CONSULTA ONLINE
PERIODICO TELEMATICO ISSN 1971-9892

2023 FASC. II

(ESTRATTO)

MARCO LADU – NADIA MACCABIANI

L'AUTODETERMINAZIONE POPOLARE NELL'ERA DIGITALE: TRA OPPORTUNITÀ NORMATIVE E TECNOLOGICHE

3 GIUGNO 2023

IDEATORE E DIRETTORE RESPONSABILE: PROF. PASQUALE COSTANZO

Marco Ladu – Nadia Maccabiani
L'autodeterminazione popolare nell'era digitale: tra opportunità normative e tecnologiche*

ABSTRACT (EN): ***The paper, after a brief introduction of the risks and opportunities entailed by the digital transformation process in respect of the right to vote, focuses on some legal (§ 4) and technological (§ 3) developments in order to understand in which terms they intersect with the constitutional purposes that referendum underlie (i.e. the strengthening of popular self-determination). In this last respect, any new right is requested but rather the enhancement of traditional principles and rights by means of further specific "qualifications" that aims at reinforcing both, the awareness and empowerment of the voter. Consequently, the pivotal issue falls on the implementation of those prerequisites that support the voter's ability to take "direct decisions" for the collective life by means of technological tools functional to his empowerment (what we deem could be found in the double arrangement between referendum and technological systems like blockchain and gamification), as well as by means of regulatory tools functional to his awareness (what we deem could be found in the address followed by some European initiatives that support equity and transparency).***

1. *Il perimetro della ricerca*

Lo scritto, nel prendere atto delle sfide ed opportunità (v. *infra*, §§ 2-3) che il processo di trasformazione digitale comporta per gli istituti di democrazia diretta[1] e, più in generale, per il diritto di voto[2], si sofferma su alcuni recenti sviluppi di natura tecnologica e normativa che sembrerebbero condividere la *ratio* giuridico-costituzionale dell'istituto referendario: la valorizzazione dell'autodeterminazione popolare.

Al riguardo, gli "accorgimenti" di natura normativa (contemplati in recenti iniziative europee: v., *infra*, § 4) e la strumentazione tecnologica (*blockchain*, *gamification:* cfr., *infra*, § 3) sui quali si porrà l'accento, pare possano contribuire al perseguimento di tale finalità senza tuttavia passare attraverso la configurazione di "nuovi diritti", quanto piuttosto introducendo ulteriori "qualificativi", rispetto a diritti e principi già esistenti, essenziali per le dinamiche politico-democratiche (in termini, come si vedrà, di trasparenza, equità, sicurezza ed affidabilità).

Questi strumenti, di natura tecnologica e normativa, risultano quindi accomunati da un *idem sentire*, volto al rafforzamento dell'*awareness* e dell'*empowerment*[3] dell'individuo, che viene

---

* *Il presente contributo, frutto di una riflessione condivisa tra gli autori, è direttamente riferibile, quanto ai §§ 2.2, 3, (3.1, 3.2 e 3.3) a Marco Ladu, e, quanto ai §§ 1, 2 (2.1), 4 (4.1) e 5 a Nadia Maccabiani*.

[1] Per una distinzione degli strumenti di democrazia diretta si veda J. ORGAN, *Direct Citizen Participation in the EU Democratic System*, in A. ALEMANNO, J. ORGAN, *Citizen Participation in Democratic Europe: what next for the EU?* ECPR Press, London-New York, 2021, 43-57.

[2] P. COSTANZO, *La democrazia digitale (precauzioni per l'uso),* in *Diritto Pubblico*, n. 1/2019, 71 ss.

[3] Volendo seguire la "scala" proposta da S.R. ARNSTEIN, *A ladder of citizen participation*, in *Journal of the American Planning Association*, vol. 35, n. 4/1969, 216 ss., l'*empowerment* è il massimo grado della partecipazione popolare perché si traduce in un *decision-making* paritario, non solo del potere pubblico, ma anche del popolo (gli altri due gradini della scala sono l'*enablement* e l'*engagement*).

"posto al centro" e "potenziato", mediante le richiamate "qualificazioni" ulteriori di principi e diritti tradizionali (tra cui spiccano il principio personalista, democratico e, con essi, il diritto di voto ed i presupposti diritti di pensiero e informazione). Tale connubio alimenta un circolo virtuoso che vede protagoniste, da un lato, le "potenzialità" ammesse dalle nuove tecnologie, dall'altro lato, una maggiore consapevolezza dell'elettore edificata su nuove basi normative che (come detto) implementano con "qualificativi" ulteriori categorie classiche di diritti e principi, creando presupposti funzionali all'autodeterminazione popolare (finalità primigenia e tipica dell'istituto referendario).

Simile mutua implementazione ci pare tanto più importante nella realtà odierna dove «Referendum democracy is a growing feature of constitutional politics in Europe»[4] e – per conseguenza – adeguate garanzie vanno edificate per uno strumento che consegna al popolo decisioni definitive, prive di intermediazioni partitiche o istituzionali[5], e che pertanto scopre ancor più il fianco della carica "costituzionalmente lesiva" di alcuni aspetti dell'ambiente digitale. Da qui l'importanza del "mezzo", sia esso normativo o tecnologico, volto a meglio strutturare la presupposta autodeterminazione degli elettori. Per far sì che questi, quali *inforgs*, nell'era dell'*onlife*[6], sappiano orientarsi e – per conseguenza – consapevolmente autodeterminarsi, a fronte dell'espandersi dei rischi legati alla manipolazione e, con essa, alla banalizzazione[7] della partecipazione politica[8].

---

[4] E. CASANAS ADAM, D. KAGIAROS, S. TIERNEY, *Democracy in Question? Direct Democracy in the European Union*, in *European Constitutional Law Review*, vol. 14, n. 2/2018, 262.

[5] F. BASSANINI, *I corpi intermedi nella democrazia del XXI secolo: la sfida della disintermediazione,* in F. Bassanini, T. Treu, G. Vittadini (a cura di), *Una società di persone? I corpi intermedi nella democrazia di oggi e di domani*, Bologna, 2021, 310-311, «La complessità delle forme e degli strumenti di partecipazione propria delle democrazie moderne si riduce alla partecipazione ai referendum e alla adesione atomistica alle scelte del leader, a loro volta attentamente calibrate e sapientemente comunicate in modo da favorire l'"effetto gregge"»; in questo contesto la «deriva plebiscitaria e populista… è la sensazione largamente diffusa, non solo nel nostro Paese, che la globalizzazione, la rivoluzione tecnologica, le migrazioni di massa, da un lato, e l'affermarsi di poteri sovranazionali (i mercati, la finanza globale, l'Unione europea, le agenzie di rating) dall'altra, abbiano sottratto ai cittadini (al popolo sovrano) il controllo sulle scelte dalle quali dipende il loro futuro; e che dunque l'unica possibilità *to take back control* sia quella di esprimersi direttamente nei referendum o delegare i poteri a un capo che possa rappresentare la volontà della maggioranza».

[6] L. FLORIDI, *La quarta rivoluzione – Come l'infosfera sta trasformando il mondo,* Milano, 2017, 45 ss., osserva che «la transizione dall'analogico al digitale e la crescita esponenziale di spazi informazionali in cui trascorriamo sempre più tempo illustrano con massima evidenza il modo in cui le ICT stanno trasformando il mondo in un'infosfera… Nell'infosfera, popolata da enti e agenti parimenti informazionali e in cui non vi è differenza fisica tra *processori* e *processati,* anche le interazioni divengono informazionali… Si è soliti fare riferimento a tale recente fenomeno con una varietà di espressioni: dalla "computazione ubiquitaria" all' "ambiente intelligente", dall' "Internet delle cose" alla "realtà delle cose aumentate dal web". Per quanto mi riguarda preferisco parlare di *esperienza onlife…* La graduale informatizzazione degli artefatti e dell'intero ambiente (sociale) fa sì che sia diventato difficile rappresentarsi come fosse la vita in epoca predigitale… nel prossimo futuro la distinzione tra *onlife* e *offline* è destinata a divenire ancora più sfumata e quindi a scomparire». Ne deriva che il modo con il quale concepiamo noi stessi, anche nella relazione con l'ambiente digitale in cui interagiamo, al quale spesso deleghiamo o esternalizziamo ricordi, decisioni, compiti e attività varie con modalità sempre più integrate con le nostre vite, comporta, quale conseguenza, che «abbiamo iniziato a concepire noi stessi come inforg, non attraverso qualche trasformazione biotecnologica del nostro corpo, ma, più seriamente e realisticamente, attraverso la radicale trasformazione del nostro ambiente e degli agenti che vi operano… in molti contesti le ICT hanno già iniziato a essere la squadra che gioca "in casa", nell'infosfera, con noi che giochiamo "in trasferta"», fungendo spesso da parte integrante di un meccanismo utile alle ICT per funzionare (p. 167).

[7] S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997, 55 ss.

[8] Come recentemente messo in evidenza, sia pure contestualizzato alla raccolta digitale delle sottoscrizioni referendarie, ma con osservazioni di più ampio respiro da F. PALLANTE, *Referendum digitali e autodelegittimazione del Parlamento,* in *Osservatorio Costituzionale*, n. 6/2021, 344 ss.

Accanto a queste considerazioni preliminari, si deve altresì ricordare che la dottrina non è unanime nel ritenere efficace il processo di digitalizzazione delle procedure democratiche, in particolare in termini di incremento della partecipazione dei cittadini alla vita politica (il c.d. *engagement*)[9]. Preso atto di questa incertezza, l'approccio che qui si intende assumere è di evitare ogni "fideismo digitale", per adottare piuttosto un approccio giuridico-costituzionale di natura pragmatica.

In questo senso, ciò che assume qui rilievo non è tanto se e in che misura la digitalizzazione dei processi elettorali sia in grado di stimolare l'*engagement* dei cittadini (essendo, questa, un'analisi complessa e che senz'altro coinvolge valutazioni di impatto e saperi diversi da quello giuridico); quanto, piuttosto, soffermarsi (come detto) su quei requisiti giuridici e tecnologici che – in combinato disposto – si pongono in aderenza ad una finalità di stampo immanentemente giuridico-costituzionale, peraltro sottesa allo stesso referendum. Finalità che trova il proprio fondamento nel cuore del diritto costituzionale vale a dire nel principio personalista, il quale pone al centro la persona, la sua dignità e la sua capacità di autodeterminazione, che ancor più debbono essere valorizzati nel momento democratico in cui viene ad essa attribuito il potere di assumere, attraverso l'attivazione della leva referendaria, decisioni giuridicamente vincolanti e definitive.

Se risulta quantomeno condivisibile in linea generale la premessa sino ad ora svolta, il punto di partenza che consente di sviluppare il ragionamento sotteso al presente scritto non può che consistere in un approccio meramente ricognitivo, che si traduce nella presa d'atto di alcune evidenze. Da un lato, infatti, occorre prendere atto del carattere di "manipolatività" al quale l'*onlife* ci espone (v., *infra*, § 2). Dall'altro lato, si osserva la crescente emersione di nuove tecnologie (la *blockchain* e le DLTs, di cui si dirà: v., *infra*, §§ 3.2, 3.3) e di alcune loro estensioni (la *gamification*, cfr., *infra*, § 3.1) le quali sono tutte suscettibili di "qualificare" e supportare ulteriormente le finalità giuridico costituzionali collegate all'esercizio, in particolare, del diritto di voto[10].

Una simile ricostruzione, tuttavia, presuppone necessariamente il portato di scienze diverse da quella giuridica, *in primis* quelle informatiche e, come si vedrà, anche quelle comportamentali (v., *infra*, §§ 2 e 3). Nel contesto di questa dimensione interdisciplinare sia ben inteso che deve continuare a competere al giurista (ed al giurista costituzionalista nello specifico) il compito di soffermarsi sui termini entro i quali i nuovi strumenti offerti dall'evoluzione tecnologica (e, conseguentemente, normativa) possano non solo rispettare formalmente, ma altresì contribuire alla promozione dei diritti e principi costituzionali esistenti che, nel caso di specie, si traducono nella valorizzazione dell'autodeterminazione popolare (v., *infra*, §§ 3 e 4).

Simile constatazione "metodologica" ha altresì portato a far emergere un mutamento di prospettiva del legislatore europeo, traducibile in una "chiamata in corresponsabilità" del singolo individuo, in ragione dell'evidenza che, in un contesto tanto complesso quanto multidimensionale come quello della trasformazione digitale, il "paternalismo" pubblico non basta. Questa "chiamata in corresponsabilità" diventa poi particolarmente significativa per l'istituto referendario, tanto più laddove lo si intenda strutturare per via elettronica. Da un lato, infatti, la già rammentata definitività dell'esito nonché la presupposta mancanza di intermediazioni richiede, *a fortiori*, una necessaria quanto diretta "responsabilizzazione" dei partecipanti; dall'altro lato, è tuttavia necessario che gli elettori siano adeguatamente "attrezzati" attraverso i menzionati "qualificativi" con i quali è ulteriormente contornato e

[9] Come sottolineato da A. MACINTOSH, A. WHYTE, *Towards an evaluation framework for eParticipation.* Transforming Government, in *People, Process & Policy*, vol. 2, n. 1/2008, 16-30

[10] Per l'uso della tencnologia come regulatory managment tool, cfr. R. BROWNSWORD, *Law, Technology and Society – Re-imagining the regulator environment*, Routledge, New York, 2019.

"puntellato" il diritto di voto (la trasparenza e equità dell'infosfera[11], in cui si formano le opinioni; la sicurezza e affidabilità del voto elettronico: cfr., *infra*,§§ 3-4). È in questo contesto che si "chiude il cerchio" dell'a*wareness* e dell'*empowerement* dell'individuo attraverso mediazioni – giuridiche e tecnologiche – che assolvono un ruolo di supporto alla promozione dell'autodeterminazione popolare mediante referendum.

In merito, sia concesso un ultimo appunto: l'approccio metodologico e la finalità dello scritto non derivano da mera speculazione teorica. Da un lato, la normativa europea, come si vedrà (*infra* § 4), sta ponendo le basi per l'edificazione di una maggiore trasparenza e consapevolezza da parte degli individui, ormai immersi nella *onlife*. Dall'altro lato, i pubblici poteri si stanno dimostrando sempre meno refrattari all'uso delle nuove tecnologie[12], oltre che nell'*e-government*[13], per scopi di partecipazione politica (*e-democracy*)[14], anche mediante *blockchain* (v., *infra*, § 3.2). Con altre e significative parole: «the fact of the matter is that institutional systems are highly imperfect, no less so than technological systems, and only a combination of the two is likely to address the vulnerability of individuals to the diverse sources of power and coercion they face»[15].

2. *Transizione digitale e diritto di voto*

Le attuali sfide poste dalla trasformazione digitale si innestano nel punto di intreccio tra la libertà di espressione, il diritto all'informazione e il diritto di voto[16], il che equivale al punto in cui affondano le proprie radici la democrazia costituzionale e il principio personalista[17].

Numerosi documenti internazionali ed europei dichiarano la consapevolezza dei rischi che tali libertà e diritti fondamentali corrono nell'epoca di una rapida transizione digitale. Il *Rapporto sui rischi globali del 2023* rinnova la preoccupazione per la disinformazione, dopo averla inclusa, già nel 2022, nell'elenco dei rischi globali attuali[18].

---

[11] L. FLORIDI, cit.

[12] Cfr. gli spazi di sperimentazione normativa (Art. 53) previsti dalla proposta di regolamento europeo sull'Intelligenza Artificiale, in merito, per un approfondimento cfr. F. DI PORTO, A. SIGNORELLI, *Regolare attraverso l'intelligenza artificiale*, Bologna, Il Mulino, 2022.

[13] L. TORCHIA, *Lo Stato Digitale – Una introduzione*, Bologna, 2023, 97 ss. L'amministrazione digitale include ormai non solo la digitalizzazione delle procedure amministrative, ma anche l'utilizzo di algoritmi per lo svolgimento automatizzato di valutazioni, previsioni, decisioni. Con specifico riguardo alle implicazioni in termini di legittimità delle decisioni amministrative algoritmiche, cfr. S. CIVITARESE MATTEUCCI, *«Umano troppo umano». Decisioni amministrative automatizzate e principio di legalità*, in *Diritto pubblico*, n. 1/2019, 5 ss.

[14] Sui diversi significati della *e-democracy*, cfr. P. COSTANZO, *La democrazia elettronica (note minime sulla cd. e-democracy)*, in *Dir. inform.*, 2003, 465 ss. Così, per un approfondimento, si veda G. FIORIGLIO, *Democrazia elettronica. Presupposti e strumenti*, CEDAM, Padova, 2017.

[15] Y. BENKLER, *Degrees of Freedom, Dimensions of Power*, in *Doedalus, the Journal of the American Academy of Arts & Sciences*, n. 1/2016, 29.

[16] Cfr. ex plurimis, D. BUTTURINI, *Le notizie false su internet e il ruolo delle piattaforme digitali*, in G. Ferri (eds.), *Diritti costituzionale e nuove tecnologie*, Edizioni scientifiche italiane, Napoli, 2022, 79; F. DONATI, *Democrazia, pluralismo delle fonti di informazione e rivoluzione digitale*, in federalismi.it, n. 23/2013; MEOLA F., *Tecnologie digitali e* neuro-marketing *elettorale. A proposito di una possibile regolamentazione delle nuove forme di propaganda politica*, in Costituzionalismo.it, n. 1/2020; M. MEZZANOTTE, *Fake news nelle campagne elettorali digitali. Vecchi rimedi o nuove regole?* in federalismi.it, n. 24/2018.

[17] L. FERRAJOLI, *La costruzione della democrazia – Teoria del garantismo costituzionale*, Laterza, Bari-Roma, 2021, 235

[18] *World Economic Forum's Global Risk Report* – 2023, 24: «"Misinformation and disinformation" are, together, a potential accelerant to the erosion of social cohesion as well as a consequence. With the potential to destabilize trust in information and political processes, it has become a prominent tool for geopolitical agents to propagate extremist beliefs and sway elections through social media echo chambers».

Anche l'Unione Europea include la *disinformation* e la *misinformation* tra i rischi sistemici per i processi democratici[19]: il Regolamento UE n. 2065/2022 (DSA) statuisce, infatti, che la disinformazione o le attività di manipolazione e abuso sono rischi sistemici concreti ed effettivi per la democrazia e la società[20]. Inoltre, come sottolineato dalla proposta dell'UE sull'intelligenza artificiale (AIA), quest'ultima può «essere utilizzata impropriamente e… fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento e controllo sociale. Tali pratiche sono particolarmente dannose e dovrebbero essere vietate poiché contraddicono i valori dell'Unione relativi al rispetto della dignità umana, della libertà, dell'uguaglianza, della democrazia e dello Stato di diritto e dei diritti fondamentali dell'Unione»[21]. La proposta vieta, quindi, pratiche di intelligenza artificiale «che presentano un elevato potenziale in termini di manipolazione delle persone attraverso tecniche subliminali, senza che tali persone ne siano consapevoli, oppure di sfruttamento delle vulnerabilità di specifici gruppi»[22].

Nella proposta di regolamento sulla pubblicità politica, inoltre, l'UE ha ammesso che «La pubblicità politica può essere un vettore di disinformazione, specie se non ne è esplicitata la natura politica e se è mirata»[23]. A questo proposito, «I dati personali raccolti direttamente presso i cittadini o ottenuti dalle loro attività online e con profilazione comportamentale e altre analisi sono usati per indirizzare messaggi politici a cittadini, con pubblicità che prende di mira gruppi, e per amplificarne l'impatto e la diffusione personalizzando contenuto e diffusione in funzione di caratteristiche determinate grazie al trattamento di dati personali e la loro analisi»; ciò che produce «precise ripercussioni negative sui diritti dei cittadini, tra cui la libertà di opinione e di informazione, nel prendere decisioni politiche ed esercitare il diritto di voto»[24]. Più specificamente, «visto il potere e il potenziale insiti in un uso improprio dei dati personali nel *targeting*, compreso il *microtargeting* e altre tecniche avanzate, tali tecniche possono costituire una minaccia particolare per legittimi interessi pubblici quali l'equità, le pari opportunità e la trasparenza del processo elettorale e il diritto fondamentale a un'informazione obiettiva, trasparente e pluralistica»[25].

Tanto considerato, è quindi evidente la presa di coscienza degli amplificati rischi cui oggi è sottoposto il diritto all'autodeterminazione, anche politica, quindi il diritto a un voto libero e personale[26].

La sfida va, pertanto, affrontata su un duplice fronte: in primo luogo quello – più generale e omnicomprensivo – della *onlife* degli *infosgs*[27]; in secondo luogo quello – più specificamente riferito all'istituto referendario – del *design* del quesito referendario e della strumentazione elettronica su cui possono essere strutturare le procedure di voto. Tuttavia, prima di entrare nel

[19] Regolamento UE n. 2065/2022, considerando n. 79 e n. 82; proposta di Regolamento relativo alla trasparenza e al *targeting* nella pubblicità politica – COM(2021) 731 final – considerando n. 4 e n. 5.

[20] Regolamento UE n. 2065/2022, considerando n. 104

[21] COM(2021) 206 final, considerando n. 15.

[22] COM(2021) 206 final, par. 5.2.2.

[23] COM(2021) 731 final, considerando n. 4.

[24] COM(2021) 731 final, par. 1.

[25] COM(2021) 731 final, considerando n. 5.

[26] Sui mutamenti intervenuti nella "public sphere" di habermasiana e weberiana memoria nonché sui conseguenti rischi per la libertà di pensiero e di informazione, cfr. M. KÖKCÜ, *Global Transformation of the Public Sphere in the Digital World: From Public to Silent Sphere?*, in *Academia Letters*, Article 3018/2021; E. LONGO, *Rivoluzione digitale e sviluppi della partecipazione democratica nell'Unione europea*, in *Osservatorio sulle fonti*, n. 3/2021, 1313, "la sfera digitale offre strumenti che rendono molto facile la manipolazione mirata su scala globale, senza offrire alcuna forma di trasparenza, né esiste una disciplina chiara degli attori nell'ecosistema pubblicitario o dei processi proprietari sottostanti".

[27] L. FLORIDI, *La quarta rivoluzione – Come l'infosfera sta trasformando il mondo, c*it.

merito di tali fronti (v, *infra*, §§ 3 e 4), sia consentito un breve *excursus* sulla portata dei rischi in oggetto.

2.1. *L'amplificarsi degli strumenti di manipolazione*

La questione del ricorso ai referendum come strumenti di manipolazione politica non è nuova, come del resto ben evidenziato già da Lipjhart[28]. Ciò che semmai rappresenta una novità è la pervasività e viralità degli strumenti di manipolazione attualmente messi a disposizione dalla tecnica, in ragione del rapido sviluppo delle nuove tecnologie e del loro connubio con le scienze comportamentali. Al riguardo, come anticipato, l'attenzione sarà prima posta – in prospettiva più generale e comprensiva – sui rischi posti dall'ambiente digitale entro il quale gli elettori formano le loro opinioni *(a)*, per poi scendere nel dettaglio della formulazione dei quesiti referendari e delle insidie ad essa sottese *(b)*.

(a) Anzitutto potremmo evocare dei "rischi sistemici" che l'ambiente digitale pone al diritto di voto[29], tra cui rientrano, a titolo di esempio, alcuni concetti sintetizzabili in cosiddette *buzzwords*: *disinformation, malinformation, misinformation*[30] e *hate speech*. Il potenziale nocivo di tali approcci risulta incrementato dal ricorso a pratiche di profilazione comportamentale e *micro-targeting*[31]. A questo proposito, vi è chi ha osservato come «Social media can shape ideas and redesign society. It can increase sensitivity and strengthen the social response. Anything can become a reality through social media, and society can become part of this simulated or artificial world. Social media can manipulate reality to weaken the administration, society, military, or economy of a country»[32].

In questo contesto, i mezzi per diffondere la disinformazione sono molteplici (*bot, botnet, troll, account* hackerati o rubati, strategie di propaganda)[33] e la loro efficacia è stata dimostrata

[28] A. LIPJHART, *Democracies: patterns of majoritarian and consensus government in 21 countries*, Yale, 1984, 197 ss.

[29] H. ALCOTT, M. GENTZOKOW, *Social Media and Fake News in the 2016 Election,* in *Journal of Economic Perspectives*, Vol. 31, No. 2/2017, 211 ss.

[30] Secondo *l'High-Level Expert Group on Fake News and Online Disinformation (HLEG*) della Commissione Europea, il termine "fake news" non è dotato di adeguata carica descrittiva rispetto alla disinformazione, intendendosi per quest'ultima «all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit», cfr. *High level Group on fake news and online disinformation, A multi-dimensional approach to disinformation*, 2018, 10,. Secondo quanto precisato da M.F. COMMON, R.K. NIELSEN, *Submission to UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression – Report on disinformation*, 15 febbraio 2021, per disinformazione si intendono «false information that is created and spread, deliberately or otherwise, to harm people, institutions and interests»; per *misinformation* si intende «false or misleading information, spread without intent to harm», e per *malinformation* si intende «information that is not false, but strategically used with intent to harm». Secondo gli Autori «behaviours and forms of expression discussed under the heading disinformation often overlap with misinformation… and malinformation… and with wider discussions under the imprecise and misleading but frequently used term "fake news"», ne deriva pertanto «the lack of conceptual clarity in defining the problem, and frequent lack of substantial agreement what exact kinds of behaviour and content are problematic, are… parts of the problems we face in addressing these problems».

[31] E. LONGO, Rivoluzione *digitale e sviluppi della partecipazione democratica nell'Unione europea*, cit., 1327, "le campagne elettorali online sono diventate tanto più efficaci quanto sfruttano meccanismi molto dubbi come la profilazione psicologica, tecniche complesse di microtargeting e altri metodi di *digital nudging*".

[32] L. CHEN, J. CHEN, C. XIA, *Social network behavior and public opinion manipulation*, in *Journal of Information Security and Applications*, n. 64/2022, 2.

[33] Benché la dottrina non sia giunta ad una definizione condivisa e univoca di "propaganda", è convinzione comune che si sostanzi nel condizionamento, la manipolazione ed il controllo delle opinioni e dei comportamenti per una pluralità di obiettivi, tra cui campagne pubblicitarie politiche, soprattutto durante il periodo elettorale; il tentativo dei movimenti ideologici di influenzare e raccogliere *followers*, oppure l'attività di governi di Paesi terzi

da specifiche ricerche sulla *social media warfare*, sulle cc.dd. armi psicologiche nelle mani dei *social media*[34] e sugli orientamenti degli utenti *social*: «Social media can quickly push selected information to hundreds of millions of target audiences in the form of pictures and texts, which affects the target audience's views and attitudes towards the event»[35]. Ciò può accadere per le più svariate finalità, senz'altro anche politiche[36], come dimostrano gli accadimenti di *Capitol Hill*[37], in Myanmar[38] o le elezioni brasiliane[39] (certo è che rimane difficile, da un punto di vista empirico, misurare l'entità delle concrete incidenze dei *social media* rispetto ai singoli eventi)[40].

Il potenziale dannoso della disinformazione risulta, in ogni caso, rafforzato dalla "triplice alleanza" tra profilazione, *microtargeting* e scienze comportamentali[41]. La *digital footprint* degli individui è composta da una quantità crescente di informazioni significative, le quali consentono a sempre più sofisticati algoritmi di sviluppare, con crescente precisione, valutazioni e previsioni sulla personalità dei cittadini elettori[42]. Come hanno dimostrato alcuni

intenzionalmente rivolta ad incidere sulle procedure democratiche di altri Stati, cfr. J.BAYER, N. BITIUKOVA, P. BARD, J. SZAKACS, A. ALEMANNO, E. USZKIEWICZ, studio richiesto dalla Commissione LIBE - *Disinformation and Propaganda – Impact on the functioning of the rule of law in the EU and its Member States*, PE 608.864 - Febbraio 2019, 26.

[34] C. O'NEIL, *Weapons of Math Destruction – How Big Data increases inequality and threatens democracy*, New York, 2016, 63 ss.

[35] L. CHEN, J. CHEN, C. XIA, *Social network behavior and public opinion manipulation,* cit.

[36] C. SUNSTEIN, *#republic*, Princeton-Oxford, 2018, 62.

[37] L'assalto a *Capitol Hill* realizzato da parte di un gruppo di sostenitori dell'ex Presidente Donald Trump è simbolo della "forza" della disinformazione, in questo caso ricollegabile alla diffusione sui *social networks* della denuncia da parte di Trump di brogli elettorali e della conseguente vittoria "fraudolenta" dell'attuale Presidente Joe Biden. Come sottolineato da B. CARAVITA, *Davanti ad un mondo che cambia chi è più pericoloso tra Trump e Zuckerberg? Alla ricerca di una risposta che penetri nei meccanismi che governano la nostra vita in rete*, in *federalismi.it*, n. 1/2021, VII, «Trump - come tutti i populisti negli ordinamenti tendenzialmente democratici (i populisti autoritari non hanno questo tipo di problemi) - ha operato da catalizzatore di questa rabbia, ne è stato il primo incendiario sperando di essere il primo e unico beneficiario. Per far ciò Trump ha utilizzato i social, gli stessi social che adesso si rivoltano contro di lui, bandendolo o sospendendolo, come è capitato in questi giorni in cui Twitter ha definitivamente chiuso l'account di Trump è Facebook lo ha sospeso e infine Google, Amazon hanno bandito il social Parler dai propri data base»: sulla vicenda, v. P. COSTANZO, *"Social" Democracy*? in *Cultura constitucional y derecho viviente. Escritos en honor al profesor Roberto Romboli*, IV, 1135, Tribunal Constitucional. Centro de Estudios Constitucionales, lIma, 2021.

[38] In Birmania, le forze armate che hanno guidato il colpo di stato e destituito il governo democratico di Aung San Suu Kyi hanno fatto ampio uso dei social media per finalità di propaganda pro-golpe quindi per incitare violenza e odio contro i leader politici al potere, cfr. A. ALÙ - A. LONGO, in *Birmania, primo colpo di Stato "digitale": i social accettano il proprio ruolo politico*, in *Agenda Digitale.eu*, 12 marzo 2021.

[39] Analogamente a quanto accaduto negli Stati Uniti, in conseguenza del risultato elettorale che ha consegnato la vittoria al Presidente Joe Biden, anche in Brasile i sostenitori dell'ex Presidente Bolsonaro hanno utilizzato i social media, sia per diffondere false teorie di complotto in merito alle elezioni che per organizzare, attraverso l'utilizzo di un linguaggio in codice, un tentativo di colpo di stato, facendo leva su rabbia e odio popolare, cfr. M. BORGOBELLO, Brasile, i social hanno favorito il colpo di Stato: un problema irrisolto, in *Agenda Digitale.eu*, 16 gennaio 2023.

[40] Come emerge dagli approfondimenti di J.BAYER, N. BITIUKOVA, P. BARD, J. SZAKACS, A. ALEMANNO, E. USZKIEWICZ, *Disinformation and Propaganda – Impact on the functioning of the rule of law in the EU and its Member States,* cit., 36 ss., secondo cui «Causal links to concrete real-world events are notoriously hard to establish as well, rendering the assessment of effects more difficult» (p. 47).

[41] F. GALLI, F. LAGIOIA, G. SARTOR, *Consent to target advertising*, in *European Business Law Review*, vol. 33, n 4/2022, 510, ritengono che il consenso, espresso ai sensi dell'art. 9 del Regolamento UE n. 679/2016, non dovrebbe legittimare la *targeted online political adverstising* «the validity of consent should be excluded whenever targeted advertising pursues political rather than commercial goals, as in electoral propaganda. This approach could prevent undue influence over elections, politics, and public opinion. It would exclude that people can be "paid" to accept being influenced for political purposes on the basis of their characteristics and patterns of behaviour».

[42] Ciò è facilitato dai nuovi modelli di machine learning (apprendimento non supervisionato e deep-learning): J. BARTLETT, J. SMITH, R. ACTON, *The Future of political campaigning*, in *Demos*, London, 2018, 26 ss.; K.

studi proprio nell'ambito della scienza comportamentale, le probabilità di successo di un messaggio aumentano quando questo è basato su una profilazione psicometrica e, quindi, quando esso risulti adattato agli interessi e alle attitudini personali dei destinatari[43]. Sicché, il potenziale di influenza oggetto di studio delle scienze comportamentali[44] risulta a sua volta amplificato dagli strumenti messi a disposizione dalle nuove tecnologie e, precisamente, dalle tecniche di intelligenza artificiale, le quali consentono una comprensione approfondita delle emozioni e dei sentimenti personali, per poterli meglio manipolare senza che gli interessati ne siano consapevoli[45].

Se quelli di cui si è dato brevemente conto sino ad ora rappresentano alcuni nuovi e attuali rischi digitali, è altrettanto vero che invocarne la regolamentazione significa entrare in un terreno costituzionalmente scivoloso[46]. La disciplina della disinformazione è, infatti, oggetto di contestazione, sia per la difficoltà nel definire di cosa sia "vero"[47], sia per la sua stretta attinenza alla fondamentale libertà di manifestazione del pensiero[48], rispetto alla quale operano approcci diversi (tra cui spiccano in modo significativo le differenti impostazioni di Stati Uniti e Unione Europea)[49].

(b) Con specifico riguardo al "confezionamento" del quesito da sottoporre all'elettorato, invece, le scienze sociali insegnano che le modalità di formulazione della domanda possono,

---

SHAFFER, *Data versus Democracy: How Big Data Algorithms Shape Opinions and Alter the Course of History*, Apress, Colorado, 2019. Per una definizione delle diverse tecniche di intelligenza artificiale, tra cui il *machine learning*, cfr. S. RUSSEL, P. NORVIG, *Artificial Intelligence – A Modern Approach*, Pearson, Hoboken, 2021, 651 ss.

[43] B. ZAROUALI, T. DOBBER, G. DE PAUW, C. DE VREESE, *Using a Personality-profiling Algorithm to Investigate Political Micro-Targeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media*, in *Communication Research*, vol. 49, n. 8/2022, 1066 ss. Gli autori analizzato il *targeting* personalizzato osservando che sebbene la pubblicità politica abbia sempre cercato di influenzare l'elettorato e guidarne il comportamento, il *targeting* elettorale consentito dalle nuove tecnologie risulta essere più insidioso perché i cittadini non si rendono conto di essere "bersagli" di una "tailored ad", confenzionata sulla base delle loro preferenze e convinzioni. V. anche A. KOZYREVA, S. LEWANDOWSKY, R. HERTWIG, *Citizens Versus the Internet: Confronting Digital Challenges With Cognitive Tools*, in *Psychological Science in the Public Interest*, n. 3/2020, 103 ss.

[44] Le tecniche impiegate dalle neuroscienze risultano in grado di manipolare il comportamento umano attraverso la stimolazione neurale che agisce sulle emozioni e gli istinti umani, cfr. L. TAFARO, *Neuromarketing e tutela del consenso*, Napoli, 2018, 71 ss. Con specifico riguardo alle pratiche neuroscientifiche maggiormente invasive come le *Brain Computer Interfaces*, cfr. gli Atti del Convegno organizzato dall'Autorità Garante per la Privacy, *Privacy e neurodiritti – La persona al tempo delle neuroscienze*, 28 gennaio 2021.

[45] D. SCHREIBER, *Neuropolitics: Twenty years later*, in *Politics and the Life Sciences*, vol. 36, n. 2/2017, 124-125, «Neuropolitics researchers have used machine-learning algorithms to classify individuals as liberal or conservative based on brain structure or function… However, the machine learning approach allows for even more provocative applications such as "mind reading" (inferring perceptual, emotional, and cognitive states from brain imaging data) and "neuroforecasting"' (inferring the future behaviour of individuals or mass populations from brain activity in small groups of individuals)». Sulla base di questa premessa, l'Autore chiede «how long will it take until the neuromarketing techniques that are currently influencing other sectors of society come into full play in the political domain? Trends would indicate not that long. Already, some are engaged in practical neuropolitics, but the ethical implications and the threats to democratic deliberation are woefully underappreciated».

[46] Come osservato da C. PINELLI, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, in *Diritto Pubblico*, n. 1/2022, 184, «Il punto cruciale è che viene meno la stessa possibilità di individuare una falsità, per la già ricordata tendenza a trasformare la contrapposizione vero/falso in un contrasto di opinioni o di interpretazioni, e a rendere così irrilevante la prima».

[47] G. PITRUZZELLA, *La libertà di informazione nell'era di Internet,* in G. Pitruzzella, O. Pollicino, S. Quintarelli (a cura di), *Parole e Potere – Libertà di espressione, hate speech, fake news,* cit., 72 si chiede se è possibile distinguere le opinioni dalle *fake news*.

[48] Cfr. C. PINELLI, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, cit., 173 ss.

[49] O. POLLICINO, A. MORELLI, *Le metafore della rete. Linguaggio figurato,* judicial frame *e tutela dei diritti fondamentali nel* cyberspazio*: modelli a confronto,* in *Rivista AIC*, n. 1/2018, 1-24.

già di per sé, rivelarsi suscettibili di influenzare la risposta e, di conseguenza, di incidere significativamente sul risultato, nel nostro caso quello di un referendum[50]. In questo senso, la progettazione del quesito può non essere trasparente, come nel caso dell'impiego dei cosiddetti *dark-pattern* che «mislead users and lead them toward a certain decision path, hiddenly affecting their decision-making process» [51].

Anche rispetto a ciò, come per quanto descritto sub *(a)*, le possibilità di raggiungere lo scopo ne escono rafforzate laddove si faccia impiego della combinazione tra la profilazione fondata sulle tecniche di *big data analytics* e le conoscenze derivanti dagli studi comportamentali[52].

In aggiunta, ove si faccia ricorso al voto elettronico, è il *design* stesso dell'interfaccia che può contribuire ad influenzare ulteriormente l'elettorato. Lo attesta la soglia di guardia elevata dal *Digital Services Act*, laddove denuncia (e, quindi, di fatto vieta) le interfacce progettate in modo da ingannare o manipolare i destinatari del servizio o in modo da distorcere o compromettere materialmente la capacità dei destinatari di prendere decisioni libere e consapevoli[53].

Si tratta quindi di approntare precauzioni volte ad evitare quesiti referendari nascostamente fuorvianti e ingannevoli, sia nella formulazione testuale che nella interfaccia digitale (ove il voto sia elettronico), conformemente del resto a quanto richiesto dalla Commissione di Venezia in merito ai referendum: «the question put to the vote… must not be misleading…[and] must not suggest an answer» [54].

2.2. *Il voto elettronico: libero, personale e segreto?*

Il voto espresso tramite strumenti elettronici offre opportunità[55], ma sottopone altresì a significativi rischi alcune tradizionali categorie costituzionali[56], che risultano ancor più stringenti nel nostro ordinamento giuridico[57].

---

[50] C. M. KNEIER, *Misleading the Voters in Initiative and Referendum Elections in Cities*, in *DePaul Law Review*, vol. 8, n. 1/1958, 36 ss.

[51] R. DUCATO, *Spaces for legal design in the European General Data Protection Regulation*, in R. Ducato, A. Strowel (a cura di), *Legal Design Perspectives – Theoretical and Practical Insights from the Field*, cit., 198.

[52] A. Alemanno, A.L. Sibony (a cura di), *Nudge and the Law. A European Perspective*, Hart Publishing, Oxford, Portland, Oregon, 2015.

[53] Cfr. Regolamento UE n. 2065/2022, art. 25, par. 1.

[54] European Commission for Democracy through law, *Code of Good Practice on Referendums*, par. I, 3.1.

[55] Sulle sperimentazioni del voto elettronico in Italia, cfr. A. GRATTERI, *Il valore del voto. Nuove tecnologie e partecipazione elettorale*, CEDAM, Padova, 2015; L. TRUCCO, *Il voto elettronico nel quadro della democrazia digitale*, in T.E. Frosini, O. Pollicino, E. Apa (a cura di), *Diritti e libertà in internet*, 2016, 431 ss.; S. ROLANDO, *Democrazia digitale. Difficile equilibrio tra e-democracy, e-publicity, e-government*, in *Rivista italiana di comunicazione pubblica*, n. 9/2001, 21 ss.; M. ROSINI, *Il voto elettronico tra standard europei e principi costituzionali, prime riflessioni sulle difficoltà di implementazione dell'*e-voting *nell'ordinamento costituzionale italiano*, in *Rivista AIC*, n. 1/2021, 1 ss.; S. SCAGLIARINI, *Tecnologie informatiche e procedimento elettorale: un matrimonio che s'ha da fare*, in, *Liber Amicorum per Pasquale Costanzo. Diritto costituzionale in trasformazione*, I, *Costituzionalismo, reti e intelligenza artificiale*, Genova, 2020, 327 ss.; M. SCHIRRIPA, *Il voto elettronico nell'esperienza europea tra pregi e criticità*, in *federalismi.it*, n. 6/2020, 238 ss. Per la sperimentazione da ultimo introdotta con la legge di bilancio del 2020, limitatamente agli italiani all'estero e agli elettori che, per motivi di lavoro, studio o cure mediche, si trovino in un comune di una regione diversa da quella del comune nelle cui liste elettorali risultano iscritti, cfr. G. DI COSIMO, *La partecipazione nell'era digitale,* in *Osservatorio sulle fonti*, n. 2/2022, 102-103.

[56] Per un approfondimento sulle caratteristiche costituzionali del voto, cfr. M. ARMANNO, *Personale, uguale, libero e segreto. Il diritto di voto nell'ordinamento costituzionale italiano*, Napoli, 2018; M. RUBECHI, *Il diritto di voto. Profili costituzionali e prospettive evolutive*, Torino, 2016; G. CHIARA, *Contributo allo studio del diritto di voto. Appunti delle lezioni*, Milano, 2012.

[57] V. DESANTIS, *Le nuove prospettive dell'internet voting tra avanzamento tecnologico e sostenibilità giuridica*, in *Rivista AIC*, n. 4/2022, 40, "l'intera conformazione del sistema di voto, nel nostro ordinamento, present[a] degli

Semplificando, quanto alle opportunità del voto elettronico, esso può, ad esempio, agevolare in termini di "accesso" al voto le persone con problemi di disabilità e potrebbe forse contribuire ad incrementare la partecipazione e ridurre l'astensionismo involontario (ma la questione dell'astensionismo è molto complessa e l'efficacia del voto elettronico a questo scopo è - come sopra accennato - contestata)[58]. Il voto elettronico, inoltre, può evitare voti non validi e rendere più semplice, rapida e certa la procedura di calcolo dei voti[59].

Quanto, invece, ai pericoli sottesi alle procedure elettroniche di voto si deve distinguere a seconda che il voto elettronico avvenga in un seggio elettorale o in ambiente non presidiato[60]. In entrambi i casi, comunque, si pone la questione della sicurezza del sistema, volta a garantire la segretezza e a prevenire la manipolazione del voto[61], così come si fa questione dell'accessibilità del sistema, ossia dell'esistenza di una procedura comprensibile e agevole per l'elettore, nel rispetto del principio di equità ed uguaglianza[62].

Se poi si entra nel merito del voto elettronico espresso in ambiente non presidiato, è la garanzia della personalità e della libertà di voto che subisce un'ulteriore attenuazione[63].

In particolare, per ciò che attiene al profilo della *segretezza*[64], le procedure di voto elettronico, basate sulle nuove tecnologie, dovrebbero essere in grado di porre al riparo da eventuali tentativi di intrusione all'interno dei server, con la conseguente possibilità di associare il dato acquisito all'identità del soggetto che ha espresso il voto[65]. Si tratta di una problematica molto rilevante e che, però, sembra poter essere chiarita e definita soltanto attraverso un'attenta sperimentazione e messa a punto del meccanismo. In termini generali, tuttavia, se ci si attiene al dato tecnico, i sistemi di crittografia e la possibilità di replicazione dei dati sui vari registri distribuiti alla base della tecnologia *blockchain*, sembrano poter assicurare la segretezza del voto[66].

Per ciò che, invece, concerne la *personalità*, qualsiasi sistema di voto elettronico dovrà necessariamente garantire un'univoca identificazione dell'elettore, verificando che vi sia un'esatta corrispondenza tra chi esprime il voto mediante il dispositivo e l'effettivo titolare del diritto, in ciò ponendosi un concreto problema rispetto al parametro costituzionale. Si tratta, effettivamente, di uno snodo nel ragionamento attorno all'implementazione di modalità di voto non presidiato.

---

importanti requisiti di legittimità costituzionale che sconsigliano o impediscono l'adozione di alcune soluzioni, in quanto potenzialmente lesive dei principi costituzionali in materia".

[58] L. PRATCHETT, *Local e-democracy in Europe: Democratic x-ray as the basis for comparative analysis*, paper presented to the *International Conference on Direct Democracy in Latin America*, 2007.

[59] A. GRATTERI, *Finalità e problemi del voto elettronico*, in *Forum di Quaderni costituzionali*. Per una disamina di queste implicazioni legate alla digitalizzazione del diritto di voto sia consentito rinviare a M. LADU, *Contrastare l'astensionismo e favorire la partecipazione: il voto elettronico basato sulle tecnologie* Blockchain *e* Distributed Ledger, in *MediaLaws*, n. 1/2023.

[60] L. TRUCCO, *Il voto elettronico nella prospettiva italiana e comparata*, in *Diritto inform.*, n. 1/2011, 57; M. CUNIBERTI, *Tecnologie digitali e libertà politiche*, in *Diritto inform.*, n. 2/2015, 273 ss.

[61] Per un approfondimento sulle criticalità dal punto di vista della sicurezza del voto elettronico, cfr. G. GOMETZ, *Democrazia elettronica. Teoria e Tecniche*, ETS, Pisa, 2017, cap. 4.

[62] Per approfondimenti in merito, cfr. G. GOMETZ, *Democrazia elettronica. Teoria e tecniche*, Pisa, 2017, in particolare alle 153 ss.

[63] La dottrina si è espressa in termini di incompatibilità con la costituzione del voto elettronico non presidiato, con specifico riguardo alla violazione dei «canoni della libertà e della segretezza del voto», cfr. S. CATALANO, *Il voto elettronico*, in G. Ferri (a cura di), *Diritti costituzionale e nuove tecnologie*, cit., 361.

[64] E, nel caso di specie, riferita non tanto ai rapporti tra i privati quanto piuttosto rispetto alla possibilità che dall'esterno si riesca ad accedere ai dati acquisiti e, in modo diretto o indiretto, si riesca ad associare l'elettore alla scelta da esso compiuta.

[65] Si veda, tra gli altri, il recentissimo contributo di C. CHIARIELLO, *Voto elettronico e principio di segretezza tra regola ed eccezioni*, in questa *Rivista* 2023/I, 59 ss.

[66] Cfr. G. GOMETZ, M.T. FOLARIN, *Voto elettronico presidiato e blockchain*, in *Ragion Pratica*, n. 2/2018.

Non solo. Anche l'impiego di nuove tecnologie, come le *Distributed Ledgers Technologies*, che "architetturalmente" sembrano garantire una maggiore sicurezza ed integrità nelle procedure di voto, si è prestato ad una sorta di *blue-washing* democratico, essendo in realtà state sfruttate da poteri autocratici, come accaduto con la piattaforma *Active Citizen* implementata dal Comune di Mosca. Essa ha offerto ai moscoviti una mera illusione di *empowerment* democratico-partecipativo, essendosi poi rivelata una forma di controllo sulle scelte pubbliche[67].

Per chiudere sul punto, è senz'altro difficile individuare precauzioni che rendano il voto elettronico, espresso al di fuori di un seggio elettorale, conforme ai requisiti giuridico-costituzionali, volti ad assicurarne libertà, segretezza e personalità[68], salva la possibilità di "scendere" a scelte di compromesso per situazioni rispetto alle quali il voto già è ammesso a distanza (italiani all'estero o, nella forma del voto per corrispondenza, nella provincia autonoma di Bolzano) oppure per soggetti che sono lontani dal luogo di residenza o per soggetti fragili e vulnerabili che, in quanto tali, non potrebbero recarsi al seggio elettorale[69] .

3. *Strumenti tecnologici funzionali al voto referendario*

Dopo aver brevemente ricordato, nei paragrafi precedenti, i rischi che lo sviluppo delle *ICT* e delle loro pratiche evolutive possono comportare per il formarsi dell'opinione pubblica e per il diritto di voto (pratiche che, se si svolgono in modalità elettroniche, risultano rinvigorite dalla grande quantità di dati, dall'incremento della potenza di calcolo, dall'elaborazione di modelli algoritmici sempre più sofisticati nonché dal connubio con le scienze comportamentali), si passi ora ad alcune opportunità che lo sviluppo delle nuove tecnologie può comportare per l'istituto referendario.

Lungi dall'essere catturati dal cosiddetto "complesso di Borg"[70], e consapevoli del fatto che politiche pubbliche complesse molto spesso sono difficilmente riducibili ad una serie di "si" e "no", a meno che si voglia declinare verso una dimensione plebiscitaria della democrazia[71], l'intento, come detto in premessa, resta quello di mantenersi su di una linea di pragmatismo giuridico-costituzionale, per prendere in considerazione quanto i possibili impieghi delle *ICT* (e delle loro implicazioni, tra cui la *gamification*, come subito si vedrà nel successivo paragrafo)

---

[67] H. ESTECAHANDY, *The Democratic Illusion through the Technological Illusion: a Case Study of the Implementation of a Blockchain to Support an E-voting Platform in Moscow (Active Citizen)*, in *arXiv.org*, Cornell University, 10 gennaio 2023.

[68] Come evidenziato da V. DESANTIS, *Le nuove prospettive dell'internet voting tra avanzamento tecnologico e sostenibilità giuridica*, cit., 43: «per quanto sia necessario prendere atto che nessun sistema di voto tecnologico sia, in astratto, inattaccabile e che, almeno per il momento, è inverosimile che un sistema di voto elettronico possa replicare, più o meno nella stessa misura, le garanzie di segretezza che offre, fisicamente, la cabina elettorale, si può comunque essere più fiduciosi per il futuro perché, a differenza di quanto accadeva nel recente passato, si può, oggi, disporre di forme di voto elettronico non presidiate significativamente più sicure di quelle elaborate originariamente».

[69] Come ipotizzato da V. DESANTIS, *Le nuove prospettive dell'internet voting tra avanzamento tecnologico e sostenibilità giuridica*, cit., 62 ss.

[70] Per come originariamente introdotto da L.M. SACASAS, *Borg Complex: A primer*, 1° marzo 2013.

[71] M. PATRONO, *Democrazia rappresentativa e democrazia diretta nell'era digitale,* in G. Ferri (a cura di), *Diritti costituzionale e nuove tecnologie*, cit., 389. Analogamente, come sottolineato da J. BAYER, N. BITIUKOVA, P. BARD, J. SZAKACS, A. ALEMANNO, E. USZKIEWICZ, *Disinformation and Propaganda – Impact on the functioning of the rule of law in the EU and its Member States,* cit., 57 e 65, "As the complexity of public issues grows, decisions (like voting) are based more on emotions and social identity, as opposed to reasoned argumentation"; against this backdrop «Populism gives easy to understand but oversimplified and false answers to complex questions, and emotional politics builds on the worst characteristics of the people».

siano suscettibili sia di rispettare che di promuovere diritti e principi costituzionali in relazione alle pratiche referendarie[72].

Pertanto, l'approccio adottato sarà utile a far emergere punti di forza e criticità dell'utilizzo delle nuove tecnologie in un ambito delicato quale la consultazione referendaria.

3.1. *La* gamification

Il *design thinking* è un approccio che si inserisce, come una sub-sezione, nel più ampio fenomeno dello sviluppo delle tecnologie dell'informazione e della comunicazione (*ICT*, per l'appunto) e che con esse può modificare il rapporto e le "connessioni" tra cittadini e pubblici poteri[73].

Nello specifico, il *design-thinking* mira a promuovere una prospettiva centrata sulla persona, sia nelle modalità di identificazione dei singoli problemi sia nelle modalità volte ad affrontarli, al fine di raggiungere una soluzione il più possibile persona-centrica[74]. In questi termini, il *design-thinking* funge da supporto esterno a una prospettiva che è immanente al diritto, quella del rispetto e della promozione del principio personalista e, con esso, della dignità umana e della autodeterminazione.

Non è un caso che tale prospettiva stia guadagnando salienza anche con riguardo ai processi di partecipazione politica, al fine di contribuire a combattere astensionismo e disaffezione crescenti, motivando l'impegno dei cittadini attraverso strumenti più "attraenti" e "stimolanti", quali la *gamification.* Quest'ultima è parte dell'approccio di *desing-thinking* e si traduce – almeno nella sua accezione positiva, che qui si accoglie[75] – nell'idea «of using game design elements in non-game contexts to motivate and increase user activity and retention»[76]. In questo senso, dunque, la *gamification*, fa leva sull'attenzione e sull'interesse degli individui, sollecitandone la motivazione intrinseca ed estrinseca[77]. Nello specifico, «Gamification refers to designing systems, services and processes to provide positive, engaging experiences similar to the engaging experiences games provide, commonly with the aim of motivating beneficial behaviors»[78]. Tra le più note esperienze di gamificazione della democrazia digitale si possono citare Decide Madrid e vTaiwan, piattaforme create nel 2015, allo scopo di sfruttare «new gamified solutions to tackle issues in Taiwanese and Spanish democracy such as distrust, low motivation, and disengagement. The app interfaces, which incorporate game elements (e.g., avatars, rules of competition and visual aid effects), claim to excite and motivate citizens to

[72] About the possibility to deploy technological management tools in order to foster and enforce legal rules, see R. BROWNSWORD, *Law, Technology and Society – Re-imagining the Regulatory Environment,* Routledge, New York, 2019.

[73] G. SGUEO, *Games, Powers and Democracies,* Bocconi University Press, Milano, 2018, 17.

[74] A. LE GALL, *Legal Design beyond Design Thinking: processes and effects of the four spaces of design practices for legal field,* in R. Ducato, A. Strowel (a cura di), *Legal Design Perspectives – Theoretical and Practical Insights from the Field,* Ledizioni, 33.

[75] Vi è, infatti, chi intravede nella *gamification* un rischio, dovuto alla sottovalutazione, per l'appunto come fosse un gioco, delle frequenti occasioni di partecipazione che le modalità elettroniche di voto e di consultazione possono offrire. Si tratta, in sostanza, del rischio di una "banalizzazione" della democrazia (come denunciato, tra gli altri, da P. COSTANZO, *La democrazia digitale (precauzioni per l'uso),* cit., 84 ss.). Un approccio "positivo" al tema della *gamification*, viceversa, punta a metterne in luce la capacità attrattiva e di maggiore predisposizione del destinatario ad una riflessione seria rispetto a quel che viene proposto.

[76] S. DETERDING, D. DIXON, R. KHALED, L. NACKE, *From game design elements to gamefulness: defining gamification*, in *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, ACM Press, 2011, 9; B. BURKE, *Gamify: How Gamification Motivates People to Do Extraordinary Things*, Bibliomotion, 2014, 6.

[77] G. SGUEO, *Games, Powers and Democracies*, cit., 20.

[78] L. HASSAN, J. HAMARI, *Gameful civic engagement: A review of the literature on gamification of e-participation*, in *Government Information Quarterly*, n. 37/2020, 1.

vote and comment on digital issues (vTaiwan) or propose and vote on participatory budgeting proposals (Decide Madrid)»[79]. Ma anche in alcuni comuni e città della Germania, allo scopo di incrementare l'*engagement* dei cittadini, si è assistito ad una *gamification* della partecipazione. In particolare può essere rammentato il *participatory budget* della città di Potsdam, dove le tecnologie *Web2.0*, supportando la *gamification*, hanno consentito lo sviluppo di piattaforme che attraverso *game-like tools* hanno permesso agli elettori di selezionare progressivamente le proposte in competizione; oppure il caso della pianificazione infrastrutturale di Ludwigshafen dove un software con visualizzazioni, simulazioni e animazioni tridimensionali ha semplificato, reso chiare e quindi facilitato le scelte dei votanti[80].

Il *design* dell'intera procedura di voto referendario – dalle modalità di accesso alla piattaforma, alla progettazione dell'interfaccia, alle modalità di attivazione delle risposte al quesito – potrebbe contribuire notevolmente ad agevolare l'esercizio del diritto di voto[81].

In merito, l'analisi pubblicata dal *Servizio europeo di ricerca parlamentare* indica la *gamification* delle procedure democratiche come uno dei dieci temi sui quali investire[82]. In particolare, tale rapporto sottolinea che «public regulators are looking at how to harness the motivational potential of game design to counter disenchantment with politics, and foster civic engagement», ammettendo, tuttavia, che una simile prospettiva «presents EU legislators with legal and ethical concerns. Legal challenges will demand appropriate measures to protect citizens' privacy and guarantee inclusiveness. Ethically speaking, it could be argued that incentivising participation via game design might implicitly suggest that weaker or simpler forms of participation exist next to stronger more complex forms of civic engagement – thus acknowledging that game design nurtures a second-class civic spirit at best»[83].

In definitiva, la posta in gioco sembra risiedere, come osservato dal menzionato rapporto europeo, nel cogliere le opportunità che il *design-thinking* e la *gamification* mettono a disposizione, agevolate dagli sviluppi delle ICT, senza tuttavia scadere nella "banalizzazione" della democrazia.

In ogni caso, ciò che rileva sottolineare, a questo punto della ricerca, è la possibilità che alcune modalità di strutturazione delle nuove tecnologie possano assecondare obiettivi perseguiti da principi e diritti costituzionali: la valorizzazione della persona insita nel principio di autodeterminazione referendaria. A questo contribuisce, oltre la menzionata *gamification*, anche la tecnologia *blockchain*, grazie alla sua "architettura" decentralizzata, trasparente e resistente a manomissioni: ciò che sarà oggetto di attenzione nei due successivi paragrafi.

3.2. *La tecnologia* blockchain

Prima di entrare nello specifico dell'implementazione di una tecnologia *blockchain* per le procedure di voto elettronico nei referendum, si ritiene opportuno richiamare, seppur concisamente, le caratteristiche di fondo del sistema.

In sintesi, la *blockchain* è una *distributed ledger technology* composta da una "catena" di blocchi contenenti copie identiche di un registro[84]: «it is primarily a distributed decentralized

[79] Y.-S. TSENG, *Rethinking gamified democracy as frictional: a comparative examination of the Decide Madrid and vTaiwan platforms,* in *Social & Cultural Geography,* 2022, 3.

[80] K. MASSER, L. MORY, *Citizens' Participation and Gamification – Lessons Learnt from Previous and Recent Participation Boosts in Germany,* in *International Journal of Open Government*, 2017-01-05, 50 e 58-61.

[81] K. Masser, L. Mory (a cura di), *The Gamification of Citizens' Participation in Policymaking*, Springer, 2018, 19 ss.

[82] *European Parliamentary Research Service* (EPRS), PE 646.116 – Gennaio 2020,

[83] *European Parliamentary Research Service* (EPRS), PE 646.116, cit., pp- 10-11.

[84] K. WERBACH, *Trust, But Verify: Why the Blockchain Needs the Law*, in *BTLJ*, vol. 33, 2018, 493. «Everyone can maintain a copy of a dynamically-updated ledger, but all those copies remain the same, even without a central

database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Blockchain allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks. Each block is assigned a cryptographic hash (which may also be treated as a finger print of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domain»[85]. Nello specifico, «the truthfulness of the information encrypted in the blocks is certified by third parties without the need to involve any central authority. Plus, each transaction is public (namely every user can see what, when and how a transaction has occurred) but no one can see who has made the transaction»[86].

Riassumendo, le caratteristiche che qualificano la piattaforma *blockchain* sono: *(a)* la disintermediazione, che implica una struttura *peer-to-peer* in cui «no single party controls a blockchain, and blockchains do not rely on one centralized party for maintenance or operation»[87]; *(b)* la resilienza e la resistenza alle manomissioni, grazie ad algoritmi di *hashing* che impediscono la modifica formale o il *rollback* delle informazioni una volta memorizzate su una *blockchain*; *(c)* la trasparenza, poiché «a blockchain serves as an auditable trail of activity occurring on a peer-to-peer network»; *(d)* infine, tutti i dati memorizzati sono autenticati, non ripudiabili e pseudonimizzati grazie alla firma digitale e alla crittografia a chiave pubblica-privata[88].

Le potenzialità del sistema sono quindi multiple: «This technology was first developed to allow for the transaction of *value* over the internet without an intermediary to maintain user balances, but has subsequently become a way for users to reach collective decisions outside of the realm of traditional hierarchies and political institutions»[89].

Non è pertanto un caso che la *blockchain* sia oggetto di attenzione non solo nel settore privato, ma anche in quello pubblico[90]. A quest'ultimo proposito, in dottrina si è discusso della possibilità di sostituire funzioni statali con una *governance* implementata su una *blockchain*[91]: la sua architettura e le modalità di funzionamento risulterebbero, infatti, conformi ad alcuni principi amministrativi fondamentali quali la trasparenza, la decentralizzazione, l'efficienza,

---

administrator or master version… The software enabling this uses digital cryptography and game-theoretic incentives to make it difficult to cheat the system».

[85] K. M. KHAN, J. ARSHAD, M. M. KHAN, *Secure Digital Voting System based on Blockchain Technology*, in *Int. J. Electron. Gov. Res.*, vol. 14, 2018, 54.

[86] B. Cappiello, G. Carullo (a cura di), *Blockchain, Law and Governance*, cit.

[87] P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law – The Rule of Code*, Harvard University Press, Cambridge-London, 2018, 34.

[88] P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law – The Rule of Code*, cit., 37: «Because blockchains rely on public-private key encryption and digital signatures» nessuna transazione ivi registrata può essere smentita. Questo grazie alla «core feature of cryptographic blockchains… that of authenticating data inscribed inside them, be them transactions of blocks or, in more advanced scenarios, any other sort of metadata inscribed or linked into such transactions», cfr. D. ROIO, M. SACHY, S. LUCARELLI, F. BRIA, B. LIETAER, *D-Cent Project - Technical Design of Digital Social Currency*, Version n. 1/2015, 18.

[89] A. BERG, C. BERG, M. NOVAK, *Blockchains and Constitutional Catallaxy*, in *Constitutional Political Economy*, Vol. 31, No. 2/2020, 194.

[90] Come testimoniato dai due volumi: B. Cappiello, G. Carullo (a cura di), *Blockchain, Law and Governance*, Springer, 2021; O. Pollicino, G. De Gregorio (a cura di), *Blockchain and Public Law. Global Challenges in the Era of Decentralisation*, Edward Elgar Publishing, Northapton, 2021.

[91] D. CAGIGAS, J. CLIFTON, D. DIAZ-FUENTES, M. FERNÁNDEZ-GUTIÉRREZ, *Blockchain for Public Services: A Systematic Literature Review*, in *IEEE Xplore*, vol. 9, 2021, 13904 ss.; M. ATZORI, *Blockchain Technology and Decentralized Governance: is the State still necessary?* in *Journal of Governance and Regulation*, vol. 6, n. 1/2017, 45 ss.

l'autenticità, l'integrità e l'apertura agli scambi *peer-to-peer*[92]. In particolare, «as long as DLTs can guarantee data structure and security, they represent a promising opportunity for the management and assurance of transparency and efficiency in public sector transactions while maintaining information security. This is why Blockchain application in the public sector has received increasing attention from government, practitioners and consulting services. Another important feature is their temporary sealing capacity and the inalterability of the data they contain, as well as the reduced risk of unauthorized access and data manipulation - even by insiders who previously had access to documents and could potentially alter their contents»[93].

In merito all'impiego della *blockchain* nelle procedure di voto, esistono diverse "scuole di pensiero" [94]. La *Letter to Governors and Secretaries of State on the insecurity of online voting*, redatta dall'*American Association on the Advancement of Science* il 9 aprile 2020, ha denunciato l'insicurezza di qualsiasi votazione via web, anche laddove i risultati siano memorizzati su una piattaforma *blockchain*, in ragione della non verificabilità dei contenuti registrati[95]. Altri studiosi, all'opposto, hanno sottolineato l'utilità della *blockchain*, quale strumento volto ad evitare frodi nelle procedure elettorali[96].

Dal punto di vista teorico, le piattaforme *blockchain* si qualificano per alcuni requisiti strutturali che richiamano principi alla base di un sistema democratico, quali l'uguaglianza (rete *peer-to-peer*; trasparenza), l'autodeterminazione (non è un sistema gerarchico, non ha un'autorità centrale) e la certezza (essendo non reversibile, resistente alle manomissioni) [97]. Inoltre, con specifico riferimento alle procedure di voto, alcuni requisiti di un'applicazione *blockchain* ben si adattano alla sicurezza ed equità del voto in ragione della garanzia di integrità e di non modificabilità di quanto archiviato su una *blockchain*, l'assenza di un *single point of failure* e di un *single point of control*, quindi la trasparenza legata alla architettura *peer-to-peer*[98]. Infatti, l'esistenza di registri leggibili in modo identico da tutti i partecipanti e la possibilità di "rimpiazzare" il rapporto fiduciario cittadini-istituzioni con la fiducia negli algoritmi matematici, supportano l'affidabilità della procedura e valorizzano la partecipazione dei singoli utenti[99].

Per quanto attiene alle finalità perseguite dal presente scritto, le menzionate caratteristiche "architetturali" di una *blockchain* ben si attagliano ai presupposti dell'autodeterminazione, in termini di decentralizzazione, trasparenza, non manomissione: «a blockchain can be regarded as a shared repository of information – an open, low-cost, resilient and secure storage system that nobody owns but many people maintain. Because blockchain helps people to reach consensus they may help solve some of the issues traditionally associated with common-pool resources. By recording every interaction on a public blockchain and encoding rules linking the

---

[92] M. SWAN, *Blockchain. Blueprint For a New Economy*, O'Reilly, Sebastopol, 2015.

[93] F.L. BENÍTEZ-MARTÍNEZ, M. VISITACIÓN HURTADO-TORRES, E. ROMERO-FRÍAS, *A neural blockchain for a tokenizable e-Participation model*, in *Neurocomputing*, Volume 423, 29 January 2021, 703-712

[94] Non vanno scordati i rischi costituzionali insiti nel «technological libertarianism», cfr. O. Pollicino, G. De Gregorio (a cura di), *Blockchain and Public Law. Global Challenges in the Era of Decentralisation*, cit., 3

[95] V. al sito dell'American Association for the Advancement of Science.

[96] G. GOMETZ, *Democrazia elettronica. Teoria e Tecniche*, Edizioni ETS, Pisa, 2017, 192.

[97] La dottrina «explores whether blockchain-based voting can secure foundational constitutional values and realise democratic ideals, while minimising risks in electoral and political processes»: D. JOHNSON, *Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values?* in *European Journal of Risk Regulation*, vol. 10, n. 2/2019, 331.

[98] Come sottolineato da G. GOMETZ, M.T. FOLARIN, *Voto elettronico presidiato e blockchain*, in *Ragion Pratica*, n. 2/2018, 326, non è possibile adottare un sistema blockchain che renda verificabile da parte del votante il proprio voto (da quando viene espresso a quando entra nella computazione degli esiti), pena la violazione del principio costituzionale di segretezza del voto.

[99] Ed è qui fondamentale richiamare il tema della fiducia che, complessivamente, deve essere sempre presente ove, per la vita delle istituzioni democratiche, siano in gioco dei principi fondamentali, quali l'espressione libera della propria scelta attraverso le procedure di voto.

interactions blockchain can help commons-based communities govern themseleves through decentralized incentive systems»[100].

Inoltre, sono da tempo in atto studi e ricerche volti a elaborare una *blockchain* che assicuri prestazioni più elevate e che si riveli maggiormente adatta agli scopi pubblici. In merito, è stato proposto un sistema di partecipazione "tokenizzabile" che utilizza strumenti di voto elettronico basati su una rete neuronale *blockchain* guidata dall'uso di *smart contracts*, in sostituzione del tradizionale sistema di produzione di blocchi e la conseguente necessità di "minatori" in grado di risolvere la *proof of work*[101]. L'obiettivo del progetto è duplice: non solo l'implementazione di una piattaforma *blockchain* per rendere affidabile la procedura di voto, ma anche la promozione della partecipazione (*engagement*) attraverso la consegna di un *token* (a tutti i cittadini che partecipano al voto) che dà titolo ad alcuni vantaggi nell'utilizzo dei servizi pubblici[102]. Il *trend* degli studi in corso sembra, quindi, andare verso una combinazione tra sistemi *blockchain*, applicazioni *smart contracts*[103] e crittografia a chiave privata-pubblica[104].

Alcuni Paesi (come Estonia, Svezia, Australia, Regno Unito) hanno sperimentato soluzioni DLTs per l'*e-government* e la partecipazione elettronica[105].

In particolare, nell'Unione Europea, come evidenziato dall'*European Union Blockchain Observatory and Forum* nel suo Rapporto (2022)[106]: «Romania is the first EU country to use a voting reporting tool that is based on Blockchain technology for national elections. The national parliamentary elections, held on December 6, 2020, used Blockchain technology to guarantee the integrity of the electoral process and strengthen its transparency»[107]. Al di fuori dell'UE, va

---

[100] P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law – The Rule of Code* cit., 42.

[101] F.L. BENÍTEZ-MARTÍNEZ, M. VISITACIÓN HURTADO-TORRES, E. ROMERO-FRÍAS, *A neural blockchain for a tokenizable e-Participation model*, cit., 2.

[102] F.L. BENÍTEZ-MARTÍNEZ, M. VISITACIÓN HURTADO-TORRES, E. ROMERO-FRÍAS, *A neural blockchain for a tokenizable e-Participation model*, cit., 4: «Our model… is based on a public G-Cloud system that allows a blockchain platform to be integrated as a service (BaaS). This guarantees the functional requirement of scalability necessary in any governmental and/or territorial environment. In our system, the voter would access the platform through a permissioned dApp that would connect with the interface and the voter database to proceed with the recognition and identification of a specific person in the process. Then, the System Administrator would activate the Smart Contract at the front end that would allow the citizen to participate in the process opened by the agency to register their participation and their vote. In the validation node, data encryption is performed with a one-way SHA-256 hash function so that the result of voting cannot be reversed. Once the vote is encrypted, the block will be added to the blockchain within the BaaS architecture used and, in turn, the block generates the ''token" (through a transaction generated by a smart contract… which will grant the voter a series of advantages and/or rights of use in the city)».

[103] *Smart contracts* sono applicazioni *blockchain* attraverso cui le «parties can enter into a binding commercial relationship, either entirely or partially memorialized using code, and use software to manage contractual performance… To execute a smart contract, parties must first negotiate the terms of their agreement… Once agreed upon, parties memorialize all or part of their understanding in smart contract code, which is triggered by digitally signed blockchain-based transactions… Because no single party controls a blockchain, there may not be a way to halt the execution of a smart contract after it has been triggered by the relevant parties»: P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law – The Rule of Code* cit., 74-75.

[104] J. H. HSIAO, R. TSO, C.M. CHEN, M. E. WU, *Decentralized E-Voting Systems Based on the Blockchain Technology*, in J. J. Park et al. (a cura di), *Advances in Computer Science and Ubiquitous Computing*, Springer, Singapore, 2018, 305: «The anonymities of voters, the security of ballot transmission and the verifiability of votes during the billing phase are the most fundamental requirements for voting. The anonymity and security can be achieved by the secret sharing scheme with Paillier's public-key cryptosystem while the verifiability of votes can be realized by taking advantage of the transparency and non-repudiation of blockchain. Voters can calculate the ballots and verify the election results on their own without a trusted third party».

[105] F.L. BENÍTEZ-MARTÍNEZ, M. VISITACIÓN HURTADO-TORRES, E. ROMERO-FRÍAS, *A neural blockchain for a tokenizable e-Participation model*, cit., 2.

[106] V. il report *EU Blockchain Ecosystem Developments*.elaborato dall'*European Union Blockchain Observatory & Forum.*

[107] *Ibid*., 162.

ricordato il caso svizzero (più precisamente la sperimentazione attuata dalla città di Zugo)[108], così come il sistema *blockchain* Agora utilizzato dal governo nazionale in Sierra Leone nel 2018[109].

In definitiva, se la tecnologia *blockchain* sembra conforme ad alcuni requisiti costituzionali essenziali del diritto di voto, rimane tuttavia la difficoltà, comune a tutti i casi di voto espresso lontano dal seggio elettorale, di garantire la libertà e la personalità del voto. In proposito, la dottrina ha avanzato la soluzione dell'*early voting*[110].

3.3. *Segue: sicurezza e affidabilità per le procedure referendarie*

Va anzitutto ricordato che l'affidamento alla *blockchain* per il voto referendario non intende supportare la teoria della sostituzione delle funzioni statali da parte di una società civile auto-organizzata attraverso una propria *governance* su piattaforma *blockchain*[111]. Lungi dall'abbracciare una «blockchain utopias… guilty of technological essentialism by drawing determinist conclusion from an underlying architectural design and by failing to allow for the functional and technological latencies within that design»[112], l'approccio seguito mira piuttosto a collocarsi sul percorso del già richiamato pragmatismo giuridico-costituzionale.

Un sistema *blockchain* deve, anzitutto, rispettare la legge[113] e deve farlo in un duplice senso. Non solo deve rispettare l'ordinamento giuridico esistente, ma, in ragione dei distinti usi per i quali può essere implementato, il sistema *blockchain* deve presupporre una collaborazione tra gli esperti del sistema stesso e le pubbliche autorità. In questo senso, l'architettura *blockchain* va configurata e utilizzata in funzione di obiettivi di derivazione costituzionale.

Da un lato, le caratteristiche di sicurezza e resistenza alle manomissioni proprie di tale piattaforma (v., *supra*, § 3.2), si prestano ad assicurare i requisiti di certezza giuridica (quindi integrità dei voti espressi). Dall'altro, i passaggi attraverso cui si articola la raccolta delle sottoscrizioni (o, più in generale, gli adempimenti formali richiesti per dare avvio al procedimento), il controllo di legittimità, nonché quello di ammissibilità del quesito referendario, così come il voto degli elettori, potrebbero essere resi ulteriormente affidabili e certi laddove andassero ad integrare i "blocchi" della catena, posti sotto la supervisione di differenti "nodi" costituiti da pubbliche autorità.

Potrebbero, quindi, essere caricate e codificate nella *blockchain* le fasi dell'intera procedura referendaria[114], che così verrebbero a beneficiare dei requisiti di trasparenza, sicurezza e affidabilità, che, come anzidetto, sono propri di tale tecnologia (v., *supra*, § 3.2).

---

[108] *Ibid.* 189-190, «Following a successful pilot, the city [of Zug] launched its blockchain-powered digital identity programme in November of 2017. In early summer 2018, the Ethereum-based "Zug ID" was successfully used for a non-binding referendum».

[109] T.P.J. BURGEMEESTER, *A Case for Blockchain-Based Voting Applications to Reinforce Public Trust in Elections*, in *Amsterdam Law Forum*, vol. 14, n. 2/2022, 76-81.

[110] E. CATERINA, M. GIANNELLI, *Il voto ai tempi del Blockchain: per una rinnovata valutazione costituzionale del voto elettronico*, in *Rivista AIC*, n. 4/2021, 14; R.M. ALVAREZ, T.E. HALL, A.H. TRECHSEL, *Internet Voting in Comparative Perspective: The Case of Estonia*, in *Political Science & Politics*, vol. 42, n. 3/2009, 497.

[111] M. ATZORI, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, cit., 51.

[112] U. KOHL, *Blockchain utopia and its governance shortfalls*, in O. Pollicino, G. De Gregorio (a cura di), *Blockchain and Public Law. Global Challenges in the Era of Decentralisation*, cit., 14.

[113] K. WERBACH, *Trust, But Verify: Why the Blockchain Needs the Law*, cit.

[114] M. ATZORI, *Blockchain technology and decentralised governance: is the State still necessary?* in *Journal of governance and regulation*, Vol. 6, No. 1/2017, 45. In relazione al voto elettronico in generale, V. DESANTIS, *Le nuove prospettive dell'internet voting tra avanzamento tecnologico e sostenibilità giuridica*, cit., 45, osserva che il sistema «deve presupporre l'intero affidamento dei servizi di raccolta ed elaborazione dei dati della votazione al gestore pubblico, in modo che l'intera sequenza elettorale non sia attratta o intercettata da altri e confliggenti interessi».

Sulla scorta di tale premessa e tenendo conto delle diverse "architetture" di *blockchain* possibili (centralizzata, privata e autorizzata; decentralizzata, federata e autorizzata; o distribuita, pubblica e *permissionless*)[115], la scelta dovrebbe ricadere su una *blockchain* autorizzata, nella quale le pubbliche autorità agiscono come nodi che validano le procedure, al fine di garantire adeguati livelli di controllo e coordinamento, con vantaggi rispetto alle problematiche sottese, da un lato, a registri completamente distribuiti e, dall'altro lato, ai database tradizionali, completamente centralizzati[116].

In sintesi, la scelta "tecnica" che combina diverse caratteristiche strutturali dei sistemi *blockchain*, che sembrerebbe meglio rispondente alle "esigenze costituzionali" sottese al referendum potrebbe cadere su una *blockchain* decentralizzata, federata e autorizzata: un consorzio tra diversi poteri pubblici – che svolgano compiti distinti nell'ambito della procedura referendaria – realizzerebbe l'"entità federata"; l'acceso degli elettori avverrebbe in conseguenza di autenticazione[117]; i "blocchi" della catena renderebbero un'evidenza decentralizzata di tutto quanto ivi registrato. Questa soluzione integrerebbe, quindi, un giusto equilibrio tra l'interesse delle autorità pubbliche a supervisionare il sistema e l'interesse dei cittadini a mantenere un controllo decentralizzato sui registri[118], così ponendosi in linea con gli obiettivi di autodeterminazione collettiva, sicurezza del voto e affidabilità del sistema.

Si condivide, di fatto, l'affermazione secondo la quale «fair and trustworthy voting procedures are a prerequisite of sustainable democracy. Therefore, one could explore the possibility of using distributed ledger technology, such as blockchain, in order to contribute to the efficiency and reliability of voting procedures and their monitoring»[119], tenuto peraltro conto che nessuna procedura di voto è immune da *points of failure*[120].

La *blockchain*, già sperimentata per la registrazione e il conteggio dei voti, potrebbe essere implementata anche per l'espressione del voto, a condizione che sia garantita la segretezza e la personalità del medesimo, il che, fisiologicamente, va di pari passo con l'esistenza di un luogo presidiato per l'esercizio dello stesso.

Si tratta di raggiungere un equilibrio, attraverso la strutturazione di accorgimenti tecnici che "qualificano" ulteriormente il diritto di voto in termini di sicurezza e affidabilità. Ciò che

---

[115] U. KOHL, *Blockchain utopia and its governance shortfalls,* cit., 22 e 33, sottolinea la flessibilità di una piattaforma basata su una tecnologia che può assecondare differenti configurazioni (da centralizzate a distribuite).

[116] M. ATZORI, *Blockchain technology and decentralised governance: is the State still necessary?* cit., 52.

[117] I sistemi attuali di identificazione (Spid e CIE), abilitati dal CAD (Capo V, Sezione III) e specificati dalle linee guida Agid, rispondono ad elevati livelli quanto ad autenticità e sicurezza, secondo il disposto del Regolamento UE 910/2014 (art. 8, c. 2, lett. *c*).

[118] Come sottolineato da V. DESANTIS, *Le nuove prospettive dell'internet voting tra avanzamento tecnologico e sostenibilità giuridica*, cit., 46, a garanzia della segretezza del voto, le fasi della identificazione e della raccolta e conteggio dei voti dovrebbe essere chiuso in compartimenti non comunicanti, per evitare la riconducibilità del voto espresso a chi si è autenticato sulla piattaforma: «una volta che il voto sia stato raccolto dal sistema (si tratterebbe, com'è intuibile, di rafforzare, anche in questo caso, la segretezza del voto), è necessario spezzarne la riconducibilità al suo autore, restando disponibile all'amministrazione solo il dato che attesti l'avvenuta partecipazione dell'elettore alla consultazione elettorale e non anche *in che modo* il singolo elettore abbia votato. Un risultato di questo genere potrebbe essere raggiunto istituendo un sistema di raccolta dei voti articolato su due sequenze: la prima che autorizza al voto, verificando la titolarità del diritto in base ai sistemi di riconoscimento delle identità digitali; la seconda che provvede al conteggio delle espressioni di voto, senza disporre di dati sulla provenienza delle stesse».

[119] J. GOOSSENS, *Blockchain and democracy: Challenges and opportunities of blockchain and smart contract for democracy in the distributed, algorithmic state,* in O. Pollicino, G. De Gregorio (a cura di), *Blockchain and Public Law. Global Challenges in the Era of Decentralisation,* cit., 85.

[120] Si pensi, solo a titolo di esempio, a tutte le problematiche connesse ai cosiddetti brogli, i quali si sono pur sempre verificati nella storia e che danno atto di una certa fallacia del sistema elettorale. Naturalmente, ciò che rileva, è che il sistema sia complessivamente affidabile e rilasci un risultato che è ritenuto accettabile anche al netto di eventuali "falle".

parrebbe poter essere realizzato con l'adozione di un sistema *blockchain* con le caratteristiche sopra menzionate (decentralizzata, federate, autorizzata).

In definitiva: «The major challenge for global civil society will soon be to explore new political and social dimensions, with the aim of integrating the applications of disruptive technologies such as the blockchain with citizens' rights, equality, social cohesion, inclusiveness, and protection of public sector. Such integration is vital and cannot be left to the (anti-) political engineering of IT experts, financial investors, and code developers: it requires indeed a mature and interdisciplinary effort by all the fields of human knowledge, with particular regard to political theory, humanities and social sciences, to best assess risks, benefits and outcomes of the new technologies»[121]. In questo dialogo, quindi, i poteri pubblici sono chiamati ad interpretare la loro parte nella sperimentazione di tali nuove tecnologie[122].

4. *Strumenti normativi funzionali al voto referendario*

Luciano Floridi già da tempo parla di un'etica adatta all'"ambientalismo digitale" in cui l'*inforg* sviluppa le sue relazioni[123]. Ciò significa riconoscere che la trasformazione digitale è un processo irreversibile e che – come tale – richiede un approccio adeguato. A tale stregua, il giurista, chiamato a sottoporre a verifica i "parametri giuridici" con i quali abitualmente opera per verificarne l'adeguatezza alle nuove evoluzioni tecnologiche, è altresì chiamato a prendere in considerazione lo "stato dell'arte" raggiungo in altre discipline che gli consentano di acquisire migliore contezza di problematiche tanto complesse quali quelle sottese ai processi di digitalizzazione (di cui si è detto: v., *supra*, §§ 2 e 3). Non per "piegare" la tecnica al diritto, o viceversa[124], quanto piuttosto per andare alla ricerca di una "mutua alleanza", in grado di sollecitare nuove dinamiche che, attraverso il combinato disposto di accorgimenti giuridici (come si vedrà nel presente capitolo) e tecnologici (come si è visto, invece, in precedenza: v., *supra*, § 3), portano all'implementazione di "qualificativi" ulteriori per principi e diritti già esistenti (trasparenza, equità, sicurezza, affidabilità).

Nello specifico, alla comune *ratio* sottesa a tali strumenti tecnologici, volta a porre la persona al centro (*design thinking, gamification)* e potenziarne le possibilità di "autodeterminazione" decentralizzata in ambiente sicuro (*blockchain),* fa da *pendant* analoga *ratio* sottesa ad una serie di iniziative normative europee (si veda il paragrafo successivo), volte a rafforzare – attraverso requisiti di trasparenza – la consapevolezza individuale nella sfera digitale. Entrambe queste *ratio* (come già posto in evidenza: v., *supra*, § 1) condividono, a loro turno, quella propria dell'istituto referendario che, non a caso, si traduce nella possibilità dell'individuo di autodeterminarsi sul piano collettivo.

---

[121] M. ATZORI, *Blockchain technology and decentralised governance: is the State still necessary?* cit., 59.

[122] Nel corso della XVIII legislatura, è stato previsto, nella legge di bilancio 2020, un fondo per la sperimentazione del voto elettronico con riferimento alle elezioni europee, nazionali e per i referendum. La sperimentazione, in particolare, dovrebbe coinvolgere gli italiani residenti all'estero e gli elettori che temporaneamente si trovano fuori dal comune di residenza per motivi di lavoro, di studio o per ragioni medico-sanitarie. Con il decreto-legge 31 maggio 2021, n. 77 (poi convertito, con modificazioni, nella legge 29 luglio 2021, n. 108) la sperimentazione è stata estesa alle elezioni amministrative e regionali, in programma prima per il 2022 e poi, a seguito di rinvio, per il 2023, con integrazione ulteriore del fondo. Con apposito decreto ministeriale del 9 luglio 2021, successivamente integrato da un ulteriore decreto del 21 ottobre 2021, sono state adottate le Linee guida per la sperimentazione di modalità di espressione del voto in via digitale, come previsto dal provvedimento di istituzione del fondo.

[123] L. FLORIDI, *La quarta rivoluzione – Come l'infosfera sta trasformando il mondo,* Milano, 2021, 251 ss.

[124] N. IRTI, *Il diritto nell'età della tecnica,* Editoriale Scientifica, Napoli, 2007, 11 ss.

Da questa "triplice alleanza" tra componente tecnologica, normativa e istituto referendario, scaturisce non solo il rispetto, ma anche la promozione dell'autodeterminazione collettiva e con essa del principio personalista e democratico[125].

4.1. *Trasparenza, equità*

Dopo aver affrontato "l'ingrediente tecnologico" (v., *supra*, § 3) della menzionata alleanza tra diritto e tecnologia, funzionale all'istituto referendario, si passi ora "all'ingrediente normativo", rispetto al quale vengono in questione anzitutto una serie di iniziative dell'Unione Europea.

Prima di entrare nel merito, giova ricordare che la dottrina ha qualificato le piattaforme online «come formazioni sociali in cui la personalità di ciascuno viene catturata da meccanismi occulti di manipolazione delle scelte individuali, con la conseguente messa a repentaglio di diritti inviolabili, a partire dalla libertà di pensiero»[126].

Se nell'ordinamento interno regna una sorta di anomia quanto alla pubblicità politica ed elettorale su piattaforme digitali[127], l'UE si è attivata per regolamentare le nuove tecnologie e il loro impatto sull'opinione pubblica, anche in ambito politico. In merito, si richiamano non solo il Regolamento UE 679/2016 (GDPR) che tratta la profilazione e il processo decisionale automatizzato (articolo 22), ma anche il Regolamento UE 2065/2022 (DSA), nonché la proposta di regolamento sull'intelligenza artificiale (AIA) [128] e la proposta di regolamento sulla pubblicità politica[129].

Si tratta di iniziative che sono accomunate da un analogo *fil rouge*: la costruzione di una sorta di "partnership di impegno" tra autorità pubbliche, fornitori di servizi Internet, piattaforme, motori di ricerca e imprese in generale, al fine di migliorare la consapevolezza digitale della società civile e proteggerne l'autodeterminazione[130].

L'AIA, in particolare, vieta le pratiche di intelligenza artificiale «che utilizza[no] tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento», o «che sfrutta[no] le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcer[n]e materialmente il comportamento»[131]. La proposta disciplina altresì i sistemi di intelligenza ad alto rischio (che,

[125] Nei termini in cui sono considerati intimamente connessi da L. FERRAJOLI, *La costruzione della democrazia – Teoria del garantismo costituzionale*, cit.

[126] C. PINELLI, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, cit., 197.

[127] In merito alla distinzione tra comunicazione politica ed elettorale, alla normazione nazionale per la comunicazione elettorale sui mass-media tradizionali ed alla sua inadeguatezza per le peculiarità che contraddistinguono i social media nonché al prevalere, in tale ambito, di forme di autoregolamentazione, cfr. E. CATERINA, *La comunicazione elettorale sui* social media *tra autoregolazione e profili di diritto costituzionale*, in *Osservatorio sulle fonti*, n. 3/2021, 1393 ss.

[128] COM(2021) 206 final.

[129] COM(2021) 731 final.

[130] In linea con la richiesta avanzata anche in dottrina, C. PINELLI, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, cit., 197: «Ecco perché non potremo accontentarci di ricette idonee a individuarne i responsabili, entro limiti alla libertà di espressione compatibili coi princìpi delle democrazie liberali. Dovremo pure ricercare come favorire la consapevolezza collettiva dei rischi di quei circuiti comunicativi, e come stimolare virtù trasformative volte alla formazione di circuiti alternativi, e meno costrittivi per le libertà individuali».

[131] Art. 5, c. 1, sub a), b). Tuttavia, come osserva R. J. NEUWIRTH, *The EU Artificial Intelligence Act – Regulating Subliminal AI Systems*, Routledge, London-NewYork, 2023, 15, l'AIA non specifica il significato delle "tecniche subliminali". Allo scopo si deve risalire ai lavori preparatori, nello specifico lo *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe: Final Report*, Luxembourg, 2021, 31, della Commissione Europea, da cui risulta «AI can be used to exert a significant impact on human

tra l'altro, potrebbero produrre un impatto negativo sui diritti fondamentali), statuendo che gli utenti debbano essere adeguatamente informati sulle caratteristiche, capacità e i limiti delle prestazioni del sistema di IA ad alto rischio[132]. Inoltre, *(a)* per quanto riguarda i sistemi di IA destinati a interagire con le persone fisiche, è disposto che essi debbano essere progettati e sviluppati in modo che quest'ultime siano rese edotte del fatto che stanno per interagire con un sistema artificiale; *(b)* per sistemi di IA di riconoscimento delle emozioni o di categorizzazione biometrica, le persone fisiche che vi sono esposte devono essere informate del funzionamento del sistema; *(c)* gli utenti di un sistema di IA che genera o manipola immagini, audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona (*deep fake*), devono essere informati del fatto che il contenuto è stato generato o manipolato artificialmente[133].

Il DSA[134], da parte sua, prevede garanzie di trasparenza per i sistemi di moderazione dei contenuti adottati dai fornitori di servizi (comprese le piattaforme online), in particolare quando la moderazione è eseguita da algoritmi automatizzati[135]. Alle piattaforme online è, inoltre, fatto divieto di progettare, organizzare o gestire le loro interfacce in modo da ingannare o manipolare i destinatari del loro servizio o in modo da falsare o compromettere la loro capacità di prendere decisioni libere e informate[136]. Inoltre, tutte quelle piattaforme online che mostrano pubblicità sulle loro interfacce devono provvedere affinché, per ogni singola pubblicità presentata a ogni singolo destinatario, l'utente sia in grado di identificare in modo chiaro, conciso, inequivocabile e in tempo reale che il messaggio è una pubblicità, la persona fisica o giuridica per conto della quale la pubblicità è presentata e che paga l'avviso pubblicitario, nonché informazioni significative, direttamente e facilmente accessibili dalla pubblicità, sui principali parametri utilizzati per determinare il destinatario a cui la pubblicità è presentata e, se del caso, come modificare quest'ultimi[137]. Analogamente è richiesto per i sistemi di raccomandazione[138]; mentre adempimenti supplementari in termini di trasparenza sono imposti alle piattaforme online di grandi dimensioni o ai motori di ricerca di grandi dimensioni, a causa dei rischi sistemici derivanti dalla progettazione o dal funzionamento del loro servizio, compresi i sistemi algoritmici, o dall'uso che viene fatto dei loro servizi[139]. A quest'ultimo proposito (piattaforme online o motori di ricerca molto grandi), tra le misure di mitigazione previste per ridurre i rischi

agency, including triggering cognitive manipulation through 'dark patterns'and interaction with sub-conscious processes».

[132] Art. 13.

[133] Art. 52, cc. 1-3.

[134] Artt. 15-16-17-18.

[135] Sull'inserimento di questa proposta nel solco del "Piano d'azione per la democrazia europea" - COM(2020) 790 final, nonché come *lex generalis* rispetto a quella *specialis* relativa alla proposta di regolamento europeo sulla pubblicità politica, cfr. E. LONGO, *Rivoluzione digitale e sviluppi della partecipazione democratica nell'Unione europea*, in *Osservatorio sulle fonti*, cit., 1326.

[136] Art. 25.

[137] Art. 26.

[138] L'art. 27, c. 1, dispone che i «fornitori di piattaforme online che si avvalgono di sistemi di raccomandazione specificano nelle loro condizioni generali, in un linguaggio chiaro e intellegibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché qualunque opzione a disposizione dei destinatari del servizio che consente loro di modificare o influenzare tali parametri principali».

[139] Tra i rischi sistemici, vanno inclusi (Art. 34, c. 1, sub b) «eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'articolo 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al rispetto dei diritti del minore sancito nell'articolo 24 della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta»; così come (Art. 34, c. 1, sub c) «eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica».

per i diritti fondamentali, si fa esplicito riferimento all' «adozione di misure di sensibilizzazione e l'adattamento della loro interfaccia online al fine di dare ai destinatari del servizio maggiori informazioni» nonché «il ricorso a un contrassegno ben visibile per fare in modo che un elemento di un'informazione, sia esso un'immagine, un contenuto audio o video, generati o manipolati, che assomigli notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che a una persona appaia falsamente autentico o veritiero, sia distinguibile quando è presentato sulle loro interfacce online»[140].

Alle disposizioni del DSA e dell'AIA, si aggiunge la proposta di regolamento sulla pubblicità politica[141]. Essa si rivolge a tutti i fornitori di servizi di pubblicità politica (non solo alle piattaforme online) al fine di rendere più trasparente il loro operato, sensibilizzando i destinatari e imponendo la *disclosure* di ulteriori informazioni (rispetto a quanto richiesto dal DSA: principalmente in merito allo *sponsor* che si cela dietro le pubblicità e agli obiettivi politici perseguiti)[142]. La proposta entra inoltre nel merito delle tecniche di *targeting* e amplificazione impiegate nella pubblicazione, diffusione o promozione di pubblicità politica che comportano il trattamento di dati personali rivolgendosi ad ogni titolare del trattamento, anche coloro che non sono fornitori di servizi di pubblicità politica. Vieta, quindi, le tecniche (*targeting* e amplificazione) che coinvolgono categorie particolari di dati, ai sensi dell'articolo 9 del GDPR, salvo il caso del previo consenso esplicito dell'interessato o del caso *sub* art. 9, par. 2, lett. d), GDPR. In ogni caso, i titolari del trattamento sono tenuti a trasmettere «contestualmente al messaggio di pubblicità politica, informazioni supplementari per permettere all'interessato di comprendere la logica utilizzata e i principali parametri della tecnica applicata» [143].

L'intento sotteso a tali normative è evidente: in conformità con l'approccio basato sul rischio, che dal GDPR ha accompagnato l'UE lungo il processo di trasformazione digitale[144], la protezione dei cittadini si concentra principalmente sugli "attributi" della trasparenza ed equità, nonché sui diritti procedurali che li supportano[145], al fine di rendere gli individui maggiormente consapevoli e responsabili nell'autodeterminarsi. Allo scopo, a sorvegliare che i "signori" del digitale[146] operino conformemente a quanto normativamente richiesto in termini di trasparenza ed equità, è prevista una *governance* composta da autorità di vigilanza nazionali ed europee, nonché dal loro *network* (per affrontare problematiche di natura essenzialmente transfrontaliera). L'ambito territoriale di applicazione di tali previsioni, vista la natura strutturalmente transfrontaliera del digitale, si estende oltre il caso dei soggetti destinatari stabiliti all'interno dell'UE per raggiungere quello dell'attività rivolta a persone che si trovano nell'UE, indipendentemente dal luogo in cui ha sede lo stabilimento del fornitore o del prestatore di servizi.

---

[140] Art. 35, c. 1, i), k).

[141] COM(2021) 731 final.

[142] Come recita il considerando n. 4 della proposta, «Transparency of political advertising contributes to enabling voters to better understand when they are being presented with a political advertisement on whose behalf that advertisement is being made, and how they are being targeted by an advertising service provider, so that voters are better placed to make informed choices».

[143] Cfr. il considerando n. 53 e l'art. 12, c. 3.

[144] L. CALIFANO, *Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali,* in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona – Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679,* Napoli, 2017, 34 ss.

[145] Sui diritti procedurali del *digital constitutionalism*, cfr. O. POLLICINO, *L'impatto dell'IA sul diritto e sui diritti*, in *BioLaw Journal*, No. 1/2020, 492.

[146] Per mutuare le parole di L. AMMANNATI, *I 'signori' nell'era dell'algoritmo,* in *Diritto Pubblico*, 2, 2021, 381 ss.

In definitiva, l'approccio dell'UE nei confronti del potenziale impatto del fenomeno della digitalizzazione (con suoi progressi, fatti di strumenti di IA per la profilazione e il *targeting*, che contribuiscono a potenziare le evidenze degli studi delle scienze comportamentali) opera seguendo un "rischio calcolato". Da un lato, infatti, l'UE evita di soffocare il progresso tecnologico, motivo per cui i divieti contenuti nel DSA e nelle proposte sull'IA e sulla pubblicità politica sono limitati a casi estremi, che colpiscono il cuore del principio personalista, quindi della dignità umana e dell'identità personale, attraverso tecniche di manipolazione delle persone senza che queste ne siano consapevoli[147]. D'altra parte, i rischi per la democrazia di cui tali atti si dichiarano consapevoli (definiti "rischi sistemici" dal DSA e dalla proposta sulla pubblicità politica, o "alti rischi" dall'AIA), sono "messi in conto": allo scopo è creato un "armamentario" per strutturare ed affinare la *awareness* degli individui ai quali è chiesto di sviluppare una propria *due diligence* in vista dell'autodeterminazione, nei vari campi della vita (da quello economico-sociale a quello politico-democratico). In questo modo, vengono "attrezzati" più che con nuovi diritti, principalmente con "nuovi attributi" (trasparenza, equità) per diritti e principi esistenti.

5. *Tra diritto e tecnologia: un voto referendario consapevole e sicuro?*

Gli obiettivi perseguiti dalla ricerca sono plurimi e intrecciati. *In primis*, l'inquadramento delle questioni giuridiche tradizionali (come la democrazia diretta, con specifico riguardo al referendum) all'interno del più ampio panorama della trasformazione digitale, sottolineandone rischi e opportunità (v., *supra*, §§ 2 e 3). Secondariamente, la presupposta apertura interdisciplinare, in quanto la "ricognizione" dei rischi e delle potenzialità dell'ambiente digitale da parte del giurista presuppone la presa d'atto di evidenze rese da altre scienze (in particolare quelle informatiche e comportamentali: v., *supra*, §§ 2 e 3). Infine, l'emersione di una metodologia giuridico-costituzionale che – cercando di orientarsi tra le opportunità offerte dalla trasformazione digitale, ivi incluse le sue estensioni (*blockchain* e g*amification:* v., *supra*, § 3*)* – individui in che termini la *ratio* propria dell'istituto referendario (di fatto, l'autodeterminazione popolare) possa essere non solo rispettata, ma altresì promossa da specifici strumenti tecnologici (v., *supra*, §3) e normativi (v., *supra*, § 4).

Allo scopo, si tratta quindi di combinare requisiti tecnologici (v., *supra*, §3) e normativi (v., *supra*, § 4) che, anziché tradursi in nuovi diritti, si traducono piuttosto nel rafforzamento, mediante ulteriori "qualificazioni", di principi e diritti esistenti. Tali "qualificazioni", come più volte evidenziato, ruotano attorno alla centralità della persona e, proprio per questo, acquistano salienza e momento rispetto all'istituto referendario, nel quale la consapevolezza e responsabilizzazione (una sorta di *due diligence*) dell'elettore è essenziale ai fini di una diretta autodeterminazione non intermediata dalle istituzioni.

Lungo tale percorso campeggia l'approccio *risk-based*, adottato dall'UE sin dal GDPR, volto a favorire la presa di coscienza di quanto la multidimensionalità propria delle sfide digitali non possa essere affrontata in termini meramente paternalistici e difensivi, essendo più funzionale un atteggiamento pro-attivo e sinergico, che si traduce in una chiamata in "corresponsabilità" dei privati da parte dei poteri pubblici[148], i quali si premurano tuttavia di "attrezzare" i primi strutturando i loro diritti con i menzionati "qualificativi" ulteriori (in termini di trasparenza ed equità: v., *supra*, § 4.1).

---

[147] R. J. NEUWIRTH, *The EU Artificial Intelligence Act – Regulating Subliminal AI Systems,* cit.

[148] A.PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, F.P. PATTI, O. POLLICINO, *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista,* in BioLaw Journal, n. 3/2019, 7

L'analisi delle sopra accennate evoluzioni normative (§ 4) e tecnologiche (§ 3) si è dimostrata quindi funzionale agli scopi che ci si era proposti: individuare in che termini tali sviluppi incrocino gli obiettivi giuridico-costituzionali tradizionalmente sottesi all'istituto referendario. Obiettivi che, in estrema sintesi, si traducono nel potenziamento dell'autodeterminazione popolare, e che, per realizzarsi appieno, presuppongono una "strutturazione" alquanto complessa, composta da procedure in grado di rafforzare, per utilizzare due inglesismi attualmente di moda, *awareness* ed *emporwerment* dell'individuo. In definitiva, si tratta di implementare quei presupposti volti a fare sì che la possibilità dell'elettore assumere "decisione dirette", riguardanti la vita collettiva, venga potenziata sia da strumenti tecnologici funzionali al suo *empowerment* (ciò che ci è parso possa derivare dal combinato disposto tra l'istituto referendario e l'impianto tecnologico costituito da *blockchain* e *gamification*, secondo quanto illustrato), che da strumenti normativi funzionali alla sua *awareness* (ciò che ci è parso di poter ritrovare nell'indirizzo seguito dalle menzionate iniziative europee menzionate in termini di rafforzamento della consapevolezza e trasparenza).

Non si ha certo la presunzione di considerare raggiunto l'obiettivo perseguito. Lo sforzo ricostruttivo che è stato intrapreso ha – in tutta umiltà – cercato di far emergere evidenze, "connessioni" e comunanza di finalità, sia all'interno del sistema giuridico che tra questo e altri "sistemi", nell'auspicio di delineare un "perimetro" significativo, entro il quale futuri approfondimenti scientifici possano svilupparsi.

Ferma rimane, in ogni caso, la presa d'atto che è in questa duplice alleanza (tra diritto e tecnologia; tra poteri pubblici e privati) che riposano le odierne "ragioni del diritto" e, con esse, la valorizzazione dell'autodeterminazione singola e collettiva, quindi del principio personalista e democratico[149]: alleanza tanto più importante laddove la decisione sia affidata direttamente agli elettori, com'è il caso del referendum.

[149] Evocando i concetti di "ragioni del diritto" e "democrazia costituzionale" sviluppati da L. FERRAJOLI, *La costruzione della democrazia – Teoria del garantismo costituzionale*, cit., 6 e 235.