LA MANIPOLAZIONE ONLINE

DELLE INFORMAZIONI PERSONALI E LE SFIDE DEMOCRATICHE

Giovanni Buttarelli

Negli ultimi anni l'integrità dei processi di partecipazione democratica e la fiducia nella regolarità dei procedimenti elettivi sono state oggetto di vivaci discussioni. Tra i temi più dibattuti si è parlato a lungo di fake news e di manipolazione online intendendo, con quest'ultima espressione, quel modello di business basato sulla raccolta del maggior numero possibile d'informazioni personali destinate a essere monetizzate per prevedere e orientare futuri comportamenti, scelte, preferenze e manifestazioni di volontà di cittadini anche non identificati. A questo aspetto il Garante europeo della protezione dei dati ha dedicato uno studio e una serie di iniziative con l'obiettivo di contribuire a prevenire la manipolazione e a responsabilizzare i detentori d'ingenti quantità di dati affinché intervengano nei confronti di coloro che indebitamente li manovrano.

Le moderne democrazie, anche al di fuori dell'Unione europea, prevedono il periodico ritorno alle urne per consentire ai cittadini di esprimere la propria volontà e le proprie scelte, liberamente e segretamente. Ogni tornata elettorale ha una sua specificità e rilevanza. Tuttavia, quella che si prospetta in Europa nel 2019 è di particolare interesse. In aggiunta a elezioni locali o di dimensione puramente regionale, sono previste sessioni di consultazione politica nazionale in almeno tredici paesi europei. In più, tra il 23 e il 26 maggio i cittadini dell'UE avranno un'importante opportunità per disegnare il futuro dell'Unione attraverso il rinnovo dei membri del Parlamento.

Tutto ciò accade a quasi dieci anni dall'entrata in vigore dei trattati di Lisbona (1° dicembre 2009), a quasi trent'anni dalla caduta del muro di Berlino, e a quarant'anni da quando è stato espresso per la prima volta il voto per il Parlamento europeo.

GIOVANNI BUTTARELLI

Sempre nell'anno corrente si voterà anche fuori dall'Europa. Si terranno, ad esempio, elezioni generali in India e in almeno due importanti stati africani: Sudafrica e Nigeria.
L'integrità e la regolarità di questi processi di partecipazione democratica, nonché la fiducia nella correttezza dei procedimenti elettivi sono state, negli anni più recenti, oggetto di vivaci discussioni.
Il dibattito sul referendum inglese sulla Brexit, come quello relativo alle ultime elezioni federali statunitensi, hanno portato alla luce alcune preoccupazioni circa possibili campagne di disinformazione, incidenti informatici su larga scala e, persino, indebite interferenze esterne, al punto tale che alcuni paesi, per prevenire illecite influenze e rassicurare la popolazione, hanno preferito tornare al trattamento non automatizzato delle espressioni di voto.
In tale cornice, tra i temi più dibattuti degli ultimi tempi emerge quello delle fake news e delle attività di disinformazione organizzata. In realtà, non si tratta di un argomento inedito e recente, visto che anche nel passato più remoto si sono palesate criticità in tali ambiti, sebbene tecnologie sempre più innovative e, in special modo, la febbricitante comunicazione che si sviluppa su alcune grandi piattaforme, evidenziano problematiche più forti.
Per questo, avendo avuto l'onore di essere invitato nel settembre 2017 al vertice G7 dell'Avvocatura, nel quadro della Presidenza italiana, dedicato alle fake news e alla manipolazione online, ho ritenuto significativo proporre uno studio articolato avente a oggetto soprattutto il secondo tema.
Nell'opinione che il Garante europeo della protezione dei dati ha pubblicato nel marzo del 2018 sulla manipolazione online[1] si è fatto ampio riferimento alle più moderne tecniche che permettono a un innovativo modello di business di profilare su larga scala utenti, consumatori e abbonati, e di utilizzare miliardi d'informazioni a essi riconducibili per finalità non prettamente commerciali e in termini non sempre trasparenti. A questo contributo ha fatto seguito l'opinione del 17 dicembre 2018[2], relativa al recente pacchetto[3] della Commissione europea, di cui si dirà meglio in seguito, orientato a incrementare le iniziative necessarie per assicurare serenità e piena democraticità delle imminenti elezioni europee, permettendo a tutti i partiti e movimenti politici di fare adeguato uso dei nuovi mezzi di comunicazione, senza però diminuire la fiducia di cittadini, utenti e consumatori sulle modalità di utilizzo delle informazioni acquisite.
Da queste ultime esperienze è stata tratta la conclusione che fake news e disinformazione non sono fenomeni tipici solo degli ultimi anni, anche se il ricorso a potenti piattaforme informative permette di raggiungere più facilmente obiettivi impropri.
D'altro canto, anche in ragione della specificità della missione dell'istituzione europea cui ho avuto l'onore di essere preposto, ho preferito concentrarmi su un concetto di conio più recente: la manipolazione.
Intendo qui riferirmi a un particolare modello di business che potrebbe divenire definitivamente dominante sull'intera scala planetaria, basato sulla raccolta massiccia d'informazioni personali, anche senza un preciso scopo prefissato, destinate a essere monetizzate per prevedere e orientare in maniera granulare futuri comportamenti, scelte, preferenze e manifestazioni di volontà di cittadini, anche non identificati.
Si è detto che questo modello è destinato a rimanere di fatto 'inevitabile', specie alla luce dello sviluppo delle nuove tecnologie, anche se si tratta di un fenomeno recente, sviluppatosi nel corso degli ultimi vent'anni sull'onda dell'esplosione della cosiddetta bolla «.com».
L'attuale ecosistema dell'informazione digitale rende più agevole il capillare e non del tutto trasparente monitoraggio dei più minuti comportamenti in rete, grazie anche alla crescente concentrazione della maggior parte delle informazioni nelle mani di un ristretto numero di piattaforme, al momento situate largamente nei territori di partner strategici dell'Unione europea, ma che domani potrebbero fiorire anche altrove. Questi intermediari si pongono l'obiettivo, pubblicamente dichiarato, di favorire il coinvolgimento e l'interazione di miliardi di utenti ma, si sa, niente coinvolge di più della preoccupazione, dell'ansia e del sensazionalismo. In tale ambito, l'obiettivo delle autorità per la protezione dei dati non è quello di ridurre il tasso di utilizzo delle piattaforme social da parte di utenti, consumatori e abbonati. Sarebbe deprecabile se lo sviluppo delle tecnologie si ponesse come ostacolo al diritto-dovere d'informare, essere informati ed esprimere o meno il proprio punto di vista, in pubblico o in privato.
Il nostro obiettivo è piuttosto quello di contribuire alla protezione dei dati personali, responsabilizzando maggiormente coloro che creano ingenti profitti, ma non intervengono ancora adeguatamente nei confronti di chi opera indebite manipolazioni.

1. <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf> [12-2-2019].
2. <https://edps.europa.eu/sites/edp/files/publication/18-12-18_opinion_on_election_package_en.pdf> [12-2-2019].
3. <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-free-fair-elections-communication-637_en.pdf> [12-2-2019].

Ci si occupa non tanto di ciò che è vero e di ciò che è falso, quanto piuttosto delle forme di controllo sui trattamenti dei dati di carattere personale, che possono assicurare benefici sproporzionati ad alcuni soggetti, a sfavore di altri, in un quadro di relativa trasparenza.
La dimensione del controllo, attraverso l'assembramento in tempo reale di miriadi di informazioni provenienti da più risorse, non sempre residenti nei dispositivi che utilizziamo ma a volte rese inavvertitamente accessibili tramite la rete anche quando detti dispositivi sono in apparente pausa, si basa su un tracciamento continuo, su una profilazione segreta, sulla creazione di cluster e sul cosiddetto microtargeting. Ciò può portare a situazioni di smodato vantaggio informativo o alla distribuzione ineguale di contenuti essenziali per il processo democratico, nel senso che alcune piattaforme, mediante possibili interazioni arbitrarie con talune applicazioni, possono fare la differenza nell'ambito delle prassi contrattuali con organizzazioni e partiti politici.
Vi è anche un elemento di opacità da tenere presente perché – sfortunatamente e contrariamente allo spirito del nuovo Regolamento europeo sulla protezione dei dati personali[4], pienamente applicabile dal 25 maggio 2018 – diverse *privacy policies* pubblicate o rese accessibili in rete sono state configurate con un linguaggio non comprensibile per un utente medio, e ispirate più a proteggere il titolare del trattamento che a permettere all'interessato di comprendere le conseguenze delle proprie manifestazioni di volontà. Anche quando tali privacy policies sono orientate a un tasso maggiore di correttezza, è a volte difficile comprenderne appieno il significato. Si è calcolato che se un utente medio dovesse leggere tutte le informative sulla privacy che gli si prospettano nell'ambito della sua normale attività – quale appunto utente medio – sarebbero necessari almeno 54 giorni l'anno. Ciò comporta anche una difficoltà nel contestare ed eventualmente negoziare questo tipo di clausole. Questa opacità riguarda ancor più le tecniche di analisi dei dati che derivano non soltanto dalla pionieristica intelligenza artificiale e dal *machine learning*, ma anche dall'assembramento di risorse informative, le più disparate, che possono riguardare persino le incertezze con cui utilizziamo sistemi di dettatura, tastiere e finanche il tipo di compulsività che ci caratterizza quando impartiamo istruzioni a un sistema di intelligenza artificiale contenuto nei nostri computer.

4. <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT> [12-2-2019].

Lo scenario sinteticamente descritto ha permesso ai regolatori indipendenti in materia di protezione dei dati personali di dimostrare agevolmente che il loro lecito e corretto utilizzo è un prerequisito per il pieno godimento di tutte le libertà fondamentali, ivi comprese quelle relative alla sfera religiosa, sindacale e politica.
Come affrontare tali sfide negli anni a venire, tenendo presente che le piattaforme digitali sono e saranno incessantemente usate nella campagna politica e che i social media e i video sharing hanno rivoluzionato il coinvolgimento politico?
Simili strumenti possono dare a forze e movimenti politici accesso diretto – lecito o illecito – alle informazioni personali dell'elettorato, con un grado di analisi dettagliata dei comportamenti, delle aspettative e preoccupazioni. Algoritmi dalla logica non molto trasparente sono utilizzati per creare profili di consumatori ed elettori, attenti a questo o a quel problema sociale, per classificarli come *hard believer*, indecisi o restii ad avere un'opinione precisa. Il caso Cambridge Analytica – come ho più volte affermato – non è che la punta di un iceberg, come peraltro dimostrano le indagini condotte dalla nostra autorità 'sorella' nel Regno Unito (Ico) che si sta occupando ora, dopo Facebook e Cambridge Analytica, di ben quaranta organizzazioni politiche. La prospettiva non è tanto e necessariamente quella di emanare nuove regole, perché i settori della protezione dei dati, della materia elettorale e audiovisiva nonché dell'antitrust sono governati già da un corpus consistente di norme. Piuttosto, il problema riguarda il coordinamento, la cooperazione amministrativa e anche l'*enforcement*.
Nel 2013, una ricerca europea ha dimostrato che tra le autorità operanti in materia non si verifica ancora un'efficiente collaborazione che permetta di lavorare meno a compartimenti stagni. Ciascuno di questi regolatori ha competenze e poteri efficaci, ma una migliore interazione è sempre più necessaria se vogliamo preservare effettivamente i diritti di libertà e la democraticità dei processi. In tale quadro, può essere d'esempio la recente iniziativa della Commissione europea sopra richiamata, circa un pacchetto di misure che includano un meccanismo volto a facilitare la collaborazione tra gli operatori.
Il pacchetto comprende, oltre a una proposta legislativa: una proposta di regolamento del Parlamento europeo e del Consiglio che innova il regolamento (UE, Euratom) n. 1141/2014 nella parte relativa alla procedura di verifica circa le violazioni delle norme sulla protezione dei dati personali nel contesto delle elezioni del Parlamento europeo[5]; una comunicazione

5. <http://ec.europa.eu/transparency/regdoc/rep/1/2018/IT/COM-2018-636-F1-IT-MAIN-PART-1.PDF> [12-2-2019].

sulla sicurezza di elezioni europee libere ed eque[6]; una raccomandazione sulle reti di cooperazione elettorale, la trasparenza online, la protezione contro gli incidenti informatici e la lotta contro le campagne di disinformazione nel contesto delle elezioni al Parlamento europeo[7]; una guida all'applicazione della normativa dell'Unione sulla protezione dei dati nel contesto elettorale[8].

Il pacchetto è stato redatto con l'obiettivo di assicurare libertà e giustizia in occasione delle prossime elezioni del Parlamento europeo, tenendo conto delle nuove sfide poste dalla comunicazione online e dalle recenti rivelazioni come, ad esempio, il citato caso Cambridge Analytica.

Esso si pone, peraltro, in evidente complementarietà con il comunicato stampa della Commissione del 26 aprile 2018 «Affrontare la disinformazione online: un approccio europeo», che mira a promuovere un ambiente online più trasparente, affidabile e responsabile e di cui costituisce elemento fondamentale il Codice di autodisciplina in materia di disinformazione, pubblicato il 26 settembre 2018, cui è seguito il parere del comitato di esperti del forum multilaterale sul Codice di condotta[9].

La proposta di Regolamento, peraltro, si prefigge l'individuazione di sanzioni pecuniarie pari al 5% del bilancio annuale, da comminare a partiti o fondazioni politiche europee che agiscano in violazione delle norme sulla protezione dei dati per influenzare deliberatamente, o tentare di influenzare, l'esito delle elezioni al Parlamento europeo.

Inoltre, nella raccomandazione, la Commissione incoraggia le autorità nazionali preposte alla protezione dei dati a informare immediatamente e in modo proattivo l'Autorità per i partiti politici e le fondazioni politiche europei circa le proprie decisioni aventi a oggetto violazioni delle norme sulla protezione dei dati, nelle quali l'infrazione sia collegata ad attività politiche da parte di un partito o di una fondazione politica europea «al fine di influenzare le elezioni del Parlamento europeo».

6. <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1537434682871&uri=CELEX%3A52018DC0637> [12-2-2019].
7. <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cyber security-elections-recommendation-5949_en.pdf> [12-2-2019].
8. <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf> [12-2-2019].
9. <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> [12-2-2019].

Il Consiglio ha dichiarato di aver aperto i negoziati sul testo del regolamento con il Parlamento a partire dall'inizio del 2019[10].

Il 12 marzo 2019 il Parlamento europeo e il Consiglio dell'UE hanno adottato le nuove regole, sancendo che le disposizioni sulla nuova procedura di verifica entrino in vigore il giorno della pubblicazione del Regolamento nella Gazzetta Ufficiale dell'UE, al fine di assicurarne l'applicazione alle prossime elezioni del Parlamento europeo.

Tale iniziativa si somma alle altre di soft regulation che la Commissione ha intrapreso, attraverso, ad esempio, l'aggiornamento dei codici di condotta con i quali s'invitano anche i giganti dell'informazione a impiegare più risorse per far sì che i fenomeni delle fake news, dell'*hate speech* e dell'illecita propaganda online vengano contenuti quanto più possibile.

In conclusione, l'Europa ha tutte le possibilità per dimostrare al resto del mondo di saper far fronte con saggezza a tutti questi problemi, allo scopo di favorire una maggiore circolazione delle idee e, al tempo stesso, rassicurare partiti, movimenti politici, elettori e singoli cittadini sulla trasparenza e sulla regolarità del processo elettorale.

Sta a noi, adesso, usare tali strumenti nel modo più assennato ed efficace possibile

10. <https://www.consilium.europa.eu/en/press/press-releases/2019/01/25/eu-set-to-ado pt-new-rules-to-prevent-misuse-of-personal-data-in-ep-elections/> [12-2-2019].