NOMOS
Le attualità nel diritto

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale

Casimiro Coniglione*

L'utilizzo dei *big data* in ambito politico-elettorale e il loro impatto sulla democrazia rappresentativa**

SOMMARIO: 1. Premessa: l'emersione dei *big data*. Tentativo di definizione, formazione e tipi di analisi. – 2. L'utilizzo dei *big data* come punteggio di gradimento per un candidato e la c.d. targetizzazione. – 3. *Big data* e profilazione: un contrasto con l'art. 5 del GDPR? - 3.1. Il *microtargeting* e la profilazione psicometrica. – 4. Il diritto alla spiegabilità e alla conoscenza dei processi automatizzati. – 5. Dalla democrazia rappresentativa alla postdemocrazia. – 6. Riflessioni conclusive.

1. *Premessa: l'emersione dei* big data*. Tentativo di definizione, formazione e tipi di analisi*

I periodi storici generalmente vengono ricordati attraverso etichette che riassumono le caratteristiche socio-culturali dell'epoca. Oggi, è corretto definire l'attuale società come la società dei dati, poiché vengono prodotti circa 2,5 quintilioni di byte di dati informatici. È stato affermato – a questo proposito – che l'attuale società vive una rivoluzione dell'informazione, cambiandone la comprensione e l'interpretazione della stessa realtà[1].

Com'è noto, tale massiccia formazione di enormi volumi di dati è conosciuta con il nome di *big data*. Quest'ultimi, a differenza dei *small data*, non hanno una definizione precisa né a livello legislativo[2] né a livello dottrinale, in quanto vi sono numerose definizioni che si diversificano in base alla disciplina di riferimento. Si consideri, altresì, che lo studio del fenomeno ha natura interdisciplinare in ragione delle sue molteplici implicazioni.

* Dottorando di ricerca in Lavoro, Sviluppo e Innovazione – Università degli Studi di Modena e Reggio Emilia; Fondazione Marco Biagi.

** Contributo sottoposto a *peer review*.

[1] «Non vi è un termine per indicare questa nuova forma radicale di costruzione, cosicché possiamo usare il neologismo *riontologizzare* per fare riferimento al fatto che tale forma non si limita solamente a configurare, costruire o strutturare un sistema (come una società, un'auto o un artefatto) in modo nuovo, ma fondamentalmente comporta la trasformazione della sua natura intrinseca, vale a dire della sua ontologia. In tal senso, le ICT non stanno ricostruendo il nostro mondo: lo stanno riontologizzando», così L. FLORIDI, *La rivoluzione dell'informazione*, Codice Edizioni, Torino, 2012, 16.

[2] F. FAINI, *Big data*: *aspetti e problemi giuridici*, in *Rivista elettronica di diritto*, *economia e management*, 3, 2016; Id., Data Society. *Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè, Milano, 2019, 160; F. FAINI - S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Giappichelli, Torino, 2021, 404.

ISSN 2279-7238

Ciò premesso, i *big data* potrebbero essere definiti come «una raccolta di dati informativi così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore e conoscenza[3]». Volume, velocità e varietà costituiscono un primo modello denominato 'modello 3V', che fu elaborato la prima volta dall'analista Doug Laney nel 2001[4].

In breve: per velocità si intende la capacità di acquisizione, di analisi in tempo reale o ad alta velocità[5] (se l'analisi non è effettuata nel breve periodo il dato diventa obsoleto); il volume indica l'immensa quantità di memoria occupata dai suddetti dati che vanno dai *petabytes* ai *zettabytes*[6], sono dimensioni che non possono essere gestite con *database* tradizionali; terza – ed ultima – V è la varietà che consiste nell'*eterogeneità*, ossia la diversa numerosità delle fonti di provenienza e formazione dei dati stessi.

Gli utenti – per usufruire dei diversi servizi nel web a titolo gratuito – cedono volontariamente o involontariamente i loro dati. Tra la cessione dei dati volontaria è sicuramente interessante sottolineare l'iscrizione ai social network oppure alle piattaforme di *e-commerce*; per la cessione di dati in maniera più o meno consapevole si può citare il caso dei GPS, dei rilevatori biometrici e i movimenti bancari; nei casi in cui siano soggetti pubblici a contribuire alla formazione dei *big data*, essi sono condivisi – certe volte – come il modello degli *open data*[7]; sussistono, infine, anche casi in cui la registrazione e formazione dei *big data* è automatica attraverso i *cookies*[8].

Delineata la definizione e la formazione dei *big data* è possibile esaminare le diverse analisi che si possono intraprendere attraverso i *big data*: l'analisi descrittiva, l'analisi predittiva e l'analisi prescrittiva (c.d. *big data analytics*).

All'interno della prima categoria d'analisi, ossia quella descrittiva, rientrano tutte quelle analisi orientate a descrivere situazioni attuali (o passate) e visualizzare – in modo sintetico e grafico – i principali indicatori di prestazione.

---

[3] A. DE MAURO - M. GRECO - M. GRIMALDI, *A formal definition of* big data *on its essential features*, in *Library review*, 3, 2015, 122; altresì, si veda la definizione dello standard ISO/IEC/ 20546:2019 *Information technology – Big data – Overview and vocabulary*, consultabile al sito dell'*International Organisation of Standardization*. Si sottolinea anche la definizione data dal Parlamento Europeo «*big data refers to collection, analysis and the recurring accumulation of large amount data*, *including personal data*, *from a variety sources*, *which are subject to automatic processing by computer algorithms and advanced data-processing techniques using both stored and streamed data in order to generate certain correlations*, *trends and patterns* (*big data analytics*)», European Parliament, *Report on fundamental rights implications of big data*, cit., par. A).

È da sottolineare, inoltre, che la letteratura scientifica si è spinta oltre il modello tradizionale delle 3V. Infatti, molti autori hanno aggiunto nel corso del tempo diverse V come la veridicità (i dati devono essere veritieri) e il valore (i dati devono avere un valore economico o quantomeno quantificabile) in tal senso cfr. T. DE MAURO, *I* big data *tra protezione dei dati personali e diritto della concorrenza*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali*, Giuffrè, Milano, 651-654.

[4] D. LANEY, *3D Data Management*: *Controlling Data Volume*, *Velocity and Variety*. META Group Research.

[5] Cfr. G. D'ACQUISTO - M. NALDI, Big data *e* privacy by design. *Anonimizzazione, pseudoanonimizzazione*, *sicurezza*, Giappichelli, Torino, 2017, 6.

[6] In tal senso, R. BRIGHI, *Il ruolo dei dati informatici nella costruzione della realtà. Tra vulnerabilità e esigenza di trasparenza*, Roma, Aracne, 2016, 41; nel caso dei *big data* i volumi sono sull'ordine di *zettabyte* e *yottabyte*, destinati a crescere e ad arrivare nel tempo a numeri sempre più grandi, sull'ordine di *brontobyte* e *gegobyte*, cfr. V. MAYER-SCHONERGER - K. CUKIER, Big data: *Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, Milano, 2013, 47; G. SARTOR, *L'informatica giuridica e le tecnologie dell'innovazione*, Giappichelli, Torino, 2016, 187-188.

[7] Cfr. S. FARO - N. LETTIERI, Big Data: *una lettura informatica giuridica*, in L. LOMBARDO VALLAURI (a cura di), *Scritti in onore di Luigi Lombardo Vallauri*, Wolters Kluwer-Cedam giuridica, Milano, 2016, 508.

[8] I *cookies* (dall'inglese biscotti), com'è noto, sono frammenti di dati sugli utenti memorizzati sul computer e utilizzati per implementare la navigazione. I cookie, anche conosciuti come *cookie* HTTP, web, Internet o del browser, vengono creati dal server e inviati nel browser dell'utente. Questo scambio di informazioni consente ai siti di riconoscere il computer dell'utente e inviare informazioni personalizzate in base alle sessioni di navigazioni.

L'analisi predittiva, invece, consente di prevedere in anticipo l'accadimento di eventi futuri, utilizzando tecniche di regressione, *forecasting*, *machine learning* e *data mining*. La previsione dei futuri eventi è stimata in termini di probabilità.

Infine, la terza – e ultima – analisi effettuata grazie ai *big data* è quella prescrittiva, che permette di quantificare l'effetto delle future decisioni e consigliare i possibili risultati prima dell'adozione delle decisioni. In sostanza, quest'analisi non solo permetterà di prevedere l'avvenimento, ma spiegherà la motivazione per cui si verificherà un determinato evento e – eventualmente, qualora sia necessario – come rettificarlo.

Queste *big data analytics* non sarebbero possibili senza la presenza dell'algoritmo[9].

Nel processo di estrazione del valore, gli algoritmi si basano su correlazioni che emergono dall'analisi dei dati e che sono capaci di strutturare le informazioni e di automatizzare i processi. Infatti, è stato correttamente affermato che «dietro formule e modelli matematici, dietro diagrammi e procedimenti formali, si celano meccanismi di alterazione dell'informazione e di condizionamento dell'azione[10]»: l'algoritmo non è neutro[11].

Tanto premesso, questo contributo analizza l'utilizzo dei *big data* in ambito politico-elettorale in quanto può notarsi come la profilazione automatizzata degli utenti svolta dalle c.d. Big tech sia idonea a orientare la condotta degli utenti medesimi; di qui il rischio, fra l'altro, che la democrazia rappresentativa si trasformi in una postdemocrazia, in cui viene meno la procedura egualitaria del demos e (nel contempo) viene meno il concetto stesso di democrazia, intesa come pluralismo e incertezza istituzionalizzata[12].

2. *L'utilizzo dei big data come punteggio di gradimento per un candidato e la c.d. targetizzazione*

Prima di procedere all'analisi della profilazione come strumento di targetizzazione, manipolazione. schedatura e sorveglianza degli utenti, pare opportuno soffermarsi su uno studio condotto da David Nickerson e Todd Rogers nel 2014, premettendo, tuttavia, che l'utilizzo dei *big data* in ambito politico-elettorale può essere ricondotto (in una sua prima fase) al 2012. Non è

[9] Si definisce algoritmo una sequenza finita di operazioni elementari, eseguibili facilmente da un elaboratore che, a partire da un insieme di dati I (input), produce un altro insieme di dati O (output) che soddisfano un preassegnato insieme di requisiti. Spesso. i requisiti vengono distinti in due categorie: i vincoli, ossia requisiti che devono essere soddisfatti in ogni caso, e gli obiettivi, ossia requisiti che devono essere soddisfatti il meglio possibile secondo un qualche criterio specificato. Un algoritmo è caratterizzato essenzialmente da due elementi: la complessità computazionale, relativa al numero di operazioni elementari necessarie per produrre l'output e l'approssimazione relativa a quanto vengono soddisfatti gli obiettivi secondo il criterio specificato.

[10] A.C. AMATO MANGIAMELI, *Algoritmi e* big data. *Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 1, 2019, cit., 109. La letteratura scientifica sulle discriminazioni algoritmiche (per genere, razza, orientamento sessuale etc.) è assai estesa, si veda S. VANTIN, *Il diritto antidiscriminatorio nell'era digitale. Potenzialità e rischi per le persone*, *la pubblica amministrazione*, *le imprese*, Wolters Kluwer-Cedam giuridica, Milano, 2021.

[11] A questo proposito, tra i tanti contributi, si veda G. FIORIGLIO, *La "dittatura": motori di ricerca web e neutralità della indicizzazione. Profili informatico-giuridici*, in *Bocconi Legal Papers*, 5, 2015, 113-139; L. FLORIDI, M. TADDEO, What is data ethics? *Philosphical Transcations of the Royal Society A*, consultabile in https://doi.org/10.1098/rsta.2016.0360

[12] L'idea che la democrazia non sia basata solo sulla libertà e l'eguaglianza, ma che abbia una sua essenza appunto di incertezza istituzionalizzata è ripresa assai bene dal politologo tedesco-americano J.W. MULLER, *Democracy Rules. Freedom*, *Equality*, *Uncertainty*, Macmillan Publishers, London, 2021.

un caso, infatti, che Nancy Scola usò il soprannome *big data president* per Barack Obama[13]. In breve, la strategia di Obama era finalizzata all'invio di messaggi personalizzati (a discapito dei messaggi generici) agli utenti: concentrò tutti i dati all'interno di un unico archivio e riuscì a dirottare le preferenze degli indecisi verso le sue posizioni[14]. È particolarmente interessante notare che all'inizio della campagna per la rielezione, lo staff del candidato presidente abbia cercato con insistenza dei *data scientist* capaci di lavorare con ingenti mole di dati e di fare, tra l'altro, analisi predittive[15].

In forza di ciò, come anticipato *ut supra,* Nickerson e Rogers in un *paper* studiarono la funzione predittiva dei *big data* in ambito politico-elettorale, classificando tre classi di punteggi[16].

La prima classe di punteggi sono i punteggi comportamentali e servono ad analizzare il comportamento degli elettori in passate campagne elettorali; calcolano le probabilità con cui gli utenti sono disposti a fare politica attiva. I risultati servono – sostanzialmente – per verificare la futura affluenza alle urne, ma anche per capire chi è disposto a contribuire economicamente ad una campagna elettorale.

La seconda classe di punteggi sono i punteggi di supporto ed è il passaggio successivo rispetto ai punteggi comportamentali, perché si cerca di prevedere le preferenze: attraverso i social network, o in via indiretta, si chiederà se gli utenti (*rectius*, elettori) saranno disposti a votare uno specifico candidato e le risposte date saranno usate per sviluppare modelli predittivi per le preferenze. I punteggi variano da uno a zero. Se il punteggio è zero, è assai improbabile che il candidato abbia un gradimento: nessuno sarà disposto ad esprimere la preferenza nei suoi confronti; se il punteggio, invece, è cento il candidato è ben apprezzato dagli utenti; se il punteggio è intermedio, ossia varia tra zero e cinquanta, partirà l'opera di 'monitoraggio' e di profilazione per la massa di utenti indecisi.

La terza – ed ultima – classe di punteggi sono i punteggi di reattività e hanno la funzione specifica di quantificare l'emotività degli utenti sulla base dei messaggi di una determinata campagna elettorale: più il messaggio è gradito dagli utenti, più probabilità ci sono che il candidato riesca nel suo *rush* finale. In effetti, secondo gli autori di questo studio, «*campaign data analysts must still think critically and creatively about what variables sensibly relate to their outcomes of interest to generate predictive scores with external validity required by campaigns*[17]».

Da questo pioneristico studio del 2014 possiamo dedurre importanti conseguenze: in primo luogo, ormai è fondamentale avere a disposizione un team di *data scientist* in grado di estrarre le informazioni necessarie all'interno di una squadra per le campagne elettorali; in secondo luogo, bisogna attuare una pratica d'identificazione mirata con la trasmissione di messaggi a utenti

---

[13] N. SCOLA, *Obama, the "big data" president*, Washington post, 14.06.2013, consultabile in https://www.washingtonpost.com/opinions/obama-the-big-data-president/2013/06/14/1d71fe2e-d391-11e2-b05f-3ea3f0e7bb5a_story.html (ult. consultazione 28 agosto 2022).

[14] Cfr. G. ZICCARDI, *Tecnologie per il potere. Come usare i social network in politica*, Raffaele Cortina Editore, Milano, 2019, 100-101.

[15] C. O'NEIL, *Armi di distruzione matematica. Come i* big data *aumentano la diseguaglianza e distruggono la democrazia*, Bompiani, Milano, 2016, 273-274.

[16] D.W. NICKERSON - T. ROGERS, *Political campaigns and Big data, in Journal of Economic Perspectives*, Vol. 28, 2, 2014, 54-55.

[17] «Gli analisti dei dati devono ancora pensare in modo critico e creativo a quali variabili si riferiscono in modo sensato ai risultati di interesse per generare punteggi predittivi con la validità esterna richiesta delle campagne» in D.W. NICKERSON - T. ROGERS, *Political campaigns and* Big data, cit., 55.

(elettori) dove i contenuti del messaggio siano graditi, perché perfettamente in linea con ciò che pensano. Più utenti si troveranno e più le probabilità della predizione si concretizzeranno.

Si osservi, peraltro, che il compianto Stefano Rodotà aveva teorizzato come «questa tendenza è destinata ad accentuarsi con il progredire delle analisi e delle preferenze dei cittadini e della costruzione di profili individuali, familiari e di gruppo»[18]. Evidentemente, sussistono strumenti in grado di manipolare e fuorviare il proprio comportamento.

Ciò premesso, si può analizzare in cosa consiste la profilazione e verificare il disposto normativo del GDPR 2016/679.

3. Big data *e profilazione: un contrasto con l'art. 5 del GDPR?*

Gli utenti, com'è noto, per usufruire di vari servizi a titolo gratuito, cedono i propri dati volontariamente o involontariamente; allo stato attuale, «la persona non solo è sempre più trasparente ma anche sempre più digitalizzata e profilata»[19]. Trasparente nel senso che è sempre più conoscibile, viene meno la sua intimità, e, allo stesso tempo, sempre più manipolabile.

La profilazione – che deriva dal termine 'profilare' ossia tracciare contorni – degli utenti, grazie ai dati personali, permette di classificare, valutare e prevedere i comportamenti. In linea di massima, un sistema di profilazione prevede che l'utente con determinate caratteristiche possa, con una certa probabilità, possederne altre. Una correlazione può anche riguardare la propensione di un individuo, o degli individui, a rispondere in determinati modi a diversi stimoli: è indubbio che in questo modo si stia innescando un meccanismo per favorire un comportamento desiderato. Inoltre, la profilazione permette la creazione di conoscenza predittiva e di segmentazione, ossia la suddivisione degli individui in base al loro comportamento[20].

I *big data*, in modo particolare, hanno la capacità di ampliare la profilazione, perché grazie all'automazione si riducono i costi per la raccolta, l'archiviazione e l'elaborazione delle informazioni: si apre così la strada verso una forma di sorveglianza persistente e pervasiva, in cui gli utenti sono sottoposti a forti pressioni psicologiche: da un lato, attraverso raffinate tecniche di profilazione, si suddividono gli utenti in base a caratteristiche omogenee; dall'altro, è inevitabile che si sia formata – come bene argomentato dalla letteratura scientifica – uno sdoppiamento della personalità, ossia la personalità fisica è totalmente diversa rispetto alla personalità virtuale. Infatti, in molti casi le opinioni, i sentimenti e le idee manifestate, ad esempio, presso un social network, se decontestualizzate, sono assai diverse rispetto all'identità reale.

A questo punto, però, pare emergere una tensione tra i *big data* e il GDPR.

---

[18] S. RODOTÀ, *Iperdemocrazia. Come cambia la sovranità democratica con il web*, Laterza, Roma-Bari, 2013, cit., 12.

[19] G. FIORIGLIO, *Sorveglianza e controllo nella società dell'informazione*, in *Nomos. Le attualità del diritto*, 2, 2014, cit., 1.

[20] «La profilazione è una tecnica di trattamento (parzialmente) automatizzato di dati personali e/o non personali, finalizzata alla creazione di conoscenza predittiva mediante la scoperta di correlazione tra i dati e la costruzione di profili, che possono essere poi utilizzati per assumere decisioni», così F. BOSCO - N. CREEMERS -V. FERRARIS - D. GUAGNIN- B.J. KOOPS, *Profiling technologies and fundamental rights*: r*egulatory challenges and perspectives from European Data Protection Autthorities,* in *Reforming European data protection law,* Dordecht*,* 2015, cit., 8; si veda anche V. FERRARIS, *La profilazione e i suoi rischi*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie*, Aracne, Roma, 2015, 70-72 in cui vengono descritti anche diversi significati della profilazione (in senso criminale, economico, sociale etc.).

L'art. 5 del GDPR, invero, esprime l'esigenza della limitazione della finalità: la raccolta dei dati deve avvenire per finalità determinate, esplicite, legittime, e con la minimizzazione dei dati, ovverosia i dati devono essere adeguati, limitati e pertinenti a quanto necessario rispetto alle finalità per le quali sono trattati.

È evidente che i *big data* – proprio grazie alla profilazione e dunque alla capacità di estrarre correlazioni – danno una potenziale rilevanza a qualsiasi dato per finalità non determinate[21].

Per profilazione, ai sensi dell'art 4 del GDPR, tra le altre cose, si intende «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

Per limitare questa 'sorveglianza' sussistono due livelli di intervento: il primo è quello giuridico, in cui il GDPR ha rafforzato il consenso dei soggetti coinvolti per il trattamento dei dati personali; il secondo livello di intervento, sempre previsto all'interno del GDPR, è quello tecnologico – l'art. 25 del GDPR prevede l'approccio della *privacy by design and by default* e mira a garantire attraverso impostazioni predefinite e sistemi tecnologici di alto livello il massimo livello di protezione dei dati[22].

Nonostante le positive intenzioni del GDPR, è innegabile che le soluzioni non siano la 'cura' verso le monopolizzazioni delle grandi *Tech*. I social hanno reagito facendo poco comprensibili i *consent* per i propri servizi, estrapolando così il consenso dell'interessato e vanificando la centralità del consenso dell'interessato al trattamento dei dati.

3.1. *Il* microtargeting *e la profilazione psicometrica*

La possibilità di influenzare un comportamento individuale avviene mediante l'invio di pubblicità micromirata (c.d. *microtargeting*). A sua volta, la possibilità di inviare pubblicità mirata conferisce un vantaggio competitivo per le piattaforme o per le società che si occupano di consulenza politica. Infatti, l'invio di informazioni mirate e gradite al destinatario fa sì che il destinatario resti all'interno di una bolla (c.d. *filter bubble*[23]), in cui non ha la possibilità ad accedere a informazioni diverse: in sostanza, viene meno il c.d. pluralismo dei contenuti informativi.

È noto che l'esempio più estremo di *microtargeting* è avvenuto nel corso della Brexit e nelle presidenziali degli Stati Uniti nel 2016, ossia il c.d. caso della Cambridge Analytica[24].

---

[21] G. SARTOR, op. cit, 189.

[22] Cfr. E. ORRÙ, *Verso un nuovo Panottico? La sorveglianza digitale*, in TH. CASADEI - S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters-Kluwer, Milano, 2021, 213-214.

[23] Il termine è stato coniato, per la prima volta, da E. PARISER, *The Filter Bubble*: *What The Internet is Hiding From you*, Londra, Penguin Books, 2011, e fa riferimento alla bolla informativa dove gli utenti restano intrappolati a causa della profilazione e personalizzazione estrema dei risultati di ricerca.

[24] Per un'ampia ricostruzione della vicenda si veda: B. KAISER, *La dittatura dei dati*, Milano, Harper Collins, 2019. Kaiser è stata un dirigente della società *Cambridge Analytica* e ha messo in luce non solo casi come la Brexit o le elezioni presidenziali statunitensi del 2016, ma anche altri casi come le elezioni presidenziali in Nigeria del 2015 e altri casi in America Centrale.

Ciò che interessa, in questa sede, è la profilazione psicometrica e un suo applicativo: il sistema OCEAN. Questo sistema di profilazione permetteva di creare un profilo psicologico (e quindi una correlazione) degli utenti e di prevedere, con ottime percentuali di probabilità, quale messaggio avrebbe potuto convincere uno specifico utente (o meglio, un elettore indeciso).

Un'annotazione è d'obbligo: la psicometria è quella scienza che – tramite i metodi d'indagine psicologica – tende al raggiungimento di valutazioni quantitative del comportamento umano.

Com'è noto, la società inglese raccolse i dati all'insaputa di Facebook attraverso l'app *this is your digitale life* (ideata da Alexander Kogan) e creò un *database* con i dati degli utenti privati: si stima che la società abbia avuto i dati di ottantasette milioni di utenti[25]. Dopo aver raccolto i dati, la società ideò il sistema OCEAN (*openess*, *conscientiounsness*, *extraversion*, *availability*, *neurosis*).

È possibile scomporre e analizzare ogni singola lettera: con *openess* era possibile analizzare il comportamento di un utente aperto verso nuove esperienze; *conscientiounsness* analizzava l'attitudine del soggetto alla pianificazione o alla spontaneità; *extraversion* verificava se l'utente avesse la tendenza a stare in gruppo o preferiva la solitudine; *availability* quantificava la "generosità" del soggetto, ossia la capacità dell'utente nel prendersi cura dei bisogni altrui; con *neurosis* (che probabilmente è la parte più interessante) si stabiliva quanto la paura potesse incidere sulla capacità di giudizio dell'utente.

Attraverso l'analisi e la successiva correlazione dei profili psicologici, la società C.A. identificò gli utenti indecisi, sottoponendoli a una pubblicità mirata (appunto *microtargeting*, elemento centrale in ottica predittiva e di anticipazione della volontà) con contenuti a loro graditi e basati sulle loro emozioni.

Aldilà delle prevedibili reazioni dopo lo scandalo[26], è interessante notare come, da un lato, il raccogliere i dati (e farli elaborare dall'algoritmo) ha reso il fenomeno del *microtargeting* più attuale che mai e, dall'altro lato, attraverso i *big data* si ha la capacità di creare profili assai precisi degli utenti: la possibilità di inviare pubblicità mirata permette di poter influenzare, predire e – in certi casi – modificare il comportamento degli individui.

Byung-Chul Han, a questo proposito, ha sostenuto che «si ricorre al *microtargeting* per rivolgersi ai votanti in modo mirato […] il *microtargeting* come prassi della microfisica del potere è una *psicopolitica* basata sui dati»[27].

A questo punto, è opportuno chiedersi se sussiste una conoscibilità e quindi una spiegabilità dei *big data* nel GDPR che, a sua volta, alimentano processi decisionali automatizzati compresa quella della profilazione.

---

[25] G. ZICCARDI, op. cit., 113-117. Per l'accurata descrizione delle diverse fasi di registrazione, raccolta e invio dei messaggi mirati agli utenti si veda G. SARTOR, *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022, 80-82; F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica*: *dal mercato alla sfera pubblica*, in *Federalismi.it*. *Rivista di diritto pubblico italiano*, *comparato*, *europeo*, 11, 2020, 103-104.

[26] È interessante la presa di posizione del Parlamento Europeo con Risoluzione del 25 ottobre 2018 sull'utilizzo dei dati degli utenti di Facebook da parte di *Cambridge Analytica* e l'impatto sulla protezione dei dati, dove si «ritiene l'interferenza elettorale un rischio enorme per la democrazia, da affrontare mediante uno sforzo congiunto che veda associati i fornitori di servizi, le autorità di regolamentazione nonché gli attori e partiti politici […] si sottolinea l'urgenza di contrastare qualsiasi tentativo di manipolazione delle elezioni dell'UE e di rafforzare le norme applicabili alle piattaforme online per quanto riguarda la perturbazione degli introiti pubblicitari dei conti e dei siti web che diffondo disinformazione» cit., 9-10.

[27] B. CHUL HAN, *Psicopolitica*, Nottetempo, Roma, 2016, cit., 75-76.

4. *Il diritto alla spiegabilità e alla conoscenza dei processi automatizzati*

Nel primo paragrafo di questo contributo si è avuto modo di osservare che ogni società viene ricordata attraverso l'apposizione di etichette, che delineano le caratteristiche principali della società in un preciso frangente storico. Non è erroneo sostenere che l'attuale società dell'informazione si sta evolvendo verso una società algoritmica. Infatti, la presenza sempre più massiccia di sistemi autonomi e intelligenti affianca e poi supera i sistemi tradizionali, imponendo nuove riflessioni giuridiche[28]. Questo superamento è dovuto grazie al cambiamento e allo sviluppo della ricerca, in cui lo sviluppo di un sistema intelligente ha bisogno di algoritmi capaci di compiere ragionamenti e correlazioni[29].

Un'altra etichetta che può essere affibbiata all'attuale società algoritmica è quella della *black box society*[30]. Con questa etichetta si vuole evidenziare la presenza di algoritmi sempre più opachi che sono in grado di stilare – ad esempio – un profilo della personalità, senza spiegarne la motivazione: si ottiene l'*input* e l'*output* senza comprendere il ragionamento di fondo. Questa opacità degli algoritmi[31] blocca qualsiasi aspirazione a comprendere il ragionamento svolto da queste *black box*.

Ciò nonostante, si intravedono delle timide aperture tramite il Regolamento generale per la protezione dei dati personali 2016/679. L'art. 22 prevede che – nel caso di un processo decisionale automatizzato – l'interessato ha il diritto di contestare la decisione. Il citato articolo del GDPR introduce, dunque, il concetto di non esclusività, che consiste nel richiedere l'intervento umano nel trattamento automatizzato. L'art. 22 del GDPR, peraltro, può essere letto in combinato disposto con il Considerando 71, stabilendo che, nei casi di procedimenti automatizzati che producono effetti giuridici nella sfera dell'interessato, dovrebbero essere poste delle garanzie adeguate e si raccomanda al titolare del trattamento di utilizzare «procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate […] siano minimizzati il rischio di errori e di effetti discriminatori».

Infine, il Considerando 63 fa riferimento al diritto dell'interessato di capire «la logica in cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento». Ciò significa che all'interessato – almeno in linea teorica – dovranno essere rese le informazioni necessarie per comprendere la logica del trattamento.

Anche con queste timide aperture del Regolamento, il Gruppo di lavoro di cui all'articolo 29 per la protezione dei dati osserva che non deve essere data necessariamente una spiegazione degli algoritmi o la divulgazione dell'algoritmo completo. In effetti, non è azzardato ipotizzare che il richiedere la completa trasparenza degli algoritmi possa comportare effetti negativi nel settore

[28] Cfr. G. FIORIGLIO, *La società algoritmica fra opacità e spiegabilità*, in *Ars intepretandi. Rivista di ermeneutica giuridica*, 1, 2021, 53.

[29] Cfr. G. SARTOR, *Introduzione*, in *Rivista di Filosofia del diritto*, 1, 2020, 65.

[30] Il termine compare con la monografia di F. PASQUALE, *The black box society*: *The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015.

[31] In effetti, in tempi non sospetti, Rodotà aveva intuito il rischio degli algoritmi sostenendo che «Questo confidare negli algoritmi ne determina una presenza sempre più pervasiva, che sembra non conoscere confini, giustificando il parlare di una società che essi contribuiscono a definire nelle sue nuove e significative caratteristiche» così S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, Laterza, 2012, cit., 402.

dell'informatica. Infatti, è stato osservato che richiedere la completa conoscenza degli algoritmi «comporterebbe una sostanziale revisione delle varie normative nazionali e internazionali che regolamentano la proprietà industriale e intellettuale; avrebbe un impatto devastante su gran parte del settore informatico (che si basa, parzialmente, proprio sulla confidenzialità degli algoritmi e dei codici informatici[32])».

Al di là delle questioni di natura informatica-industriale (in cui, per i motivi esposti sopra, è sconsigliabile porre una totale conoscenza dell'algoritmo), sussistono altre problematiche che non possono essere trascurate.

Da un lato, il principio di non esclusività pone la problematica dell'intervento: l'intervento umano non potrà essere indipendente senza verificare la provenienza e la categoria dei dati.

Dall'altro, è difficile sostenere la rettifica dei fattori che contribuiscano all'inesattezza dei dati se non sono noti proprio quei fattori[33]. A ciò si aggiunga anche la complessità dei sistemi di elaborazione che è nota ai pochi non ai molti; la complessità delle tecnologie, inevitabilmente, richiede un approccio interdisciplinare.

Come opportunamente messo in luce da Monica Palmirani, accanto e in aggiunta al diritto alla spiegabilità dell'algoritmo è necessario pretendere il principio di conoscibilità dei dati, ossia «non tanto e non solo quelli che sono stati contribuiti o osservati dall'utente, ma anche quelli che hanno contribuito al processo decisionale quindi quelli inferiti, derivati, collettivi, statistici, anche se anonimi»[34].

Solo attraverso l'applicazione del principio della conoscibilità dei dati, il diritto avrà la possibilità di implementare uno scenario di responsabilità (o delle responsabilità) nei casi in cui le macchine – anche se in presenza di algoritmi corretti – assumano decisioni sbagliate[35].

A questo punto della trattazione, è opportuno evidenziare che la capacità di controllo, analisi e interpretazione dei *big data* appartiene a soggetti privati che influenzano i comportamenti e le scelte dei consumatori-elettori per propri fini, monopolizzando le proprie posizioni sul mercato.

5. *Dalla democrazia rappresentativa alla postdemocrazia*

La rivoluzione tecnologica, com'è noto, ha toccato tutti gli ambiti di conoscenza e di vita di ogni singolo utente. In modo particolare, l'utilizzo delle ICT ha comportato anche una partecipazione della vita politica-sociale del demos all'interno del web. Non è infatti un caso che spesso si senta parlare di *e-democracy*[36].

[32] G. FIORIGLIO, *La società algoritmica fra opacità e spiegabilità*, cit., 55.

[33] Cfr. M. PALMIRANI, *Big data e conoscenza*, in *Rivista di Filosofia del diritto*, 1, 2020, 85.

[34] *Ibid.*, 87.

[35] Sempre all'interno del lavoro citato, Palmirani suggerisce anche le possibili soluzioni nella fase *ex ante* e nella fase *ex post* del trattamento automatizzato, 87-88.

[36] G. GOMETZ, *E-democracy. Forme e problemi della democrazia elettronica*, in TH. CASADEI - S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche, Questioni di informatica giuridica, prospettive istituzionali e sfide sociali,* cit. 57, definisce *l'e-democracy* come "l'uso delle tecnologie dell'informazione e della comunicazione come mezzo per lo svolgimento delle procedure egualitarie di autogoverno del popolo".

Ciò nonostante, nei paragrafi precedenti si è osservato che il comportamento di un utente non solo è prevedibile, ma anche modificabile e manipolabile: da una parte, l'utilizzo dei *big data* (e della profilazione) ha portato alla luce una nuova condotta denominata psicopolitica, che basa tutto sull'emotività del messaggio e dei destinatari; dall'altra parte, il potere informativo, di estrazione della conoscenza e di profilazione è in capo – sostanzialmente – a soggetti privati, che agiscono per propri fini commerciali-politici.

Fulco Lanchester, nell'individuare i quattro pericoli per la democrazia rappresentativa, identifica nell'enorme influenza dei mezzi di comunicazione di massa un rischio per la democrazia, perché «il processo decisionale del demos viene fortemente influenzato dagli stessi e distorto da un'eventuale concentrazione in mano di operatori singoli o collettivi»[37]. Sempre ad avviso di Lanchester, ciò comporta la regressione della democrazia partecipativa in una forma di postdemocrazia.

Con il termine postdemocrazia[38] si intende un sistema politico che – nonostante l'apparente vigenza delle norme e delle istituzioni fondamentali – è governato dalle lobby o dai mass media o che agisce seguendo i *diktat* delle compagnie private. Nella postdemocrazia il procedimento elettorale del demos è «una campagna di marketing basata abbastanza apertamente sulle tecniche di manipolazione usate per vendere prodotti»[39].

L'algoritmo descrive come combinare gli *input* per ottenere *l'output* desiderato, ma riesce anche ad analizzare il *sentiment* della rete; ciò è fondamentale poiché l'emotività è il canale privilegiato della politica (e delle campagne elettorali).

La presenza di bolle filtro, tra le altre cose, non permette agli utenti di visualizzare contenuti diversi, poiché sono inseriti all'interno di una bolla in cui vengono trasmessi (e pubblicati) i medesimi contenuti (o diversi contenuti con una matrice comune) senza che vi sia la possibilità di accedere alla pluralità informativa.

In pratica, ci si riferisce alla 'bolla' di informazioni in cui ogni utente viene chiuso. Le cause di questo fenomeno sono i sistemi di personalizzazione dei social media e dei risultati delle ricerche. Ogni volta che un utente effettua una ricerca online, ricerche precedenti e posizione vengono sfruttate per offrire risultati su misura. In particolare, sui social media, per ogni utente, l'esperienza può cambiare drasticamente in base a *like* messi, link cliccati, siti e pagine seguite.

Ciò significa che la sovranità del demos, in realtà, viene frammentata in piccoli atomi a sé stanti, che concepiscono e sviluppano idee (imposte) in perfetta solitudine. Viene spogliata la sovranità del demos innanzi a un contenuto veicolato, spesso tramite mere suggestioni; il demos è totalmente incapace di raccordarsi o di creare un filtro collettivo di ragionamento, che dovrebbe sorgere dall'esercizio costante della dialettica[40].

---

[37] F. LANCHESTER, *La Costituzione sotto sforzo*: *tra ipercinestimo elettorale e supplenza degli organi costituzionali di garanzia*, Wolters Kluwer - Cedam giuridica, Milano, 2020, cit., 18.

[38] Il concetto di postdemocrazia è stato introdotto, nel 2003, da C. CROUCH, *Postdemocrazia*, Laterza, Roma-Bari, 2003.

[39] *Ibid.*, 116.

[40] La mancanza di un filtro collettivo di ragionamento da parte degli utenti, che tendono a credere per vero tutto ciò che leggono all'interno della rete o nei social, è analizzata assai bene da Paolo Savarese. L'Autore, in tema di postverità, infatti rileva che «emozioni e credenze personali prevalgono sui fatti oggettivi nel dar forma alle opinioni, in specie quella pubblica», P. SAVARESE, *Dalla bugia alla menzogna*: *la postverità e l'impossibilitò del diritto*, in *Nomos*. *Le attualità del diritto*, 2, 2018, cit., 2. Sempre

D'altro canto, questa incapacità – o meglio assuefazione del demos – è dettata dal fatto che nell'odierna società algoritmica è facile manipolare la volontà del demos, ottenendo così dei risultati plebiscitari: il demos si illude di fare una scelta, ma in realtà è già indirizzato verso la scelta dettata dalla volontà altrui (*rectius,* privata) e non dalla volontà generale[41].

Enrico Pattaro definì il diritto una forma di dominio (*Heerschaft*) anche nei casi in cui gli ordinamenti giuridici avessero una natura liberal-democratica. In questo caso, parafrasando il titolo della sua monografia *Opinio iuris*, è plausibile sostenere che *big data opinio iuris* poiché «l'autorità, il potere, l'influenza non solo plasmano i significati orientati all'agire […] determinano la realtà concreta, i referenti attuali, i comportamenti concreti»[42].

6. *Riflessioni conclusive*

Il contributo ha evidenziato, da un lato, la grande importanza dei *big data* nella società contemporanea, e, dall'altro, i rischi conseguenti al loro utilizzo in ambito politico soprattutto al fine di orientare le scelte elettorali. I dati, *rectius,* il loro utilizzo consistente nella effettuazione di operazioni di 'estrazione' della conoscenza, sono stati e sono capaci di ridisegnare le sfere del pubblico e del privato, creando nuove gerarchie di potere.

Gli aspetti negativi della *data society* (qualora si desideri utilizzare questa etichetta) sono quelli della segretezza e della formazione di posizioni dominanti da parte di pochi attori pubblici o privati, che gestiscono il patrimonio informativo in forma chiusa ovvero limitando l'accesso solo a una parte dell'immenso patrimonio informativo[43].

A ciò si aggiunga che gli utenti vengono costantemente sorvegliati per conoscere i desideri e prevedere il loro comportamento. Come detto, la maggioranza degli utenti utilizza costantemente strumenti digitali e compie azioni che possono essere oggetto di controllo: stipula contratti, effettua ricerche, fruisce dei servizi ed esprime le proprie opinioni personali nei social; tutte queste attività lasciano tracce dell'attività digitale dell'utente e ne permettono la sorveglianza e, in seguito, la profilazione. Queste attività sono dettate anche dall'incuranza dell'utente che – per acquisire vantaggi o usufruire dei servizi delle piattaforme – cede volontariamente i propri dati personali, anche quelli non necessari per la prestazione dei servizi[44].

I *big data*, privi di direzione e regolamentazione, permettono una sorveglianza più semplice, economica ed efficace, che consente di sfruttarne la capacità predittiva: questa operazione,

in tema di postverità, altresì, cfr. TH. CASADEI, *L'irruzione della post-verità*, in *Governare la paura. A Journal of Interdisciplinary studies*, 2019, 1-18.

[41] G. FIORIGLIO, *Democrazia Elettronica. Presupposti e strumenti*, Wolters Kluwer, Milano, 2017, 386.

[42] E. PATTARO, *Opinio iuris. Lezioni di filosofia del diritto per l'a.a. 2010-2011*, Giappichelli, Torino, 2010, cit., 188.

[43] Cfr. A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo, in Il diritto dell'informazione e dell'informatica*, 1, 2012, 136-155.

[44] In questo contesto, infatti, è stato fatto notare come «il cittadino, dal canto suo, s'impegna spesso molto poco [...] per sfuggire a tale potere di sorveglianza […] l'utente comune non adotta particolari accorgimenti, di solito, nel non diffondere i suoi dati perché il desiderio di apparire e di essere presente nell'ambiente tecnologico ha fatto smarrire in molte persone la corretta percezione dell'importanza della privacy, della segretezza del dato e della chiusura delle informazioni personali, soprattutto di quelle più intime» così G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaele Cortina Editore, Milano, 2015, cit., 228.

tuttavia, non è esente da errori (o da interpretazioni fuorvianti) e favorisce le discriminazioni, negando il pluralismo informativo e la libera scelta[45].

In modo particolare, nel caso delle analisi predittive degli utenti per manipolare l'autodeterminazione dell'orientamento politico-elettorale, è innegabile che proprio i social media dipendano ontologicamente dal monitoraggio e dalla vendita dei dati a terzi[46].

Ciò nonostante, per cercare di arginare il problema della conoscibilità dei dati, è opportuno soffermare l'attenzione su un interessante progetto di regolamentazione sull'utilizzo dei *big data* in ambito politico-elettorale per limitare la manipolazione informativa[47]: a) gli utenti dovrebbero essere al corrente di chi sta effettuando una campagna mirata (c.d. *microtargating*); b) gli utenti – per comprendere la profondità del problema – dovrebbero essere informati sul pubblico preso di mira; c) gli utenti hanno il diritto di sapere i costi sostenuti da ogni team che effettua campagne micromirate, questo per evitare manovre occulte; d) le aziende dovrebbero costituire un database comune con i messaggi micromirati che vengono fatti circolare.

La *ratio* di questi punti programmatici sarebbe quella di evitare che i messaggi non pubblici prendano di mira determinate fasce di elettori, con un assedio di messaggi mirati.

Alla luce di queste considerazioni, sarebbe necessario, più che opportuno, prevedere norme atte a effettuare il bilanciamento tra diritti a fondamento costituzionale e regolazione collettiva negoziale al fine di tutelare una sorta di autodeterminazione informativa della collettività sui propri dati. Le costituzioni, com'è noto, individuano principi e valori fondamentali per la tenuta del sistema, tutelando gli individui da forme di abuso del potere da parte dei soggetti pubblici. Tuttavia, è necessario che questa tutela si estenda anche nei casi in cui l'abuso del potere venga esercitato dai soggetti privati che, come visto, costituiscono veri e propri poteri[48].

Del resto, proseguendo in tal senso sulla strada tracciata dalle normative previgenti, anche l'importanza che il GDPR riserva al consenso dell'interessato nel trattamento dei dati pare illusoria, considerando l'estremo squilibrio fra interessati (utenti) e prestatori dei servizi della Società dell'informazione: il regolamento ne considera il profilo solo dal punto descrittivo e non prescrittivo, per cui non è impedita la cessione dei dati non necessari quale condizione di accesso alle piattaforme o ai servizi[49].

Peraltro, a causa della mancata regolamentazione dei *big data*, ciò che viene a mancare oltre al libero consenso, alla libera scelta e al pluralismo informativo è l'autonomia dell'individuo (utente)

---

[45] Per Mayer Schonberg e Cukier è essenziale gestire il fenomeno perché «se non sarà così, i *big data* avranno sovvertito l'essenza stessa della natura umana, ovvero il pensiero razionale e la libera scelta. I *big data* sono una risorsa e uno strumento. Servono a informare, più che a spiegare; ci aiutano a capire, ma possono indurci anche al fraintendimento, a seconda di come vengono utilizzati» così V. MAYER SCHONBERG - K. CUKIER, op. cit., 266.

[46] Cfr. Z. BAUMAN - D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, Laterza, Roma-Bari, 2015, XV.

[47] Persuasori social - Trasparenza e democrazia nelle campagne elettroniche digitali, Centro per la riforma dello Stato. Il rapporto è consultabile qui: https://centroriformastato.it/wp-content/uploads/2020/12/Persuasori-Social-Finale-per-stampa-1.pdf (ult. consultazione 14.11.2022).

[48] Cfr. G. FIORIGLIO, *Trasformazioni del diritto. Alla ricerca di nuovi equilibri nell'esperienza giuridica contemporanea*, Giappichelli, Torino, 2017, 166-167.

[49] A questo proposito, è stato osservato infatti che «La *ratio* del Regolamento appare annacquata rispetto alla difesa di valori economici, che pure dovrebbero essere subordinati alla protezione dei dati. La norma dovrebbe vietare all'imprenditore di condizionare la fruizione di un servizio alla cessione di informazioni non necessarie alla prestazione», così M.F. DE TULLIO, *La privacy e i* big data *verso una dimensione costituzionale collettiva*, in *Politica del diritto*, 4, 2016, cit., 675.

intesa come set di opzioni disponibili per le sue scelte[50], minando così la stessa essenza della democrazia rappresentativa che si basa anche su quanto appena esposto.

Un altro rischio certamente connesso all'utilizzo dei *big data*, è quello di acuire la vulnerabilità[51] dei gruppi sociali più svantaggiati, che rischiano di essere sempre più assoggettati ai *desiderata* delle grandi Tech.

Il diritto, e di conseguenza la politica legislativa, non può restare inerme innanzi al progredire della tecnica: deve riaffermare i valori fondamentali degli ordinamenti democratici e dell'uomo, ossia affermare una visione umanocentrica che pare essersi persa nell'uso delle tecnologie.

Si auspica, dunque, che il problema venga preso sul serio e che la legislazione (sia essa nazionale o comunitaria) metta in atto un processo di riforme che regolamenti le nuove tecnologie partendo proprio da esse, allo scopo di tutelare maggiormente la libertà di manifestazione del pensiero, la privacy e – più in generale – i diritti fondamentali dell'uomo, senza, al contempo, limitare il progresso tecnologico. Affinché ciò avvenga, i legislatori non possono continuare a rimanere sostanzialmente inerti, in quanto solo appositi interventi legislativi sono idonei a imporre ai prestatori di servizi precise limitazioni che consentano di equilibrare efficacemente il diritto alla libera iniziativa economica privata con i diritti appena menzionati.

Risuona oggi il monito di Rodotà che affermava come «i diritti fondamentali si pongono a presidio della vita, che in nessuna sua manifestazione può essere attratta dal mondo delle merci»[52].

[50] Cfr. GF. ZANETTI, *Eguaglianza come prassi. Teoria dell'argomentazione normativa*, Il Mulino, Bologna, 2015, 21.

[51] Per una completa esposizione del concetto di vulnerabilità legato ai gruppi sociali più svantaggiati di fronte al potere si veda F. MACIOCE, *La vulnerabilità di gruppo. Funzioni e limiti di un concetto controverso*, Giappichelli, Torino, 2021. Cfr. in modo particolare, il V capitolo, legato alle dinamiche tra vulnerabilità di gruppo e potere, 107-125. Per l'analisi completa del concetto di vulnerabilità, cfr. B. PASTORE, *Semantica della vulnerabilità, soggetto, cultura giuridica*, Torino, Giappichelli, 2021; GF. ZANETTI, *Filosofia della vulnerabilità. Percezione, discriminazione, diritto*, Roma, Carocci, 2019. Per un'indagine giusfilosofica e semantica del termine vulnerabilità si rinvia a S. VANTIN, *Vulnerabilità, morte e* pietas. *L'atto della sepoltura e le sue implicazioni giuridiche*, in *Stato, Chiese e pluralismo confessionale*, 21, 2019, 57-62.

[52] S. RODOTÀ, *La vita e le regole: tra diritto e non diritto*, Feltrinelli, Milano, 2009, cit., 38.

ABSTRACT

L'enorme massa di dati presente all'interno della rete permette, grazie alle operazioni di big data analytics e di profilazione, di predire i comportamenti degli utenti e indirizzare le preferenze degli stessi verso i desiderata delle grandi aziende. In forza di ciò, il contributo – adottando una prospettiva informatico-giuridica – esamina l'utilizzo dei big data in ambito politico-elettorale. Soffermandosi dapprima sulla loro definizione e sulle loro diverse funzioni, per poi focalizzarsi sulla loro funzione predittiva, che fu sistematicamente analizzata da Nickerson e Rogers. Discusso il potenziale utilizzo di big data in contrasto in violazione del GDPR (*General Data Protection Regulation*) e dopo aver verificato un possibile contrasto tra big data e GDPR, l'attenzione sarà rivolta alla profilazione (analizzando il concetto e lo scopo) e a una sua particolare forma: il *microtargeting*. Ciò comporta la necessità di interrogarsi, da un lato, sul potenziale diritto dell'utente-interessato alla conoscibilità e alla spiegabilità dei processi automatizzati, nonché, dall'altro, sull'impatto dei big data sulla democrazia rappresentativa, a partire dal concetto di postdemocrazia di Crouch. Vengono, infine, proposte talune possibili soluzioni finalizzate a consentire un uso dei big data che sia rispettoso della normativa vigente e che possa contribuire positivamente all'evoluzione, e non all'involuzione, della democrazia rappresentativa.

The enormous mass of data within the network makes it possible, thanks to big data analytics and profiling operations, to predict users' behaviour and direct their preferences towards the *desiderata* of big companies. By virtue of this, the contribution - adopting a informatics legal perspective - examines the use of big data in the political-electoral sphere. It first dwells on their definition and their different functions, and then focuses on their predictive function, which was systematically analysed by Nickerson and Rogers. After discussing the potential use of big data in contravention of the GDPR (General Data Protection Regulation) and after verifying a possible clash between big data and GDPR, the focus will be on profiling (analysing the concept and purpose) and one particular form of it: microtargeting. This implies the need to question, on the one hand, the potential right of the user-interested to the knowability and explainability of automated processes and, on the other hand, the impact of big data on representative democracy, starting from Crouch's concept of post-democracy. Finally, a number of possible solutions are proposed in order to allow the use of big data that is respectful of current regulations and that can contribute positively to the evolution, and not the involution, of representative democracy.

PAROLE CHIAVE: Big data analytics, profilazione, spiegabilità, postdemocrazia, democrazia rappresentativa.

KEYWORDS: Big data analytics, profiling, explainability, postdemocracy, representative democracy.