resto, la pretesa alla spiegabilità è *giustificata da* vari motivi, fra cui la necessità di evitare decisioni arbitrarie nonché una corretta e precisa imputazione e graduazione della responsabilità (e la sua stessa allocazione in sistemi complessi in cui si ha interazione fra esseri umani e artefatti tecnologici e sociali<sup>21</sup>). Questa pretesa concerne qualsiasi sistema informatico intelligente e diviene tanto più importante quanto più il sistema medesimo costituisce una infrastruttura essenziale o fornisce servizi essenziali o di grande importanza per la società.

Tuttavia, sino ad oggi, l'oscurità e l'opacità degli algoritmi e dei codici informatici hanno sostanzialmente bloccato qualsiasi ambizione di spiegabilità e dunque di poter conoscere quali ragionamenti siano svolti da queste "scatole nere" che si affollano nella Società dell'informazione, per quanto possano registrarsi talune aperture sul punto grazie alla normativa in materia di protezione dei dati personali.

L'art. 22 GDPR, in particolare, prevede che, in un processo decisionale automatizzato e in determinati casi, l'interessato possa avere il diritto di contestare la decisione. Il considerando 71, del resto, prevede che un trattamento automatizzato che produce effetti giuridici (o analoghi) sull'interessato (nei casi in cui viene consentito), "dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto [...] di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione".

Sul punto, il Gruppo di lavoro articolo 29 per la protezione dei dati ha osservato che il titolare dovrebbe comunicare in modo semplice all'interessato la logica o i criteri sui quali si basa l'adozione della decisione, "ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo"<sup>22</sup>.

21. Su questo profilo cfr. Contissa, 2017.

22. Gruppo di lavoro articolo 29 per la protezione dei dati, 2018, p. 32. Cfr. altresì Pagallo, 2018, 2020; Palmirani, 2020.

Del resto, la trasparenza potrebbe essere illusoria anche qualora si potesse visionare tutto il codice informatico adoperato durante i processi decisionali, poiché sarebbe difficilmente comprensibile, anche ove dovesse esserne consentito l'accesso a chi ha il controllo sul medesimo (cui si aggiunge la difficoltà di cristallizzarne una versione a causa di costanti modifiche al codice medesimo).

Anche spiegazioni fornite sulla scorta di quanto osservato dal Gruppo di lavoro articolo 29, ad ogni buon conto, potrebbero essere insufficienti ove non dovesse essere possibile verificarne l'implementazione in un caso concreto. Ragionando in senso contrario, il creatore (o gestore) degli algoritmi godrebbe di una presunzione assoluta di buona fede previo adempimento di un'astratta obbligazione di *disclosure*, cui conseguirebbe una sostanziale irresponsabilità (fatti salvi casi estremi in cui sia possibile dedurre l'inadempimento dall'output del sistema o della piattaforma nel caso in cui dovesse essere palesemente in contrasto con quanto dichiarato).

Negli ultimi anni, però, il quadro sta mutando; la letteratura in materia è oramai sterminata così come i dibattiti e le discussioni a livello della società intera<sup>23</sup>.

Ciò nonostante, i legislatori sono in notevole ritardo: i proclami, i lavori delle commissioni, le raccomandazioni, e così via<sup>24</sup>, non si sono ancora colpevolmente tradotti in testi normativi che effettivamente impongano una evoluzione che si potrebbe definire costituzionalmente orientata della Società algoritmica, che viene ora guidata in modo quasi totalmente esclusivo dai poteri privati a scapito di quelli pubblici. Già le procedure (e i pesi e i contrappesi) che regolano l'azione di quest'ultimi, del resto, appaiono basate su concezioni calate in realtà in cui l'evoluzione avanzava in modo rapido ma non incessantemente vorticoso come accaduto dopo la diffusione del web e il passaggio dalla Società dell'informazione a quella algoritmica.

23. Cfr., in particolare, Floridi *et al.*, 2018, nonché Tsamados *et al.*, 2021; per una panoramica delle soluzioni tecniche che potrebbero essere adoperate al fine di migliorare l'equità, la responsabilizzazione e la trasparenza nei processi decisionali algoritmici, cfr. Lepri *et al.*, 2018.

24. A titolo esemplificativo, si possono qui citare la Comunicazione della Commissione comunicazione della Commissione europea del 25 aprile 2018 su "l'intelligenza artificiale per l'Europa" (237 final), la Comunicazione della Commissione europea dell'8 aprile 2019 su "creare fiducia nell'intelligenza artificiale antropomorfa" (168 final), la relazione del Commissione europea del 19 febbraio 2020 (64 final) "sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità" (in cui si legge, fra l'altro, che "la grande quantità di dati necessari, la dipendenza da algoritmi e l'opacità del processo decisionale dell'intelligenza artificiale rendono più difficile prevedere il comportamento dei prodotti basati sull'intelligenza artificiale e comprendere le possibili cause di un danno"), nonché la Risoluzione del Parlamento europeo del 20 gennaio 2021 su "l'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale (2020/2013(INI))".

#### 4. SFIDE E POSSIBILI SOLUZIONI NELLA SOCIETÀ ALGORITMICA

La Società algoritmica mette ciascuno Stato e ciascuna persona dinanzi a sfide estremamente ardue, dal momento che i processi decisionali e la loro esecuzione vengono affidati sempre più di frequente agli algoritmi: pertanto, agenti software e robot possono addirittura giungere a sostituire, parzialmente o totalmente, l'essere umano nello svolgimento di una molteplicità di operazioni, materiali o immateriali che siano.

Sta così trovando realizzazione un obiettivo che, sin dagli anni Cinquanta e Sessanta, veniva posto nelle pionieristiche riflessioni sull'intelligenza artificiale, all'informatica giuridica e alle sue applicazioni.

Ogni medaglia ha, però, il suo rovescio. Già quanto sin qui discusso evidenzia una molteplicità di problemi che rendono sempre più stringenti ed attuali alcune domande.

Innanzitutto, si pone il problema di una (tecno)regolazione<sup>25</sup> che consenta di raggiungere un equilibrio sostenibile fra progresso tecnologico e tutela dell'iniziativa economica privata, da un lato, e progresso umano e tutela dei diritti, dall'altro – il tutto mediante una normativa che non rimanga lettera morta, ma che possa invece orientare concretamente il percorso dell'intelligenza artificiale verso una Società in cui gli algoritmi (e coloro i quali li controllano e li adoperano, a seconda dei casi) non siano al di sopra della legge. Non è un compito facile e non può essere svolto da un unico legislatore, dal momento che molti sistemi operano su scala globale, così come i soggetti che detengono il potere su di essi.

In linea generale, oltre alla “tradizionale” difficoltà appena citata (che caratterizza l'ambito informatico-giuridico sin dai suoi primordi), se ne aggiungono altre, fra cui hanno un ruolo primario quelle della differente velocità del diritto e della tecnologia (per cui il primo rincorre la seconda), del tecnicismo delle regole (che potrebbe oltretutto aumentare il rischio della loro precoce obsolescenza) e della valutazione della loro applicazione (demandata a soggetti che abbiano determinate conoscenze e competenze).

In tale quadro, la dicotomia fra opacità e spiegabilità appare cruciale, in quanto la segretezza che contraddistingue la prima può impedire l'applicazione di eventuali norme in materia e privare di tutela chi viene danneggiato dagli algoritmi adoperati (da chi viene escluso da una graduatoria a chi subisce il rifiuto di una richiesta di mutuo, da un sito di commercio elettronico che viene nascosto da un motore di ricerca web a un medico che viene indotto in errore da un sistema di supporto alle decisioni, e così via).

Non appare dunque più procrastinabile una regolamentazione effettiva ed efficace della Società algoritmica sotto questo fondamentale aspetto, evitando

25. Cfr. Amato Mangiameli, 2017.

tuttavia soluzioni troppo nette e rigide in ragione dei diversi e contrastanti interessi coinvolti nonché della molteplicità delle fattispecie ipotizzabili.

Così, da un lato vi sono le legittime pretese di chi crea e gestisce gli algoritmi, poiché essi possono contribuire all'evoluzione tecnologica della società e quindi migliorare la qualità della vita dei consociati sotto numerosi profili, potendosi tendere verso una sanità migliore e più efficiente, la deburocratizzazione, mezzi di trasporto più sicuri, la personalizzazione di servizi di varia tipologia; dall'altro, vi sono i diritti, anche fondamentali, di chi utilizza tali sistemi (ad esempio, un istituto bancario o una struttura sanitaria) o comunque sopporta le conseguenze del loro utilizzo (ad esempio, la clientela dell'istituto bancario o gli assistiti e le assistite del servizio sanitario).

Si può dunque proporre una soluzione: una opacità bilanciata, parziale e condizionata, differenziata in base a ciascuna categoria di prodotto o servizio, prendendo altresì in esame i relativi ambiti di applicazione.

L'opacità, così, costituirebbe il punto di equilibrio fra la segretezza che oggi contraddistingue la tecnologia informatica (e gli algoritmi) e la trasparenza assoluta che molto difficilmente potrebbe essere imposta a chi li crea e li controlla.

Pertanto, si propone di superare il paradigma della segretezza assoluta del codice per contemperarlo con quello della trasparenza, mediante l'applicazione di criteri che permettano di bilanciarle tenendo conto di metodi e strumenti concretamente utilizzabili. La valutazione potrebbe essere svolta partendo dalla considerazione di due macro-elementi: l'ambito di applicazione del sistema o della piattaforma "intelligente", da un lato, e le distinte posizioni del detentore del potere di controllo degli algoritmi, dell'utilizzatore del sistema o della piattaforma che tali algoritmi eseguono e, infine, dei soggetti (persone fisiche o giuridiche) che ne subiscono, o ne potrebbero subire, le conseguenze.

Più specificatamente, l'ambito di applicazione orienta le successive operazioni concettuali e pratiche, dovendosi guardare ai potenziali effetti sui diritti delle persone e dei gruppi sociali. Quanto più essi saranno potenzialmente severi, tanto meno "opaco" dovrebbe essere il codice; basti pensare, in tal senso, al settore sanitario e a terapie sui singoli o a screening e ricerche su gruppi di popolazione; o, ancora, alla lotta alla criminalità e al riconoscimento facciale adoperato dalle forze di polizia.

Quanto alle posizioni soggettive, può argomentarsi che tanto più chi controlla gli algoritmi gode di una posizione dominante o di monopolio quanto più diminuirà l'opacità; il medesimo rapporto di proporzionalità può applicarsi anche in relazione alle persone fisiche o giuridiche (quest'ultime escluse, com'è noto, dalla protezione riservata dal GDPR) facendo riferimento al rango e all'importanza dei loro diritti in gioco e partendo, in relazione alle prime, non dalla loro qualità di consumatore, professionista o utente, bensì di essere umano (con tutto ciò che ne consegue in ordine al rispetto della dignità di chi è

persona, prima di essere consumatore). L'utilizzatore dei sistemi si trova fra queste due figure, ma può avere un legittimo interesse alla trasparenza dei sistemi utilizzati sia per esimersi, eventualmente, da responsabilità sia per controllare concretamente i flussi informativi che riguardano la propria attività.

Alle questioni qui citate si aggiunge altresì quella, cruciale, della sicurezza dei sistemi e delle piattaforme che eseguono gli algoritmi (in quanto eventuali falle potrebbero "indurli" in errore, con conseguenze anche molto gravi in base al loro ambito di applicazione). Una soluzione potrebbe consistere nell'imporre la fornitura di garanzie esplicite per un periodo predeterminato, cui accompagnare l'obbligo del deposito del codice presso banche date pubbliche costituite *ad hoc*, che siano ad accesso riservato e che siano protette in massimo grado.

In conclusione, le sfide che si pongono dinanzi ai legislatori e al *demos* sociale e politico appaiono numerose e delicate. Non v'è dubbio, però, che la costruzione di una Società algoritmica possa e debba avvenire nel rispetto, e non nella violazione, dei principi e dei valori degli Stati costituzionali: il che non può avvenire seguendo la massima del *laissez-faire* e tutelando concretamente più gli *arcana imperii* che i diritti fondamentali.

#### RIFERIMENTI BIBLIOGRAFICI

- Amato Mangiameli, A.C. (2017). *Tecno-diritto e tecno-regolazione*. Spunti di riflessione. *Rivista di filosofia del diritto*, speciale, 87-112.
- Id. (2019). Algoritmi e big data. Dalla carta sulla robotica. *Rivista di filosofia del diritto*, 1, 122-123.
- 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.
- Brighi, R. (2017). La vulnerabilità nel cyberspazio. *Ars interpretandi*, 1, 81-94.
- Canale, D. (2015). Norme opache. Il ruolo degli esperti nel ragionamento giuridico. *Rivista di filosofia del diritto*, numero speciale, 93-124.
- Casadei, T. (2017). Mondi della vita, rete, trasformazioni del diritto. *Ars interpretandi*, 1, 7-14.
- Contissa, G. (2017). Automation and liability. An analysis in the context of socio-technical systems. *I-lex*, (11)1, 17-45.
- Fioriglio, G. (2015a). Controllo e sorveglianza nella società dell'informazione. *Studi sulla questione criminale*, 2-3, 7-24.
- Id. (2015b). La "dittatura" dell'algoritmo: motori di ricerca web e neutralità della indicizzazione. Profili informatico-giuridici. *Bocconi Legal Papers*, 5, 113-139.
- Id. (2016). Opacità dei sistemi intelligenti e sicurezza informatica: un difficile equilibrio fra regolazione e tecno-regolazione. *Rivista elettronica di Diritto, Economia, Management*, 3.

- Floridi, L., Cows, 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, <https://doi.org/10.1007/s11023-018-9482-5>.
- Floridi, L., Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A*, <https://doi.org/10.1098/rsta.2016.0360>.
- Gruppo di lavoro articolo 29 per la protezione dei dati (2018). *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*. WP 251, rev. 01 (versione emendata).
- Lepri, B., Oliver, N., Letouzé, E., Pentland, A., Vinck, P. (2018). Fair, Transparent, and Accountable Algorithmic Decision-making Processes. The Premise, the Proposed Solutions, and the Open Challenges. *Philosophy & Technology*, 31, 611-627.
- Lessig, L. (2006). *Code. Version 2.0*. Basic Books.
- Maestri, E. (2017). *Lex informatica* e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio. *Ars interpretandi*, 1, 15-28.
- Mittelstadt, B.T., Allo, P., Taddeo, M., Wachter, S., Floridi, L. (2016). The ethics of algorithms. Mapping the debate. *Big Data & Society*, 1-21, <https://doi.org/10.1177/2053951716679679>.
- Nino, M. (2020). La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo. *Diritti umani e diritto internazionale*, 3, 733-759.
- Pagallo, U. (2018). Algo-Rhythms and the Beat of the Legal Drum. *Philosophy & Technology*, 31, 507-524.
- Id. (2020). Algoritmi e conoscibilità. *Rivista di Filosofia del diritto*, 1, 93-106;
- Palazzani, L. (2020). *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*. Studium.
- Palmirani, M. (2020). Big data e conoscenza. *Rivista di Filosofia del diritto*, 1, 73-91.
- Pasquale, F. (2015). *The Black Box Society. The Secret Algorithms that Control Money and Information*, Harvard University Press.
- Pastore, B. (2021). *Semantica della vulnerabilità, soggetto, cultura giuridica*. Giappichelli.
- Pietropaoli, S. (2017). La rete non dimentica. Una riflessione sul diritto all'oblio. *Ars interpretandi*, 1, 67-80.
- Rodotà, S. (2012). *Il diritto di avere diritti*. Laterza.
- Salardi, S., Saporiti, M. (2020). Perché l'IA non deve diventare Persona. Una critica all'ineludibile 'divenire antropomorfo' delle macchine. *Le tecnologie 'moralì' emergenti e le sfide etico-giuridiche delle nuove soggettività*, a cura di S. Salardi, M. Saporiti (52-74). Giappichelli.
- Sartor, G. (2003). Gli agenti software e la disciplina giuridica degli strumenti cognitivi. *Il diritto dell'informazione e dell'informatica*, (19)1, 55-87.
- Sartor, G. (2020). Introduzione. *Rivista di filosofia del diritto*, IX(1), 65-72.
- Tsamados, A., Aggarwal, N., Cows, J., Morley, J., Roberts, H., Taddeo, M., Floridi, L. (2021). The ethics of algorithms: key problems and solutions. *AI & Society*, <https://doi.org/10.1007/s00146-021-01154-8>.

- Vantin, S. (2019). Automobili a guida autonoma: un'inedita opportunità per le persone con disabilità fisiche? In S. Scagliarini (a cura di), *Smart roads e driverless cars. Tra diritto, tecnologie, etica pubblica* (55-64). Giappichelli.
- Zanetti, Gf. (2019). *Filosofia della vulnerabilità. Percezione, discriminazione, diritto*. Carocci.
- Ziccardi, G. (2015). *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*. Cortina.
- Zuboff, S. (2019). *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri* (trad. it.). Luiss University Press.

