PUBLIC AND PRIVATE IN CONTEMPORARY SOCIETIES

A cura di
Claudia Morgana Cascione,
Giorgio Giannone Codiglione, Paolo Pardolesi

Studies in Law and Social Sciences 11

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

Nella stessa Collana

1. G. Rojas Elgueta, N. Vardi (a cura di), *Oltre il soggetto razionale*, 2014
2. F. Mezzanotte (a cura di), *Le «libertà fondamentali» dell'Unione europea e il diritto privato*, 2016
3. C.A. D'Alessandro, C. Marchese (a cura di), *Ius dicere in a globalized world. A comparative overview*, 2018
4. A. Zoppini, P. Sirena (a cura di), *I poteri privati e il diritto della regolazione*, 2018
5. F. Caggia, G. Resta (a cura di), *I diritti fondamentali in Europa e il diritto privato*, 2019
6. A. Somma, V. Zeno-Zencovich (a cura di), *Comparazione e diritto positivo. Un dialogo tra saperi giuridici*, 2021
7. R. Lupi, *Studi sociali e diritto*, 2022
8. G. Giannone Codiglione, L. Pierdominici (a cura di), *Comparative Law in Times of Emergencies*, 2022
9. M. Filomeno, I. Rocchetti, *Dati e metodi per la statistica giudiziaria*, 2023
10. M.L. Vazquez, *Varieties of Religious Space. Freedom, Worship and Urban Justice*, 2024

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

Collana “Studies in Law and Social Sciences”

11

PUBLIC AND PRIVATE IN CONTEMPORARY SOCIETIES

A cura di
Claudia Morgana Cascione,
Giorgio Giannone Codiglione, Paolo Pardolesi

Roma TrE-Press
2024

Collana pubblicata nel rispetto del Codice etico adottato dal Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, in data 22 aprile 2020.

Il volume pubblicato è stato sottoposto a previa e positiva valutazione nella modalità di referaggio *double-blind peer review.*

Coordinamento editoriale:
Gruppo di Lavoro *Roma TrE-Press*

Elaborazione grafica della copertina: MOSQUITO. mosquitoroma.it

Impaginazione: Colitti-Roma colitti.it

Caratteri tipografici utilizzati:
Brandon Grotesque(copertina e frontespizio)
Adobe Garamond Pro (testo)

Edizioni: Roma TrE-Press
Roma, novembre 2024
ISBN: 979-12-5977-393-7

http://romatrepress.uniroma3.it

L'attività della *Roma TrE-Press* è svolta nell'ambito della
Fondazione Roma Tre-Education, piazza della Repubblica 10, 00185 Roma

Table of Contents

III - THE PUBLIC DIMENSION OF CONTRACT

IV - LAW IN TIME OF EMERGENCIES

Laura Fabiano

Spazio pubblico ed interessi privati nell'era digitale: spunti comparativi in tema di voto elettronico[*]

Sommario: 1. La *partnership* pubblico/privato nell'"era digitale" – 2. Interessi pubblici e poteri privati nell'espressione elettorale. – 3. Il dibattito sull'utilizzo della tecnologia *Blockchain* nei processi elettorali.

1. *La* partnership *pubblico/privato nell'"era digitale"*

Il progresso tecnologico ed informatico degli ultimi decenni ha prodotto dei significativi cambiamenti nella vita quotidiana di ogni individuo dando inizio ad una nuova fase della vita umana, simbolicamente definita "era digitale"[1], caratterizzata da un'integrazione a volte inestricabile fra spazio fisico e dimensione informatico-virtuale[2] nella quale le categorie tradizionali sono soggette a continua rivalutazione[3] e le raggiunte soluzioni

[*] Il presente contributo si inquadra in una linea di ricerca del progetto competitivo *Horizon Europe Seeds* finanziato dall'Università degli Studi di Bari, Aldo Moro, su "Libertà di opinione, nuove tecnologie e formazione del consenso".

[1] Nella c.d. era digitale le generazioni umane sono suddivise in relazione al grado di esposizione tecnologica cui sono state esposte (cfr. sul punto R. Stella, C. Riva, C.M. Scarcelli, M. Drusian, *Sociologia dei New Media*, UTET, Milano, 2018) per cui ai *boomers* ed alla generazione Z si contrappone la generazione 2.0 (https://www.treccani.it/enciclopedia/generazione-2-0_%28altro%29/) e quella dei nativi digitali. L'espressione nativi digitali è stata coniata nel 2001 da Mark Prensky il quale la contrapponeva alla generazione degli immigrati digitali ovvero tutti coloro che, nati in epoche precedenti alla diffusione di determinate tecnologie, le hanno apprese in età adulta. Cfr. M. Prensky, *Digital Natives, Digital Immigrants*, in *On the Horizon*, 2001, 9(5), pp. 1-6; si rinvia, inoltre, a Id., *Digital Natives, Digital Immigrants, part II. Do they really think differently?*, in *On the Horizon*, 2001, 9(6), pp. 1-6; Id., *Listen to the Natives*, in *Educational Leadership*, 63(4), 2005, pp. 8-13. Cfr. per la dottrina italiana anche M. Martoni, *Datificazione dei nativi digitali, Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in *federalismi.it*, , 2020.

[2] Sul tema cfr. A. Pin, *Nella Rete, anche se offline. Il ruolo dello spazio pubblico nell'era digitale*, in *Mondo Digitale*, Dicembre 2022; cfr. inoltre L. Floridi, *Soft Ethics and the Governance of the Digital*, in *Philosophy & Technology*, 1, 2018, p. 1 ss.

[3] La significativa portata innovativa insita nell'evoluzione digitale ha spinto inizialmente

giuridiche finalizzate a regolare l'uso della tecnologia telematica divengono spesso improvvisamente obsolete e da rinegoziare.

Se, sotto innumerevoli profili, tali cambiamenti rappresentano delle immense risorse per l'evoluzione complessiva della società umana, oltre che per gli individui singolarmente intesi, è nondimeno vero che questa evoluzione (come probabilmente tutti i cambiamenti significativi nei modi di vivere e di fare le cose degli esseri umani) pone di per sé anche delle nuove ardue sfide in termini di regolazione dei rapporti e di garanzie dei diritti e delle libertà[4].

Uno fra i numerosi elementi che rappresenta una sfida in tale particolare contesto è certamente l'importante ruolo giocato nella *governance* dello spazio pubblico dai diversi colossi della tecnologia informatica e dunque la conseguente inevitabile *partnership* fra dimensione pubblica e privata che caratterizza le soluzioni giuridiche (e tecniche) che possono essere adottate per regolare i rapporti nei contesti digitali[5].

Il dibattito dottrinale e dell'opinione pubblica sul tema è da sempre particolarmente vivace risultando evidente come alcune caratteristiche tecniche del mezzo informatico sono in grado di manipolare la volontà individuale ed alterare, dunque, la libertà personale e di opinione dei privati e delle col-

la dottrina giuridica ad interrogarsi sulla stessa praticabilità dell'estensione al mondo telematico del diritto territoriale vigente nel mondo reale e, dunque, sul c.d. "statuto costituzionale di Internet". L'espressione è di M. Bassini (*Internet e libertà di espressione*, Aracne, Canterano, RM, 2019) al quale si rinvia per una completa analisi dell'evoluzione storica della dottrina giuridica internazionale concernente la dimensione costituzionale oltre che il diritto applicabile e la giurisdizione competente per la disciplina del cyberspazio.

[4] Sul punto la bibliografia è oramai sterminata e, dunque, ci si limita solo ad alcuni fondamentali riferimenti: S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma, 1997; V. Zeno-Zencovich, *Informatica ed evoluzione del diritto*, in *Diritto dell'informazione e dell'informatica*, 1, 2003; M. Bassini, *Internet e libertà di espressione*, cit.; P. Costanzo, *Il fattore tecnologico e le sue conseguenze*, in *Rassegna parlamentare*, 4, 2012, pp. 811 ss.; T.E. Frosini, *Tecnologie e libertà costituzionali*, in *Diritto dell'informazione e dell'informatica*, 3, 2003, pp. 487 ss.; T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, Le Monnier Università, Firenze, 2017; M. Olivetti, *Diritti fondamentali e nuove tecnologie. Una mappa del dibattito italiano*, in *Revista Estudos Institucionais*, 6(2), pp. 395-430, *maio/ago* 2020. Sul tema dell'impatto dell'evoluzione tecnologica informatica sul diritto pubblico e sulla tenuta delle garanzie costituzionali si rinvia, inoltre, in generale, ai numerosi interessanti contributi presenti nel vol. 1 del *Liber Amicorum* per Pasquale Costanzo dedicato a *Costituzionalismo, Reti e Intelligenza Artificiale*, in *ConsultaOnLine*, 2020.

[5] Sul tema, con particolare riguardo alla questione dell'incremento, nell'ambito dell'attività regolatoria di alcuni importanti questioni pubbliche quali le campagne elettorali, dell'uso di tecniche normative di *soft law* quali l'autoregolazione o la coregolazione si rinvia a M.R. Allegri, *Oltre la Par Condicio, comunicazione politico elettorale nei social media, fra diritto e autodisciplina*, Franco Angeli, Milano, 2020.

lettività. Le ICT (*Information and Communication Technologies*) sono infatti tecnologie dotate di profonda potenzialità manipolativa in quanto attraverso la c.d. profilazione algoritmica le grandi aziende del *tech* sono in grado di selezionare i contenuti determinanti per la formazione dell'opinione pubblica: l'algoritmo definisce gli utenti a partire dai dati che li riguarda - e che essi stessi consapevolmente o inconsapevolmente forniscono - (*profiling*) ed offre loro informazioni selezionate (*targeting*[6]). Ciò conduce al paradosso per il quale, in un contesto come quello della rete *web*, ove circolano continuamente milioni di dati e di informazioni, i singoli individui vengono sostanzialmente chiusi in una bolla informativa realizzata dal filtro algoritmico (*filter bubble*[7]). Si tratta di una "esposizione selettiva" per la quale, privati di fatto della possibilità di un'informazione libera e completa[8] gli individui tendono ad estremizzare le proprie opinioni con un generale effetto polarizzante[9] che riguarda l'intera collettività[10]. In questo contesto il ruolo svolto dalle grandi aziende tecnologiche è cruciale in quanto esse «dietro l'appa-

[6] A. Perrini, *Microtargeting: cos'è e quali sono gli impatti per la protezione dei dati personali*, consultabile all'url: https://www.agendadigitale.eu/sicurezza/privacy/microtargeting-cose-e-quali-sono-gli-impatti-per-la-protezione-dei-dati-personali/ (23 marzo 2020).

[7] E. Pariser, *Il filtro. Quello che Internet ci nasconde*, il Saggiatore, Milano, 2012; Cfr. sul tema E. Longo, *Dai big data alle "bolle filtro": nuovi rischi per i sistemi democratici*, in *Percorsi costituzionali*, 1, pp. 29-44, 2019; M. Bianca, *La filter bubble e il problema dell'identità digitale*, in *MediaLaws – Rivista di diritto dei media*, 2, 2019, pp. 39 ss.

[8] Afferma efficacemente Sunstein a tal proposito che «se alle persone viene negato l'accesso a pareri contrastanti su argomenti di interesse pubblico e se, da parte loro, c'è come risultato una mancanza di interesse per questi punti di vista, si verifica una mancanza di libertà, qualunque sia la natura delle loro preferenze e scelte», *Republic.com. Cittadini informati o consumatori di informazioni?*, cit., p. 126.

[9] L'Agcom, in uno studio pubblicato a novembre 2018 (Agcom, *Rapporto Tecnico. Le strategie di disinformazione online e la filiera dei contenuti fake*, 9 novembre 2018. Il documento è disponibile a seguente link: https://www.agcom.it/documents/10179/12791484/Documento+generico+09-11-2018+1541763433144/e561edf2-a138- 443e-9937-303f68d92cc3?version=1.0.) ha rilevato come sussista un rapporto direttamente proporzionale fra la polarizzazione ideologica degli utenti dei *social network* e l'intensità e la frequenza delle loro attività in rete. Accade dunque che gli individui più schierati dal punto di vista ideologico ricorrono ad Internet come mezzo di comunicazione per informarsi sulle scelte politico-elettorali assai più ampiamente rispetto alle persone con scarso livello di polarizzazione ideologica. Sul punto cfr. M.R. Allegri, *Oltre la Par Condicio, comunicazione politico elettorale nei social media, fra diritto e autodisciplina*, cit.; G. Origgi, *La democrazia può sopravvivere a Facebook? Egualitarismo epistemico, vulnerabilità cognitiva e nuove tecnologie*, in *Ragion Pratica*, 51 (2), 2018, pp.445-458 (la quale efficacemente definisce tale condizione "vulnerabilità cognitiva", p. 447); O. Grandinetti, *La par condicio al tempo dei social, tra problemi "vecchi" e "nuovi" ma, per ora, tutti attuali*, in *MediaLaws – Rivista di diritto dei media*, 3, 2019, p. 92 ss.

[10] Cfr. sul tema E. Longo, *Dai big data alle "bolle filtro": nuovi rischi per i sistemi democratici*, cit.

rente gratuità dei propri servizi, richiedono all'utente, quale contropartita […] la cessione (in varia misura e a vario titolo) di dati di eterogenea natura (riguardanti sia la sfera personale sia, più in generale, inclinazioni, gusti e preferenze)»[11] al fine tanto di potenziare la loro capacità pubblicitaria sul mercato quanto per rivendere questi dati a soggetti terzi.

Il tema si è particolarmente animato a partire dal 2016. In quell'anno si è difatti reso evidente il potenziale distorsivo insito nelle campagne politiche *on line* e le possibili interferenze private cui esse sono soggette. Ciò è avvenuto in occasione della prima campagna elettorale di Donald Trump per la corsa alla presidenza degli Stati Uniti D'America ed alla campagna referendaria sulla *Brexit*[12]. Il tema è nuovamente esploso nel 2018 con il noto scandalo *Cambridge Analytica* in relazione al quale si è evidenziato come, attraverso l'analisi dei dati disponibili sulla rete, un'azienda privata è in grado di interferire incisivamente in una campagna elettorale alterandone la democraticità[13].

L'erompere della pandemia mondiale da Covid 19 ha infine costituito, pochi anni più tardi, un'ulteriore vicenda storica a fronte della quale si è reso manifesto l'immenso potenziale pervasivo delle tecnologie digitali nella vita quotidiana individuale ed ha posto all'ordine del giorno, come priorità assoluta, la necessità di regolare i numerosi fenomeni connessi alla rete Internet e risolvere sia tecnologicamente, ma anche giuridicamente, problematiche da tempo note divenute oramai ineludibili.

A fronte degli scandali politici del 2016 e delle problematiche sorte in relazione ad un mondo connesso prevalentemente *on line* (più che in presenza) a causa della pandemia si è reso difatti del tutto evidente l'insufficienza dell'approccio tendenzialmente liberista prescelto per orientare la regolazione dei fenomeni di espressione e costruzione del consenso (anche politico) *on line* che ha caratterizzato per diversi anni alcune scelte normative e giurisprudenziali. Si è dunque assistito ad un'evoluzione recente in termini di spinta ad una maggiore regolazione di alcuni fenomeni e di più significativa responsabilizzazione degli attori privati che in ambito digitale svolgono funzioni e ruoli talmente importanti

[11] B. Rabai, *I Big Data nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in *Amministrare*, 3, 2017, pp. 407 ss.

[12] Cfr. P. Norris, R. Inglehart, *Cultural Backlash, Trump, Brexit and Authoritarian Populism*, Cambridge University Press, 2019.

[13] Sul tema E. Assante, *Cosa ci può insegnare il caso Cambridge Analityca*, in *federalismi.it*, Editoriale, 25 aprile 2018. D. Messina, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"*, in *federalismi.it*, 20, 2018.

da essere qualificati come veri e propri poteri[14] in quello che si usa oramai chiamare, forse ancora arditamente[15], il costituzionalismo digitale[16].

2. *Interessi pubblici e poteri privati nell'espressione elettorale*

Un ambito nel quale la *partnership* fra dimensione pubblica e potere dei privati si realizza, ponendo in essere un insidioso potenziale pervasivo (e dunque, ipoteticamente, anche distorsivo), è quello dell'espressione elettorale attraverso lo strumento elettronico nelle sue multiformi possibilità. Esse vanno dal più semplice voto elettronico (l'*e-voting*) realizzato in contesti "presidiati" (all'interno di postazioni pubbliche e sotto la supervisione del personale elettorale) attraverso un supporto tecnologico informatico, fino all'*home voting*, procedura di espressione elettorale "non presidiata" (e dunque non sottoposta alla supervisione di funzionari pubblici), che realizza la forma più estrema di *internet voting* (*i-voting*); tale modalità di esercizio della volontà politica assicura certamente una grande accessibilità all'espressione elettorale e tuttavia presenta dei maggiori rischi in termini di sicurezza e di segretezza del voto[17].

Il tema del voto elettronico è da lungo tempo oggetto di dibattito e analisi giuridica e politologica[18] ed è divenuto certamente argomento particolarmente attuale a seguito della vicenda pandemica del 2020[19].

[14] M. Betzu, *Poteri pubblici e privati nel mondo digitale*, in *La Rivista del Gruppo di Pisa*, 2, 2021, pp. 166 ss.; A. Venanzoni, *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in *MediaLaws – Rivista di diritto dei media*, 3, 2020, pp. 178 ss.

[15] Critico rispetto a tale espressione che considera equivoca e atecnica è G.E. Vigevani, *Piattaforme digitali private, potere pubblico e libertà di espressione*, in *Diritto Costituzionale*, 1, 2023, pp. 41 ss.

[16] A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, in *Rivista italiana di Informatica e Diritto*, 1, 2020, pp. 5 ss.; T.E. Frosini, *Il Costituzionalismo nell'età tecnologica*, in *Diritto dell'Informatica*, 2020, pp. 465 ss.

[17] Un esempio di voto non presidiato è quello che si svolge per corrispondenza; con l'evoluzione tecnologica a tale tipologia di espressione elettorale si è affiancato il voto via Internet o quello tramite telefono. Sulle classificazioni in tema di voto elettronico si rinvia a M. Schirippa, *Le nuove frontiere del diritto di voto*, Padova, Cedam, 2022. Cfr. anche L. Trucco, *Il voto elettronico nel quadro della democrazia digitale*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, cit., pp. 425 ss.

[18] Si pensi all'intenso dibattito suscitato dalla vicenda occorsa alle elezioni presidenziali statunitensi del 2000. Sul punto per la dottrina italiana F.G. Pizzetti, *Bush v. Gore. Un nuovo caso di federalismo giurisdizionale*, Giappichelli, Torino, 2002.

[19] Sul punto cfr. C. Binder, A. Drnovsky, *To vote or not to vote*, in *Verfassungsblog*, 7 luglio

I-Voting ed *e-voting*, come è evidente, rappresentano due modalità di espressione della volontà rappresentativa del cittadino potenzialmente molto diverse e pongono problematiche che non sempre coincidono. L'*internet voting*, difatti (soprattutto nella sua modalità più estrema più estrema rappresentata dall'*home voting*), pone numerose questioni che non si evidenziano nelle altre forme più "moderate" di voto elettronico: fra le tante possono esemplificativamente annoverarsi le significative minacce di attentato alla libertà dell'espressione elettorale (legate all'impossibilità di garantire che l'elettore non subisca delle pressioni illegittime o anche semplicemente inopportune -in questo si concreta ad esempio il fenomeno detto del *family voting*-) oltre che il possibile rischio che un voto espresso in modo "poco solenne" possa non essere percepito nella sua rilevanza politica e dunque finire per non essere adeguatamente ponderato nella sua espressione[20].

Alcune problematiche sono invece riscontrabili in tutto l'ampio ecosistema del voto elettronico (dunque, sia nel voto *on line* sia in quello, più semplicemente, solo espresso attraverso mezzi elettronici). Fra queste, un tema importante concerne, appunto, il rapporto fra la dimensione pubblica insita nel momento elettorale e dell'espressione del voto e l'intrinseca natura privatistica del supporto tecnico necessario all'espletamento del medesimo in relazione alle problematiche connesse alla tutela del segreto commerciale.

Tale argomento è relativamente risalente in quanto si è posto ed è stato discusso nell'esperienza statunitense, anche nelle aule giudiziarie, già a metà del primo decennio del nuovo secolo.

Un caso emblematico si è verificato difatti nel 2006, in Florida, nella vicenda *Jennings v. Buchanan*[21].

2020, online: https://verfassungsblog.de/to-vote-or-not-to-vote/ . Cfr. inoltre, *Why voting online is not the way to hold an election in a pandemic*, in *The Economist*, 28 aprile 2020, *online*: https://www.economist.com/international/2020/04/27/why-voting-online-is-not-the-way-to-hold-an-election-in-a-pandemic.

[20] Il detto tema è rintracciabile in numerose sentenze nella giurisprudenza costituzionale comparata. In particolare, in una decisione del 2007 (*Conseil Constitutionnel. Décision n. 2007-142 PDR, 7 juin 2007 ; Observations sur l'élection présidentielle des 22 avril et 6 mai 2007. Délibération des 31 mai et 7 juin 2007*) esprimendosi sull'uso delle c.d. *machine a voter* nelle elezioni politiche, parlava esplicitamente di "resistenza psicologica" dell'elettore dinanzi ai cambiamenti tecnologici il Consiglio Costituzionale francese. Per una chiara illustrazione della complessità del tema si rinvia alle riflessioni di M. Schirippa, *Le nuove frontiere del diritto di voto*, cit.

[21] Su cui cfr. J.R. Amuson, S. Hirsh, *The Case of the Disappearing Votes: Lessons from the Jennings v. Buchanan Congressional Election Contest*, in *William & Mary Bill of Rights Journal*, 17(2), 2008, pp. 397 ss.

Il 7 novembre del 2006 nella contea di Sarasota, in Florida, l'elettorato aveva votato per il rinnovo dei rappresentanti al Congresso: all'esito del voto, il rappresentante risultato vincitore, il repubblicano Vern Buchanan aveva ottenuto 369 voti più della candidata risultata sconfitta, la democratica Christine Jennings. I voti espressi erano stati oltre 238.000 e, a seguito dello spoglio elettorale, risultava che quasi 18.000 persone (circa 1 su 7) non avevano espresso il proprio voto che, nella Contea di Sarasota, si esercitava attraverso uno strumento elettronico per mezzo di delle *paperless electronic touchscreen voting machines* (*iVotronic*) fornite dall'azienda ES&S. Nel contenzioso che ne è seguito la parte ricorrente è riuscita a dimostrare che almeno 14.000 di quei 18.000 voti erano schede sulle quali gli elettori erano convinti (o sostenevano di esserlo) di avere espresso una preferenza e, dunque, il risultato dello spoglio risultava presumibilmente alterato.

Vennero avanzate tre ipotesi principali per la causa del problema: in primo luogo, quale possibilità più grave ai fini dell'integrità dell'elezione appena svolta, si ipotizzò un "Codice dannoso" ovvero si valutò la possibilità che il *software* nelle macchine *iVotronic* fosse stato hackerato con l'esplicito fine di non registrare alcuni voti in un modo da favorire l'elezione di Buchanan. Tale possibilità avrebbe concretato la sussistenza di una vera e propria frode elettorale. Una seconda possibilità avrebbe potuto consistere in un *bug* del software. Infine, si ipotizzò semplicemente che si fosse verificato un problema con il *layout* della scheda elettorale valutando l'eventualità che lo stesso, per come era stato predisposto, aveva potuto indurre molti elettori a non votare correttamente.

Ne seguì, come già anticipato, una intensa vicenda giudiziaria (che si consumò in sede di giurisdizione statale oltre che attraverso un ricorso alla preposta Commissione sulla verifica delle elezioni presso la Camera dei rappresentanti federale) nel corso della quale ciò che fece estremo scalpore agli occhi della pubblica opinione fu che l'azienda privata che aveva fornito i mezzi tecnici utilizzati nelle elezioni contestate si rifiutò di fornire alcune informazioni specifiche riguardanti *hardware* e *software* invocando il segreto commerciale. L'eccezione avanzata dall'azienda privata venne accolta dal giudice in quanto considerata conforme alla legge statale sulle garanzie al *trade secret*, allo *Uniform State Secret Act* federale ed anche a quanto disposto nel *Freeedom of information Act*. Tale ultima normativa che pure, come noto, è volta a garantire la trasparenza nell'azione amministrativa e il diritto di accesso, prevede alcune clausole in deroga, fra cui la nota *Exemption 4* che garantisce la riservatezza sul segreto commerciale. Alcuni elementi tecnici del momento elettorale non

poterono dunque essere debitamente approfonditi e, probabilmente, anche a causa di questa circostanza il contenzioso giudiziario non condusse ad un'esaustiva risoluzione della vicenda all'esito della quale venne confermato vincitore il candidato repubblicano.

La vicenda riferita, pur risalente, rappresenta un caso emblematico del rischio per il quale l'utilizzo della tecnologia digitale nel momento elettorale corrisponde anche ad un pericoloso ingresso della dimensione privata in un momento eminentemente pubblico.

Non sorprende dunque che solo 3 anni dopo il giudice federale tedesco, in una nota sentenza del 3 marzo 2009[22], abbia rilevato, fra i diversi elementi di fragilità nelle modalità di effettuazione del voto elettronico in Germania[23], il fatto che si utilizzassero macchine prodotte da un'azienda

[22] *2 BvC 3/07*. La vicenda processuale era sorta dopo le elezioni federali del 2005 a seguito di un ricorso presentato da due elettori, i quali avevano sporto denuncia anche presso la Commissione per il controllo delle elezioni. I ricorrenti sostenevano che l'uso delle macchine per il voto elettronico fosse incostituzionale in quanto fosse possibile hackerare i dispositivi elettronici e dunque mettere a rischio l'attendibilità dei risultati elettorali. Il tribunale costituzionale si pronunciò a favore dei ricorrenti sottolineando la necessità che i cittadini possano nutrire fiducia nel controllo pubblico del voto, nell'affidabilità delle procedure elettorali, nella verificabilità del processo elettorale e nel buon funzionamento e nell'imparzialità degli apparecchi tecnologici utilizzati. Sulla decisione si rinvia per la dottrina italiana A. Gratteri, *Germania: le garanzie minime necessarie e il voto elettronico secondo il Tribunale Costituzionale*, in forumcostituzionale.it, 2009; E. Bertolini, *Il polling place e-voting nella recente pronuncia del Bundesverfassungsgericht: un futuro da riconsiderare?*, in *Diritto Pubblico Comparato ed Europeo*, 2, 2009, pp. 599 ss.

[23] Sui quali emblematicamente il Tribunale afferma: «la natura pubblica delle elezioni è un presupposto fondamentale per la formazione della volontà politica democratica. Assicura la correttezza e la verificabilità degli eventi elettorali, e quindi crea un presupposto importante per la fondata fiducia del cittadino nel corretto svolgimento delle lezioni. La forma statale della democrazia parlamentare, in cui il governo del popolo è mediato dalle elezioni, cioè non direttamente esercitato, esige che l'atto di trasferimento della responsabilità statale ai parlamentari sia soggetto a uno speciale controllo pubblico… in una democrazia rappresentativa, le elezioni della rappresentanza popolare costituiscono l'atto fondamentale di legittimazione… Il rispetto dei principi elettorali applicabili in materia e la fiducia nel rispetto di essi costituiscono dunque i presupposti per una democrazia vitale. Solo attraverso la possibilità di controllare se le elezioni rispettano i principi elettorali costituzionali è possibile garantire che la delega del potere statale alla rappresentanza popolare, che costituisce il primo e più importante tassello delle ininterrotta catena di legittimazione del popolo agli organi e titolari di cariche incaricate di incarichi statali non soffre di alcun difetto la legittimazione democratica delle elezioni esige che gli eventi elettorali siano controllabili in modo che la manipolazione possa essere escluso o corretta e il sospetto ingiustificato possa essere confutato. Questo è l'unico modo per facilitare la fondata fiducia del sovrano nella corretta formazione dell'organo di rappresentanza l'obbligo che incombe sul legislatore e sull'esecutivo di garantire che la procedura elettorale

privata (peraltro non tedesca ma olandese - *la Nedap* -)[24].

Al tema dell'intreccio fra tecnologia privata e interesse pubblico si collega senz'altro la questione della pubblicità del c.d. codice sorgente[25].

Nell'esperienza che è considerata la patria dell'*internet voting*, l'Estonia, la documentazione di *i-voting* ed il codice sorgente del sistema sono informazioni che vengono rese pubbliche con la finalità di aumentare la trasparenza e permettere a tutti gli interessati di studiare il *software* del sistema di voto elettronico e di sottoporli a *test*.

In India, dove dagli anni duemila si è progressivamente imposto il voto elettronico presidiato, il *software* impiegato è sviluppato e prodotto direttamente dal governo, senza l'intermediazione di alcuna azienda privata. In particolare, il *software* è realizzato attraverso un gruppo scelto di ingegneri del Ministero della difesa del Ministero dell'energia atomica, senza alcuna forma di contratti esterni. Nell'esperienza indiana il codice sorgente del programma è mantenuto segreto e non condiviso al di fuori del gruppo di sviluppo il che peraltro, sotto alcuni profili può anche fra sorgere dei dubbi sulla possibilità che il governo faccia un uso distorto di tali dati. L'*hardware* è invece prodotto dalle aziende Bharat Electronics e dalla Electronics Corporation of India. In India si è peraltro sviluppato

sia concepita costituzionalmente e si è attuata correttamente non è di per sé sufficiente a garantire la necessaria legittimità solo se l'elettorato può convincersi in modo affidabile della legittimità dell'atto di trasferimento, se le elezioni vengono dunque attuate "sotto gli occhi del pubblico" è possibile garantire la fiducia del popolo nel Parlamento composto in modo corrispondente alla volontà degli elettori elemento necessario per il funzionamento della democrazia e la legittimità democratica delle decisioni statali» (p.ti da 107-109). Il giudice tedesco aggiunge inoltre che «una procedura elettorale in cui l'elettore non è in grado di comprendere in modo affidabile se il suo voto è registrato in modo non falsificabile ed è incluso nell'accertamento del risultato elettorale, e non è in grado di comprendere in che modo i voti totali espressi sono assegnati e contati, esclude gli elementi centrali della procedura elettorale dal monitoraggio pubblico e dunque non è conforme ai requisiti costituzionali» (punto 113).

[24] In particolare, nella decisione si legge che l'uso delle macchine per il voto elettronico della società Nedap «non garantisce un controllo che corrisponda al principio costituzionale del voto pubblico», 2 BvC 3/07 (Traduzione dell'A.).

[25] Il Codice sorgente è la «Versione di un algoritmo scritta in un linguaggio di programmazione ad alto livello (ossia più vicino al linguaggio umano, tipicamente in pseudo inglese), le cui istruzioni sono poi eseguite dalla macchina mediante appositi programmi (compilatori, assemblatori o interpreti). L'impiego di un codice sorgente è finalizzato all'esecuzione, sull'insieme dei dati di ingresso, di azioni definite nel linguaggio di programmazione scelto tramite un numero limitato di istruzioni» (M. Capelli, *Codice sorgente (voce)*, in *Enciclopedia delle Scienze e della tecnologia*, Treccani, 2008, consultabile all'url https://www.treccani.it/enciclopedia/codice-sorgente_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/).

il dibattito sulla possibilità di introduzione dell'*internet voting*: l'*Indian Institute of Technology* di Madras ha difatti lavorato ad un sistema di voto elettronico via *Internet* basato su *Blockchain*[26] e collegato ad Aadhaar (il più grande sistema di identificazione biometrica del mondo, strumento strategico per l'inclusione sociale e finanziaria per le riforme di attuazione del settore pubblico e la gestione dei bilanci fiscali); tuttavia, questa ipotesi è in effetti, allo stato attuale, piuttosto remota e risulta interessante evidenziare come nel dibattito sulla possibilità di introduzione dell'*internet voting* sia stata evidenziata la necessità di rendere pubblico, in quel caso, il codice sorgente per consentire a chiunque di esaminarlo. In effetti la necessità di rendere pubblico il codice sorgente rientra fra le ragioni per cui in India il dibattito sull'introduzione dell'*home voting* sembra aver subito una significativa battuta d'arresto.

3. *Il dibattito sull'utilizzo della tecnologia* Blockchain *nei processi elettorali*

Un elemento di grave preoccupazione nell'implementazione del voto elettronico per le elezioni politiche risiede nei rischi di manipolazione e di hackeraggio cui esso è virtualmente soggetto e nei pericoli di ingerenza da parte di Stati stranieri nei processi elettorali di numerose democrazie al fine di alterarne l'esito[27].

In tempi recenti si è dunque valutata la possibilità di utilizzare, per le esperienze di *internet voting*, una tecnologia informatica che possa garantire l'espressione del voto da tali ingerenze ed in particolare l'attenzione si è appuntata su *Blockchain* ovvero quella tecnologia, nata e sviluppata in relazione alle criptovalute, che sembra offrire, tecnicamente, ampie garanzie di trasparenza, verificabilità ed immutabilità[28].

[26] Sulla tecnologia *Blockchain* in ambito elettorale si rinvia al prosieguo del testo.

[27] In una ricerca pubblicata nel 2019 sul sito dell'ASPI (*Australian Strategic Policy Institute*) è stata proposta una classificazione delle possibili interferenze che possono essere realizzate nell'ambito di un momento elettorale da parte di uno Stato straniero attraverso il supporto elettronico ed è stato sottolineato come le stesse consistono oltre che nella manipolazione dell'elettore attraverso la sua esposizione a *fake news* anche nell'hackeraggio degli strumenti infrastrutturali utilizzati, per l'espressione del voto, dallo Stato attaccato. Sul punto cfr. F. Hanson, S. O'Connor, M. Walker, L. Courtois (a cura di), "*Hacking democracies Cataloguing cyber-enabled attacks on elections*", 15 maggio 2019, reperibile sul sito https://www.aspi.org.au/ .

[28] Sul punto, ampiamente, D. Johnson, *Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values?,* in *European Journal*

La tecnologia *Blockchain* è recente, complessa e in forte evoluzione[29]. È recente in quanto, come detto, è stata sviluppata pochi anni or sono in relazione alle transazioni finanziarie con le criptovalute (in particolare in relazione a *Bitcoin*)[30]; è complessa in quanto, oltre ad essere caratterizzata da elementi tecnico informatici articolati, non è univoca in termini di definizioni e di *governance* (distinguendosi diverse tipologie: pubbliche o private, *permissionless* o *permissioned*)[31]; è in forte evoluzione in relazione all'ambizione di utilizzare tale tipo di tecnologia per applicazioni diverse da quelle per le quali inizialmente essa era stata pensata. Nelle tecnologie *Blockchains* si possono infatti ipotizzare possibili strumenti tesi a garantire la certezza e la segretezza nell'esercizio a distanza del diritto di voto, ma anche, per fare altri esempi, la certezza e la riservatezza della documentazione relativa alla salute -in specie nell'attestazione del consenso (in particolar modo quello anticipato) rispetto al trattamento medico-sanitario-, la certezza e la tracciabilità delle filiere agro-alimentari, così come la "regolazione" dell'economia circolare.

La *governance* della tecnologia *Blockchain* inizialmente pensata per le transazioni finanziarie collegate alle criptovalute (la *public and permissionless*) non è considerata attualmente adeguata a scopi pubblicistici (in relazione ai quali è considerata più corrispondente la *governance* di *Blockchain permissioned*)[32].

of Risk Regulation, 10, 2019, pp. 330 ss.

[29] Sul tema cfr. E. Navarretta, *Introduzione ai profili giuridici della tecnologia Blockchain*, in E. Navarretta, L. Ricci, A. Vallini (a cura di), *Il potere della tecnica e la funzione del diritto: un'analisi interdisciplinare di Blockchain*, 1, Giappichelli, Torino, 2021, pp. 7 ss. Cfr. anche R. Tas, Ö. Tanriöver, *A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting*, in *Symmetry*, 2020, pp. 1328 ss.; *P. Boucher*, *What if blockchain technology revolutionised voting?*, consultabile sul sito http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ ATA(2016)581918_EN.pdf; European Parliamentary Research Service, Settembre 2016.

[30] Sul tema cfr. in generale C. Poncibò, *Il diritto comparato e la Blockchain*, Memorie del Dipartimento di Giurisprudenza dell'Università di Torino, ESI, Napoli, 2020.

[31] Le *permissionless blockchain* sono ambiti del tutto pubblici ove ogni utente può liberamente partecipare e svolgere qualunque attività. Le *permissioned blockchain* sono quelle nelle quali gli utenti possono partecipare solo su invito e le attività che possono svolgere sono soggette a restrizioni. Sul tema L. Ricci, *La tecnologia del Blockchain: concetti di base*, in E. Navarretta, L. Ricci, A. Vallini (a cura di), *Il potere della tecnica e la funzione del diritto: un'analisi interdisciplinare di Blockchain*, cit., pp. 15 ss. Cfr. anche A. Miller, *Permissioned and Permissionless Blockchains*, in S.S. Shetty, C.A. Kamhhoua, L.L. Njilla (eds.), *Blockchain for Distributed System Security*, Jhon Wiley and Sons, New Jersey, 2019, pp. 193 ss.

[32] Particolarmente chiara in questo senso è E. Navarretta, la quale afferma «Nel primo

La tecnologia *Blockchain* è stata utilizzata sperimentalmente in alcuni eventi elettorali: a novembre del 2018, ad esempio, il *Thai Democrat Party* ha utilizzato *Blockchain* nelle elezioni primarie per eleggere il segretario di partito. La detta tecnologia è stata utilizzata per analizzare la partecipazione dall'estero al referendum in Colombia relativo al processo di pace con le Forze armate rivoluzionarie della Colombia (FARC)[33] ed è stata inoltre sperimentata, sempre nel 2018, alle elezioni di medio termine in West Virginia (per il voto dei militari e dei cittadini all'estero). Nel 2019 *Blockchain* è stata sperimentata alle elezioni municipali a Denver. Un test pilota è stato infine svolto per le elezioni presidenziali in Sierra Leone sempre nel 2018[34].

Cionondimeno, il dibattito sull'utilizzabilità della tecnologia *Blockchain* in eventi elettorali di larga scala è ancora molto vivace ed aperto.

Un tema in discussione, come già riferito, attiene in primo luogo alle diverse caratteristiche collegate alle varie tipologie di *governance* di

solco di indagine è irrinunciabile confrontarsi con la ben nota dicotomia che separa i public and permissionless blockchain systems dai permissioned (tanto public quanto private) blockchain systems, rispetto alla quale una più attenta analisi consente di sfatare più d'un luogo comune. La tipologia public and permissionless (si pensi a Bitcoin, Ethereum o Dash), nel potenziare la struttura decentralizzata senza porre limiti di accesso (e per questo definita pubblica), ha alimentato la narrazione della massima democraticità e autosufficienza del sistema, ma, in effetti, ha disvelato non pochi profili di criticità. Il modello, da un lato, non si dimostra in senso stretto paritario, poiché valorizza i soggetti con maggiori capacità computazionali (e risorse energetiche a basso costo), che consentono di risolvere l'hash e di svolgere il ruolo di miners. Da un altro lato, con il suo preteso autoregolamentarsi sulla base di un consenso assoluto, finisce per tradursi in un'organizzazione di tipo "tribale", nella quale o si condividono le scelte relative alle regole della rete o resta solo l'opzione to branch out, e, quindi, la scelta di generare un'autonoma biforcazione. Non stupisce, dunque, che la capacità di blockchain di "creare fiducia attraverso la disintermediazione", riconosciuta dalla Risoluzione del Parlamento Europeo (2018/2085), in realtà si rivolga fondamentalmente a tipologie non destrutturate, bensì a blockchain di tipo permissioned. Queste o limitano l'accesso al ruolo di miners, assegnandolo a nodi fidati che assumono una veste istituzionale rispetto alla rete (masternodes), seppure la comunità degli utenti resti aperta (blockchain permissioned pubbliche, quali sono Ripple o Neo), o limitano lo stesso accesso alla rete a soli utenti selezionati e il mining a nodi qualificati (blockchain permissioned private, quali sono Chain e Bankchain)», *Introduzione ai profili giuridici della tecnologia Blokchain*, cit., pp. 8-9.

[33] Su questo caso cfr. C. van Ooijen, *How Blockchain Can Change Voting: The Colombian Peace Plebiscite. Case Study From the 2017 OECD Report: Embracing Innovation in Government*, reperibile all'url: https://web-archive.oecd.org/2017-02-08/427225-embracing-innovation-in-government-colombia.pdf .

[34] I detti casi sono riportati nel sito: https://www.eublockchainforum. eu/search/node?keys=voting. Cfr. inoltre, D. Carboni, M. Simbula, *La blockchain per proteggere il voto dall'interferenza straniera: troppi problemi*, in *Agenda Digitale*, 28 agosto 2019.

Blockchain: esse sono rilevanti giacché nessuna sembra essere, attualmente, del tutto completamente idonea a soddisfare i requisiti di segretezza, decentramento (e dunque non manipolatività) e velocità necessari ad un evento elettorale complesso quale, ad esempio, le elezioni politiche di uno Stato democratico. Difatti solo le *Blockchains permissioned* possono assicurare del tutto la segretezza del voto e, nondimeno, solo le *Blockchains permissionless* sono completamente decentralizzate, caratteristica che garantisce la cosiddetta "disintermediazione" e dunque l'impossibilità (quasi completa) di modificare i dati del registro distribuito e dunque scongiurare possibili frodi elettorali[35].

Il tema della velocità delle transazioni elettorali è invece collegato alla questione della cosiddetta *scalability*[36]. Anche in relazione ad esso si evidenzia come «le *blockchain permissioned* sono in grado di processare transazioni velocemente (fattore fondamentale in un processo elettorale su larga scala) ma sono controllate da enti privati. Viceversa, le *blockchain permissionless* sono decentralizzate ma non sono in grado di rispondere alle esigenze collegate a votazioni su larga scala»[37]. La *governance* di tipo *permissioned*, dunque, sembra maggiormente adatta a scopi pubblici sotto alcuni profili (quantomeno in relazione al tema della *scalability*) e tuttavia è soggetta al rischio definito come "*dominating power*" ovvero alla minaccia della possibile posizione di "egemonia tecnologica" che potrebbero assumere le società private incaricate di sviluppare le tecnologie necessarie per il voto tramite *Blockchain*[38].

Oltre alle problematiche descritte le tecnologie *Blockchains* non risolvono tuttora, peraltro, alcune questioni critiche che si evidenziano tipicamente nelle elezioni elettroniche ovvero, ad esempio, alcune problematiche connesse all'identificazione certa dell'elettore ed alle garanzie dell'espressione del voto completamente libera[39]. La tecnologia Blockchain

[35] Sul punto cfr. F. Martines, *I principi internazionali in materia di processi elettorali e le tecnologie Blockchain*, in E. Navarretta, L. Ricci, A. Vallini (a cura di), *Il potere della tecnica e la funzione del diritto: un'analisi interdisciplinare di Blockchain*, cit., pp. 33 ss

[36] L'espressione *scalability* indica la velocità con cui il programma processa i dati e ottiene i consensi necessari al suo funzionamento a mano a mano che si aggiungono nuovi utenti. Cfr. sul punto A. Gopalan, A. Sankararaman, A. Walid, S. Vishwanath, *Stability and Scalability of Blockchain Systems*, in *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 4 (2), pp 1-35.

[37] F. Martines, *I principi internazionali in materia di processi elettorali e le tecnologie Blockchain*, cit. p. 40

[38] Sul punto cfr. S. Park, M. Specter, N. Narula, R. L. Rivest, *Going from Bad to Worse: From Internet Voting to Blockchain Voting*, in *Journal of Cybersecurity*, 7(1), 2021.

[39] L'espressione *scalability* indica la velocità con la quale un sistema blockchain processa i dati

non può porre infatti rimedio elle possibili ingerenze "fisiche" sull'elettore che vota da remoto: tale problematica, molto sentita nel contesto italiano, è meno rilevante in altre esperienze nazionali (si pensi alla svizzera o agli Stati uniti) ove è ampiamente diffuso il voto per posta che da sempre presenta questioni di tale genere.

Le complessità delle dette tecnologie, inoltre, sembrano essere attualmente incompatibili con la necessaria fiducia nei processi elettorali da parte dei cittadini votanti che è presupposto fondamentale per conferire legittimazione agli esiti del medesimo processo elettorale[40].

Non sembra un caso, dunque, che persino esponenti del mondo accademico, scientifico e tecnologico particolarmente accreditati abbiano dubitato esplicitamente dell'attuale utilizzabilità delle tecnologie *Blockchains* nei processi elettorali complessi.

Significativa risonanza ha avuto, ad esempio, un noto articolo del novembre 2021 redatto da alcuni ricercatori del MIT e dell'Università di Harvard particolarmente accreditati i quali hanno messo in discussione l'opportunità dell'utilizzo della tecnologia *Blockchain* per i processi elettorali[41] sottolineando che, come prima accennato, a fronte del fatto che *Blockchain* non risolve alcune problematiche connesse al voto elettronico (la garanzia della libertà di espressione del voto in formato elettronico espresso dal cittadino che vota in modalità decentrata), la medesima tecnologia e la sua complessità rendono difficile allo stesso elettore la comprensione delle modalità attraverso cui è "processata" l'espressione della propria volontà politica (minando la fiducia nei conseguenti risultati e, dunque, la legittimità dell'intero processo elettorale). I medesimi ricercatori hanno inoltre evidenziato come la tecnologia *Blockchain* non è del tutto immune a manipolazioni e, nondimeno, la sorveglianza su di essa è particolarmente complessa. A fronte di tali aspre critiche il dibattito rimane ad oggi aperto nella considerazione dell'attuale necessità di aggiornare le pratiche di voto alla modernità contemporanea e della altresì importante esigenza di

e verifica il consenso degli utenti. Le *public permissionless blockchains* registrano performance in termini di *scalability* meno brillanti delle *private permissioned blockchains*. Sul tema M. Scherer, *Performance and Scalability of Blockchain Networks and Smart Contracts*, *Dissertation*, 2017. Reperibile all'url: https://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-136470 .

[40] Si rinvia a tal proposito al Piano d'azione per la democrazia europea COM(2020)790 final, punoto2,3. sul tema più in generale cfr. L. Fabiano, *Crisi dello Stato democratico Rappresentativo, partecipazione politica elettronica e consapevolezza della società civile*, in *federalismi.it*, 28, 2023.

[41] Cfr. S. Park, M. Specter, N. Narula, R. L. Rivest, *Going from Bad to Worse: From Internet Voting to Blockchain Voting*, cit.

garantire che tale aggiornamento rappresenti un modo migliore (garantito meglio, più veloce, più economico ecc.) di svolgere i processi elettorali.

Sembra dunque incredibilmente ancora attuale la frase pronunciata da Prometeo, nell'opera di Eschilo "Prometeo incantato" ove il protagonista (che pure è colui che ha fornito agli uomini il fuoco animando in loro il concetto di tecnologia) rispondendo al Coro che gli chiede se sia più forte la natura o la tecnica, afferma con sicurezza: «la tecnica è di gran lunga più debole della necessità che governa le leggi della natura»[42].

Abstract

The so-called "digital age" is marked by a particularly profound relationship between private powers and public interests. The electronic tool for electoral expression is one area where this partnership is realized. This conceals a pervasive, even distorting potential. The work investigates this complex topic.

It assesses the issues that legal systems that have implemented or tried out electronic voting have encountered. It also examines the margins for implementing emerging Blockchain technology in this field.

Keywords: Electronic-voting; Democracy; Representation; Elections, Parliament; Blockchain.

[42] Eschilo, *Prometeo incatenato*, v. 514: τέχνη δ' ἀνάγκης ἀσθενεστέρα μακρῷ («la tecnica è di gran lunga meno potente della necessità»), dove per «necessità» – ἀνάγκη – si intende qui quel principio che «regola la natura e la scansione del suo ciclo che nessun progetto umano può infrangere e di fronte al quale ogni espediente tecnico dimostra il suo limite». U. Galimberti, *Psiche e techne. L'uomo nell'età della tecnica*, Feltrinelli, Milano, 1999, pp. 51-52. Sul punto cfr. anche G. Canè, *La lezione di Prometeo e il filologo nell'era digitale*, in *Diacronie* [Online], 10 (2), 2012, http://journals.openedition.org/diacronie/2880; DOI: https://doi.org/10.4000/diacronie.2880.