Note su digitale e comunicazione politica all’epoca dei Social Network

(Alberto Berretti)

Le opinioni, anche di cosiddetti *esperti*, ahimé, sono spesso condizionate pesantemente o determinate da *onde*. Siamo passati dall'*onda* delle tecnologie digitali come cura universale ad ogni problema (*tele*questo, *e*quest'altro, etc.) all'inevitabile *backlash*, l'*onda* del digitale come padre e madre di ogni disgrazia, in particolare per quanto ci riguarda nel mondo della comunicazione politica e piú in generale nella vita politica del paese. I luoghi digitali dove la gente si incontra e cazzeggia (piú noti come *Social Networks*, concetto di per sé nebuloso ed in cerca di una definizione) in particolare.

Innanzitutto una nota storica: qui è nato, sicuramente in Italia ma con una certa primogenitura anche su scala mondiale, perlomeno nelle intenzioni e nella teorizzazione, non dico *tutto* ma una significativa parte di esso. A Via di Torre Argentina 76 (quindi non proprio qui, ma comunque…) alla fine degli anni '80, quando la rete Internet in Italia era in ambito accademico ai suoi primi vagiti – figuriamoci altrove – c’erano i server, e c’era la batteria di modem, e c’erano le persone, non solo quelle che hanno progettato il software e gestito le macchine, ma anche quelle che hanno pensato ad un’idea di comunicazione on line come ausilio alla comunicazione politica, anche a livello di massa (massa che per l’epoca non poteva che essere estremamente limitata): v. ad es. *Una piazza per la babele radicale* di Caterina Caravaggi e Roberto Cicciomessere, che ancora si può leggere on line archiviato, un testo del 1989. Vi ricordate il 1989? Ecco. Le persone che giravano intorno ad Agorà Telematica hanno, poi, mantenuto contatti e costituito un *nucleo duro* di esperti che sono andati a diffondere l’idea della comunicazione on line come strumento, come dire, per allargare l’area della coscienza, ciascuno nel suo contesto e secondo le sue altre esperienze. È stata una comunità importante in Italia. Furono gettati dei semi.

Ho fatto questa introduzione perché poi stupisce vedere alcune proposte uscire da queste stanze – o da stanze politicamente limitrofe –, proposte piú che altro irrealizzabili, inutili e controproducenti oltre che contrarie a tutto quello che potrebbe essere associabile – ed è un minestrone molto ricco – con *i Radicali* e la loro tradizione. Vediamo, in ordine sparso, queste ed altre cose che sembrano essere poco chiare.

1. Combattiamo l’*hate speech* e le *fake news* sui Social Network introducendo l’*identificazione certa* degli utenti.

Quest’idea, che sembra fluttuare ripetutamente in una forma o nell’altra da molto tempo, è stata ripresa in un post del 13 maggio 2019, a meno di due settimane dalle elezioni europee, sulla pagina Facebook di +Europa: una specie di sondaggio on line, fatto con le reaction di Facebook – delle faccine –, per una proposta – ovviamente vaga e fumosa, non potrebbe essere diversamente – di “identità virtuale certificata” per tutti gli utenti “dei social network”.

Sorvoliamo sull’idea di fare un sondaggio tra utenti random su Facebook, per di piú con le faccine. Badiamo alla sostanza.

Si tratta di una idea sbagliata, in quanto irrealizzabile, pericolosa per il paese perché ci metterebbe su una cattiva strada (molto cattiva), sicuramente inutile e probabilmente controproducente.

Ma vediamo in dettaglio perché si tratta, scusate l'espressione, di una cazzata.

- Parlare di *fake news* non ha molto senso. È uno dei termini piú abusati, ad un livello tale che oramai vuol dire tutto e niente. Parliamo dunque di due possibili situazioni: il cretino di turno che straparla di cose che non sa, e le operazioni di disinformazione organizzate ed eterodirette. Il primo non è un problema serio, il secondo si. Se uno pensa di fermare i secondi con un codice fiscale e con la fotocopia di un documento, beh fa solo ridere. Stiamo parlando di queste cose, di queste altre cose o di queste altre ancora. Stiamo parlando di nemici come ad es. il GRU, mica pizza e fichi.

- I primi, quasi sempre usano il loro nome e cognome (come quelli che scrivevano minacce, insulti e volgarità sulla pagina Facebook della On. Boldrini e poi si sono stupiti di vedersi arrivare la Postale a casa). E comunque non hanno né i mezzi né le conoscenze per creare accessi veramente anonimi (v. sotto).

- Non confondiamo poi pseudonimato ed anonimato. Io posso chiamarmi *farfallina73* e postare con questo nickname dove mi pare, ma sicuramente mi connetto alla rete usando una connessione fissa o mobile. Se uso una connessione fissa, lo faccio da uno studio o da un ufficio o da una connessione ADSL o fibra domestica: in entrambe i casi il sito dove ho pubblicato qualcosa ha l'indirizzo IP, il provider sa qual'è il client dietro a quell'indirizzo IP e dietro mandato di un giudice questi dati saltano fuori. Se uso una connessione mobile, forse è ancora peggio. Per connettermi in forma anonima dovrei rubare una connessione Internet (e notate, le tante WiFi non autenticate che si trovavano una volta non ci sono piú… gli Internet Point ti identificano… le WiFi pubbliche vogliono il tuo numero di telefono…), ovviamente non mi metto qui a suggerire come e dove ma non è semplice ed è di per sé un illecito. E oltre alla connessione rubata, sarebbe bene utilizzare qualcosa come la rete anonimizzante TOR perché non si sa mai: ma TOR non basta, non è facile restare anonimi usando solo TOR (chiedete a Dread Pirate Roberts a.k.a. Ross William Ulbricht, che sta scontando l'ergastolo negli Stati Uniti per aver operato un *dark market* che vendeva droga ed armi via TOR e pensava che TOR e nickname fossero sufficienti per rimanere anonimi; l'FBI e le altre agenzie americane a tre lettere hanno le loro tecniche).

- A proposito, blocchiamo TOR, come in Iran o in Cina?

- Certo, per avere le informazioni di cui sopra e per sapere chi c'è dietro un nickname o dietro un indirizzo IP, addirittura per avere l'indirizzo IP, ci vuole un mandato, e quindi almeno una ipotesi di reato ed un ragionevole dubbio. Se questo non vi piace, dovreste correre a ripassare la voce "Stato di Diritto" sul vostro libro di Educazione Civica.

- Se pensate che sia lo Stato a stabilire quando un'informazione è vera o falsa, o "l'opinione corrente", dovreste correre ancora piú velocemente a ripassare la voce "Stato di Diritto" sul vostro libro di Educazione Civica.

- Stando alle ricerche di Michal Kosinski (https://www.michalkosinski.com/research) dell'Università di Cambridge, dalla nostra attività on line è relativamente facile risalire ad una quantità delle nostre caratteristiche personali. Dati di questo genere, incrociati con altri dati ottenuti in altro modo, permettono di individuare spesso con esattezza di chi è davvero un account Facebook, Twitter, o quant'altro.

- Qual'è poi il problema? Regolamentare cosa esattamente? Mentre pensosi intellettuali, social media manager ed esperti di marketing pensano a Facebook, Twitter, Youtube, Instagram, il numero di siti social è in realtà enorme. Qualunque sito che contiene *user-generated content* può essere trasformato in uno strumento di disinformazione. Segue una breve lista di ambienti social di cui forse non sapete nemmeno l'esistenza: Reddit (piuttosto noto tutto sommato); Mastodon (una rete sociale distribuita: ognuno può installarsi una istanza su un suo server e partecipare alla rete globale); Gab (frequentata dall'alt-right americana); Minds e Mewe (che promettono di non censurare nulla); 4chan (la storica imageboard dove praticamente anything goes, il punto di partenza della vicenda del *Pizzagate*); 8chan (come 4chan ma ancora peggio; conteneva nella home il manifesto di Brenton Tarrant, l'attentatore della moschea di Christchurch in Nuova Zelanda; chiusa dal provider perché gli faceva schifo averla nei sui server pare stia per riaprire); tonnellate di simili imageboard realizzate con il medesimo software e la medesima interfaccia, tante che è difficile tenerne il conto; Mokum (russa); frenf.it (realizzata da innocui e simpatici nostalgici italiani del sito Friendfeed). Ovviamente la Facebook russa, Vkontakte. Stavo per dimenticare una piattaforma popolare ed importante di chat per *gamers* come Discord. Aggiungiamo una quintalata di forum tematici che possono essere facilmente abusati per veicolare operazioni di disinformazione.

- Ma in realtà anche la sezione commenti e recensioni in siti come Amazon o Tripadvisor potrebbe essere abusata. Forse non ci si rende conto della dimensione del fenomeno perché non si sa bene di cosa si sta parlando.

- Non è dunque possibile tenere sotto controllo decine di migliaia (ma no, molti di piú…) di siti contenenti contenuti *user-generated* senza mettersi in una prospettiva di controllo sociale di tipo cinese. È interessante ricordare che nel 2006 l'allora Ministro dell'Istruzione Giuseppe Fioroni, intervistato dal quotidiano La Stampa il 28 novembre, chiese norme per tutelare i minori con filtri obbligatori sulla navigazione in rete, e a domanda «Ma lo sa che nemmeno gli USA hanno una norma simile?» rispose «Mi risulta che ci siano altri Paesi che sono riusciti ad ottenere fior di filtri». E quando l'intervistatore chiese se intendava la Cina, il ministro rispose candidamente «Si», con gli ovvi «anche se» di contorno. Se qualcuno pensa che per sconfiggere le varie "Bestie" che manipolano l'informazione on line sia necessario tutto questo, siamo ai livelli di intelligenza politica di Jar Jar Binks (quando come rappresentante di Naboo convince il Senato della Galassia a dare i pieni poteri per sconfiggere i Sith al cancelliere Palpatine, che abolirà il Senato medesimo e realizzerà l'impero dei Sith: rivedetevi la prima trilogia di Star Wars, una grande lezione sul potere e la politica).

- Infine ci sono ragioni di opportunità. Se obblighiamo solo siti cosiddetti *Over-The-Top* come Facebook, Twitter, Google, etc. a regole stringenti, dirottiamo i contenuti potenzialmente

pericolosi su altre piattaforme su cui il law enforcement ha una leva molto, molto inferiore. Facebook cancella pagine, profili, e collabora se necessario. Siamo sicuri che una imageboard a caso o un socialino come Minds o Mewe si comporti in modo analogo? Molto probabilmente non troveremmo facilmente nemmeno qualcuno con cui parlare in caso di problemi.

Piú in generale, “Regolamentare Internet” è una frase priva di senso. Perché innanzitutto “Internet” non è una cosa, è tantissime cose diversissime tra di loro (cavi, antenne, router, server, software, protocolli di rete, standard, contratti, imprese, utenti, strutture sociali e communities che ruotano intorno a siti, e cosí via). E su *tutte*, dicesi *tutte*, queste cose pesa già una quantità di regole spaventosa. Semmai talvolta si potrebbe pensare che il problema sia il contrario.

2. Ma Facebook è una azienda privata che censura e condiziona il dibattito politico senza alcun controllo!

Di nuovo ci troviamo di fronte ad una affermazione che di per sé vuol dire tutto e niente.

Senza dubbio, i social network ed in particolare Facebook hanno avuto un ruolo in alcune triste vicende politiche recenti, soprattutto tramite la questione Cambridge Analytica (dalle elezioni USA del 2016 al referendum sulla Brexit). Pregevoli studiosi e giornalisti hanno scritto grandi pagine di analisi ed informazione sulla questione (basti pensare a Zeynep Tufekci e a Carole Cadwalladr). Che esista un problema di condizionamento politico da parte dei grandi social network è un dato di fatto. Il problema è in realtà duplice.

- Da una parte, abbiamo il fatto elementare che dal momento che le forme di comunicazione digitale esistono, queste diventano *naturalmente* un terreno di scontro politico esattamente come qualsiasi altra forma di comunicazione umana. In Italia abbiamo una tradizione nello scegliere forme di regolamentazioni demenziali ed inutili se non controproducenti in tanti altri campi della comunicazione (e non solo): basta ad es. pensare alla famosa *par condicio* televisiva con tutte le norme che ne conseguono e al ridicolo silenzio preelettorale dei sondaggi (e diciamolo chiaro e forte, viva le corse clandestine di Mancia e Bressan!). I tentativi di ripetere gli stessi sbagli, o sbagli fortemente analoghi, anche nel digitale vanno accuratamente evitati. Noi abbiamo in realtà di fronte a noi un grosso problema di *antitrust*, e cioè di strapotere che alcune piattaforme digitali in specifici settori detengono (stiamo in questo caso parlando di Facebook, in Italia, per quanto riguarda la socialità on line: altrove saranno altri, ad es. Vkontakte in Russia, WeChat, QQ e Weibo in Cina…).

  Si, Facebook fa schifo per una quantità di ragioni, che vanno dall’invadenza pubblicitaria (ma è gratis!), ad un app mobile micidiale in quanto a pesantezza, consumo di batteria e problematiche di privacy, ad una interfaccia utente penosa, ad una sezione di messaggistica interpersonale – Messenger – che fa ancora piú pena e di cui nessuno in fondo sente il bisogno, ad un controllo sconclusionato ed incomprensibile dell’ordine e della visibilità dei post insieme a criteri di cancellazione dei medesimi per violazione di termini di servizio e regole mal specificate che portano a situazioni paradossali (a proposito, è stata sospesa per *hate speech* la pagina ufficiale di Netanyahu qualche giorno fa!). La soluzione però non è

obbligare Facebook a far di meglio, ma favorire un *ecosistema social* in cui altri attori possano prosperare e non solo vivacchiare ai margini. Questione che ovviamente va affrontata non a livello nazionale ma perlomeno a livello comunitario.

Questo è il problema che va affrontato, e non imporre a Facebook cosa può e non può lasciare sulla sua piattaforma (a parte quanto prescrive il codice penale ovviamente). L'affermazione secondo la quale Facebook è di fatto uno spazio pubblico di comunicazione politica e pertanto devono essere garantiti degli spazi (e chi stabilisce i criteri se non lo Stato?) è infatti pericolosissima: lo Stato non deve entrare in cosa un privato pubblica o non pubblica sulla sua piattaforma – fatto salvo, ripetiamo, il codice penale. Una delle prime cose che imparammo su Agorà Telematica fu il celebre adagio "Freedom of the press is the freedom to own one", frase che credo di aver sentito pronunciare per la prima volta là dentro da Roberto Cicciomessere. Proporre un'idea di regolamentazione di Facebook come spazio di comunicazione pubblico ci pone al livello Jar Jar Bink della politica, esattamente per le stesse ragioni e con la stessa modalità del simpatico personaggio. E sicuramente cosí ragionano i fascisti di Casa Pound e di Forza Nuova, che si sono giustamente trasferiti su Vkontakte, il social russo, dove la loro libertà di opinione verrà difesa da quel campione della democrazia che è Vladimir Putin.

- Dall'altra parte, abbiamo che questa prodigiosa macchina di comunicazione non lavora da sola e automaticamente per nefasti scopi imperscrutabili. Il problema, come dicevamo sopra, non sono tanto le *fake news* o la censura algoritmica e piú o meno ridicola ed arbitraria fatta fare in outsourcing da terzi. Il problema sono le campagne di influenza condotte da attori potenti e molto ben attrezzati che sanno esattamente cosa fanno, che sfruttano strumentalmente *utili idioti* per propagandare idee allo scopo di destabilizzare nemici strategici. Stiamo parlando dei servizi russi e cinesi. Qui non serve regolamentare Facebook, serve uno sforzo professionale di *counter-intelligence* per bloccare delle campagne che hanno un nome ben preciso nome: misure attive, Активные мероприятия, ovvero tecniche di disinformazione e provocazione utilizzate di routine dai servizi dei paesi autoritari dell'Est Europa e ancora piú a est da decenni. Potete fare un giro qui per avere un'idea della dimensione del problema. In questa battaglia, le grandi compagnie del digitale, i Google, i Facebook etc. devono essere nostri amici, sono anzi fondamentali nel contrastare tali campagne.

- Oltre ad una azione professionale di *counter-intelligence* – di cui non si può fare a meno –, oltre al coinvolgimento degli *Over-The-Top* nella repressione della disinformazione mirata alla *distruption* delle democrazie liberali, occorre un grande sforzo di contrasto di tale disinformazione on line, svolto attivamente e seriamente da persone che sappiano muoversi in quest'ambiente. Occorre creare una figura di *militanti digitali* che sappiano colpo su colpo combattere le campagne di disinformazione, veicolando i risultati del lavoro di gruppi di OSINT (*Open Source Intelligence*) come appunto il Digital Forensic Lab sopra citato, o Bellingcat, ad un pubblico vasto che altrimenti non ne verrebbe mai a conoscenza.

3. A modo di appendice: una nota sul voto digitale e sull'e-populismo.

Una delle tante idee di digitalizzazione che circola e non da poco è quella delle elezioni, dell'espressione cioè a fini politici delle preferenze popolari. Uno dei fiori all'occhiello dei pentastellati è peraltro proprio la famosa Piattaforma Rousseau, un sistema di voto on line che un notaio ha certificato essere sicuro "un po' come il televoto di Ballando con le Stelle" (non si capisce peraltro che competenza di protocolli crittografici possa avere un notaio).

Il voto tradizionale, *cartaceo*, ha – perlomeno nella sua declinazione italiana – una serie di *features* di sicurezza fortissime che non vengono in genere notate se non si è abituati a fare attenzione ai dettagli.

Innanzitutto, gli aventi diritto si presentano al voto con *due* documenti: una tessera elettorale, che viene spedita a domicilio dell'elettore e che certifica che la tal persona ha diritto al voto, ed un documento identificativo personale (ad es. una carta di identità) che ne certifica l'identità. Sostituzioni di persona su piccola scala – qualche elettore – potrebbero accadere, ma su vasta scala, tali da modificare il risultato elettorale, sono implausibili. L'avvenuta espressione del voto viene certificata con *un timbro indelebile apposto sulla tessera elettorale* e mediante *l'iscrizione dell'elettore in un registro dei votanti*, oltre che con il fatto che ogni elettore vota in una singola specifica postazione, determinata a livello di quale stanza in quale edificio, pertanto per votare due volte si dovrebbe recare due volte nel medesimo posto dalle medesime persone nell'arco di qualche ora, oltre al problema che dovrebbe cancellare il timbro dalla tessera elettorale e in qualche modo miracoloso cancellare il *record* dell'avvenuta votazione dal registro.

Pertanto per sovvertire un'elezione *cartacea* sembrerebbe che il metodo migliore sia la corruzione degli addetti al seggio, che effettuano anche la conta dei voti. In realtà questo tipo di attacco è gestito in modo brillante mediante controlli incrociati da parte di attori che hanno interessi contrapposti e che quindi si bilanciano: gli scrutatori, delegati dalle varie liste a presidiare le operazioni di spoglio dei voti. Di nuovo, è in linea di principio possibile che presso un seggio uno scrutatore possa essere corrotto, ma per modificare in modo significativo i risultati di una elezione occorre corrompere *parecchi* scrutatori in molti seggi, e certamente nascondere uno sforzo del genere è praticamente impossibile.

Non solo, ma la modifica del voto espresso sulla scheda è, come si direbbe in gergo, *tamper-evident*: una scheda con cancellazioni è immediatamente identificata. Un vantaggio delle *cose analogiche* è che le loro copie, o le loro modifiche, sono in genere sottilmente diverse dall'originale o comunque dal giusto, un po' come una vecchia copia su audiocassetta di un LP era degradata mentre la copia digitale di un file musicale MP3 è totalmente identica all'originale. Le schede marcate in modo anomalo vengono ugualmente scartate per garantire l'anonimità del voto, ed i trucchi possibili con l'espressione di preferenze multiple sono stati eliminati dal referendum del 1991.

Infine, la *sicurezza fisica* dei seggi elettorali è affidata alle forze dell'ordine, che possono ulteriormente verificare l'identità di chi entra ai seggi.

Si osservi che tutto questo accade alla luce del sole: ogni meccanismo di cui si compone lo svolgimento di una elezione è qualcosa di apparente, visibile e constatabile in forma diretta ed immediata da chiunque sia presente all'evento. Non è necessario avere *fiducia* – quello che nell'inglese informatichese si chiama *trust* – in alcun componente del sistema, perché è tutto immediatamente percepibile in forma diretta, senza oggetti tecnologici che intermediano, oggetti in cui troppo spesso poniamo una fiducia inconsapevole e mal riposta. Il meccanismo che si frappone fra la volontà dell'elettore e l'espressione del voto è banale ed immediatamente accessibile alla percezione umana senza intermediazioni (braccio, matita copiativa, scheda elettorale, urna).

Il voto cartaceo dunque – per lo meno nel modo in cui viene espresso nel nostro paese – ha delle caratteristiche di sicurezza formidabili. Quali sono i suoi svantaggi?

Gli svantaggi che vengono in genere citati sono il costo e la lentezza. Ma entrambe sono questioni molto secondarie. A fronte di tutto questo, *tutti gli esperti di sicurezza informatica degni di questo nome sono unanimi nel definire qualsiasi forma di voto elettronico una chimera, una impossibilità teorica, se vogliamo che abbia le medesime caratteristiche di sicurezza del voto cartaceo.* Punto. A cominciare da personaggi del calibro di Matt Blaze o Steven Bellovin.

Per farla breve, molto breve, qualunque tentativo di emulare il medesimo protocollo elettorale in forma digitale va a al contrario a sbattere contro un limite di *qualsiasi* tecnologia digitale. Infatti, prendiamo lo step "gli aventi diritto si presentano al voto con due documenti: una tessera elettorale che certifica che la tal persona ha diritto al voto ed un documento identificativo personale che ne certifica l'identità". Mentre come dicevamo prima nel voto tradizionale questo viene compiuto esplicitamente, e può essere verificato in modo *diretto*, in forma digitale uno step del genere non verrebbe preso direttamente dalle persone fisiche, ma da processi che avvengono in apparati informatici, verso i quali *occorre avere fiducia, trust,* ovvero l'utente deve compiere un atto di fede nella correttezza e nella reale implementazione del protocollo che si sostiene sia stato implementato.

Le tecnologie digitali insomma sono *opache*, ed ogni loro utilizzo implica un vero e proprio atto di fede nel fatto che facciano davvero quello che dicono di fare. E sappiamo bene – basta leggere un po' in giro! – che *bugs* e trappole di vario genere infestano una quantità di strumenti informatici realizzati con le migliori intenzioni. Figuriamoci quando si tratta di sistemi per il voto, che hanno un gigantesto bersaglio dipinto sopra per *hacker* e sabotatori di ogni genere. Ora, gestire questa *fiducia* e far sí che una tecnologia digitale la meriti è parte del mestiere di alcuni di noi, ed è in alcuni casi un rischio che vale la pena di correre rispetto all'utilizzo di tecnologie manuali (ad es. il telecontrollo di un sistema di distribuzione dell'energia elettrica, che è davvero quello che in gergo chiamiamo *infrastruttura critica*, è un grosso passo avanti rispetto alla gestione manuale: *anche dal punto di vista della sicurezza*). Ma non è certo il caso dell'espressione del consenso popolare. Si, so come si vota in Estonia e so che l'ideatore del sistema di e-voting estone vota cartaceo; tutta l'Estonia ha meno abitanti di Roma.

Ma c'è un problema piú sottile e complesso, e di natura fondamentale. I teorici della democrazia moderna, dai padri fondatori degli Stati Uniti, a Tocqueville, a Stuart Mills, a Edmund Burke, si sono posti il problema della degenerazione della democrazia in una *dittatura della maggioranza*.

Si sono cioè posti domande come le seguenti. Sulla base della decisione della maggioranza, è possibile abbandonare un punto di vista razionale e decidere a maggioranza di… giustiziare gli untori, bruciare le streghe o decidere che 2+2 fa 5? È possibile che un gruppo organizzato intorno ad un argomento specifico, raggiunta la maggioranza, possa imporre il suo punto di vista indipendentemente dalle conseguenze che tale punto di vista possa avere sulla società nel suo insieme? Possiamo decidere a maggioranza che un determinato gruppo etnico minoritario vada eliminato, esiliato, scacciato dal paese? Può la maggioranza meno ricca del paese decidere di tassare come se non ci fosse un domani la minoranza piú ricca e redistribuire la ricchezza? In particolare, uno dei *Federalist Papers*, scritto da James Madison, si pone esattamente quest'ultimo problema.

Sappiamo bene che non esiste una soluzione *algoritmica*, esatta come la dimostrazione di un teorema, a tale problema. Esistono però due secoli abbondanti di storia e di pratica della democrazia, un cospicuo travaglio politico e filosofico, che culmina piú o meno nel capire che la democrazia ha dei limiti senza i quali essa si trasforma nel suo opposto. Pensate al meccanismo del Collegio Elettorale negli Stati Uniti, o ai limiti posti all'istituto del referendum in Italia. La democrazia è rappresentativa, e non diretta, proprio per scongiurare i rischi di una dittatura della maggioranza.

Bene, queste *contromisure* ai rischi di derive plebiscitarie che hanno – piú o meno bene – funzionato per molto tempo sono rimaste travolte dal digitale. Infatti tutto il dibattito politico-filosofico a cui sopra accennavo si basava sul fatto che la comunicazione politica avvenisse in modo, diciamo cosí, tradizionale. Le comunicazioni digitali, con la loro elevata larghezza di banda, con la loro capacità di diffondere notizie, vere o false che siano, massicciamente e rapidamente e di disintermediare dai filtri tradizionali, hanno sconvolto questi meccanismi. In questo noi pionieri abbiamo avuto la vista corta e ci siamo sbagliati: i rischi della comunicazione politica digitale sono sicuramente maggiori dei vantaggi, ma è tardi e l'inevitabile è accaduto quindi è inutile parlarne.

Il problema viene spesso posto in questi termini: i social network vengono utilizzati dalla politica per manipolare l'opinione pubblica. Leggete la Tufekci, leggete la Cadwalladr sul *Guardian*, l'idea è tipicamente questa. E se fosse invece il contrario? E se la comunicazione digitale, grazie alle caratteristiche sopra citate (pervasività, continuità, velocità, ampiezza quantitativa del flusso informativo trasmesso), avesse passato una soglia oltre la quale i filtri tradizionali cessano di funzionare? Se fosse la comunità politica a venire incontro ad idee estreme per ottenere il consenso di folle digitali che si radicalizzano spontaneamente? Non essendo ovviamente possibile tornare indietro, occorre impare a muoversi in un mondo difficile e pericoloso conoscendone bene le regole ed il funzionamento.