QUEI POTERI DIGITALI OCCULTI

Web e politica La Rete sta diventando fonte di minacce al funzionamento della democrazia. In Italia di recente il presidente Mattarella è stato oggetto di un attacco

Corriere della Sera · 4 ag. 2018 · 1 · di Maurizio Ferrera

In politica la battaglia per la trasparenza non finisce mai, anche dopo l'abbattimento dei governi autocratici. Non è mai vinta una volta per sempre.
Così diceva Bobbio nei primi anni Novanta: per il grande studioso torinese, la democrazia deve guardarsi dai poteri occulti. Quelli che partono dai governanti, invocando la ragion di Stato (segreti e menzogne per salvaguardare la sicurezza: i cosiddetti arcana imperii); ma anche quelli che partono dal basso, ad esempio per ribaltare il regime (gli arcana seditionis).
Bobbio aveva in mente il terrorismo e lo stragismo degli anni di piombo. Due minacce non certo scomparse, ma diventate oggi semplici gocce nel grande mare del «cyperspazio».
Internet ha rivoluzionato il mondo della comunicazione, aperto e globalizzato i nostri orizzonti di riferimento, democratizzato l'accesso e l'uso della conoscenza. Sulle virtù e i benefici di questi cambiamenti non possiamo avere dubbi. Tuttavia, come in tutte le innovazioni tecnologiche, vi sono risvolti negativi. Il cyberspazio offre un terreno fertile per la emergenza di nuovi poteri occulti, moltiplica occasioni e risorse per il perseguimento di obiettivi illeciti e criminali, per subdole intrusioni nella sfera personale. Ma soprattutto sta diventando una fonte di allarmanti minacce al funzionamento della democrazia.
L'
SEGUE DALLA PRIMA esempio più eclatante è l'interferenza della Russia di Putin nelle elezioni americane del 2016, documentata in abbondanza dalle inchieste del Senato, che hanno giustamente parlato di «guerra informatica». Un episodio recentissimo ha riguardato anche l'italia. Come rivelato dal Corriere di giovedì, il presidente Mattarella è stato oggetto di un attacco digitale lo scorso 27 maggio, quando si rifiutò (nel pieno esercizio delle sue prerogative costituzionali) di avallare la nomina di Paolo Savona al ministero dell'economia. Uno tsunami di Twitter (#Mattarelladimettiti) si diffuse a macchia d'olio nei social media, indirettamente ricollegabile alla «fabbrica di falso» che la Russia ha costruito a San Pietroburgo. Secondo molti esperti, la Russia dispone oggi del più esteso ed elaborato arsenale per questo nuovo tipo di guerra e sta perseguendo una ambiziosa strategia di de-stabilizzazione delle istituzioni occidentali, attraverso campagne mirate di disinformazione.
La Cina è a sua volta diventata la seconda potenza «militare» informatica globale.
I poteri digitali occulti possono attaccare le nostre democrazie in vari modi. Innanzitutto, danneggiando i sistemi informatici. In Estonia tempo fa Internet ha smesso di funzionare

in corrispondenza con manovre russe; la Cina è nota per diffondere virus sconosciuti. Pensiamo a cosa potrebbe succedere se in città come Chicago o Mosca venisse sospesa l'energia elettrica durante l'inverno: danni certamente superiori a quelli di un bombardamento tradizionale. Un altro allarmante pericolo è la possibile distruzione di alcune infrastrutture materiali su cui poggia la Rete. Proteggersi da queste minacce non è facile. Contro il potere delle armi i governi possono ricorrere alla reciproca deterrenza, com'è successo durante la guerra fredda. Questa strategia è oggi molto meno efficace data la presenza nella Rete di una moltitudine di attori non governativi che possono controllare ingenti risorse «distruttive» con bassissimi costi di entrata e ampie possibilità di fuga. Sta nondimeno emergendo un sistema di protonorme internazionali volte a diminuire i rischi. Esistono
dProspettive preoccupanti Lo scenario che si sta delineando oggi solo pochi decenni fa era inimmaginabile
poi strumenti più o meno sofisticati di protezione per le infrastrutture materiali e immateriali della Rete all'interno di singole giurisdizioni nazionali.
Il pericolo maggiore per la democrazia resta però la manipolazione dell'opinione pubblica, sempre più «connessa» e incline a usare i social network per ottenere informazioni. Contrastare questo fenomeno è molto difficile, e non solo sotto il profilo tecnico. La disinformazione organizzata sceglie con cura i propri bersagli. Quasi sempre si tratta di elettori già orientati in un determinato senso (contro Hillary Clinton; pro-5 Stelle o pro-lega) oppure in- decisi. Le fake news amplificano passioni e pregiudizi. Le ricerche di psicologia politica forniscono sconfortanti indicazioni: anche se esposti a informazione «vera» sullo stesso fatto, gli elettori già schierati raramente cambiano opinione. Anzi: il cosiddetto fact checking può diventare un ulteriore incentivo alla mobilitazione in senso contrario. A loro volta, gli indecisi spesso non hanno le capacità per cogliere il falso. Per fortuna ci sono anche elettori non sensibili alla disinformazione. Ma questi tendono a essere meno attivi, non si mobilitano «contro». L'unica strategia potenzialmente efficace sembra essere quella di cambiare la narrazione: di usare dati e fatti «veri» per costruire cornici interpretative che rendano irrilevanti o non pertinenti le più eclatanti fake news. È una soluzione che richiede tempi lunghi ed elevate capacità di comunicazione e persuasione.
Basata com'è sul pragmatismo delle buone ragioni e del sapere empirico, la liberaldemocrazia è stata definita come una «macchina per la verità»: un insieme di regole e un ethos collettivo capaci di scartare il falso attraverso il confronto tra punti di vista e tra questi e la realtà. Con l'intreccio fra poteri occulti e cyberspazio stanno però proliferando nuove «macchine per la falsità» nei confronti delle quali le attuali pratiche liberaldemocratiche appaiono altamente vulnerabili. È come se la libertà di opinione e l'apertura stessero scatenando una pericolosa sindrome auto-immune, in cui la democrazia finisce per erodere le proprie fondamenta. Uno scenario inimmaginabile solo pochi decenni fa, e per niente rassicurante.