Teknologirådet

Valg, teknologi og politisk påvirkning

Den nye politiske kampanjen

Sosiale medier og digitale verktøy har endret hvordan valgkamper organiseres og gjennomføres. Dette gjelder særlig to områder:

- Budskap kan spisses og persontilpasses mot individer langt mer effektivt enn tidligere, samtidig som potensialet for å nå store velgergrupper er enormt.
- De digitale verktøyene er globale og lett tilgjengelige, noe som også gjør det mulig for utenlandske aktører å påvirke velgere.

I utgangspunktet kan sosiale medier bidra til å styrke kommunikasjon og den offentlige samtalen. Etter Obamas valgkamp i 2008 snakket mange om sosiale medier som et demokratiserende verktøy for å kommunisere direkte med velgerne og som en infrastruktur for at flere kan delta i politisk arbeid.

Ny innsikt fra de siste årene viser imidlertid at de samme verktøyene kan brukes til å manipulere velgere i det skjulte, og spre falske nyheter og villedende informasjon.

Valgkampteknologi

I dag kan valgkamp organiseres i sin helhet på nett. Nettbaserte verktøy er lett tilgjengelige, krever lite forhåndskunnskap og gir mulighet for å spare arbeid gjennom automatisering.

SAMMENDRAG

» Politisk reklame er forbudt på TV, men tillatt på nett og i sosiale medier.

» Valgkamp har gått fra å rette seg mot brede målgrupper, til datastyrt påvirkning av hver enkelt via sosiale medier.

» De siste årene har også utenforstående aktører tatt i bruk disse verktøyene for å påvirke velgere ved å spre desinformasjon og falske nyheter.

» Flere land mobiliserer nå for å hindre at innbyggerne blir manipulert i forkant av valg.

På sosiale medier kan partiene kjøpe persontilpasset reklame, overvåke responsen på innleggene, teste og gjøre stadige forbedringer.

Fra målgruppe til individ

Metoder og teknologi utviklet i den digitale annonseindustrien, brukes nå i stor skala innen politisk markedsføring. Når vi bruker tjenester på nett, er det en rekke aktører som følger med på aktivitetene våre. Mengden data som samles inn fører til en svært

detaljert kartlegging av livene våre. Dataene analyseres for å kunne tilby oss persontilpassede tjenester og produkter.

Politisk reklame på sosiale medier har blitt svært vanlig, og før Brexit-avstemningen i 2016 publiserte Vote leave-kampanjen rundt en milliard målrettede annonser, hovedsakelig på Facebook.

Innlegg kan målrettes basert på informasjon om kjønn, alder og bosted, men også kategorier som sivilstatus, helsetilstand eller arbeidsgiver.

I tillegg kan Facebook lage kategorier basert på utledet informasjon, for eksempel hvilken politisk tilhørighet de tror du har, eller etnisk bakgrunn, uten av dette er informasjon du selv har oppgitt.

Teste og forbedre

Med markedsføringsverktøyene kan man følge responsen på annonsene i sanntid. Dette gjør det mulig å teste ulike budskap til ulike grupper, og deretter spre videre de annonsene som treffer best.

I den amerikanske valgkampen i 2016 publiserte Trump-kampanjen 5,9 millioner ulike annonser på Facebook. De testet ulike varianter og spredde de annonsene som ble mye likt og delt, eller som førte til donasjoner. Til sammenlikning publiserte Clinton-kampanjen 66 000 ulike annonser.

En «Office-pakke» for valg

Nationbuilder er en komplett pakke av verktøy for å gjennomføre en digital valgkamp, inkludert: koordinering av arbeidet, administrasjon av nettsider og sosiale medier, finansiering og utsending av målrettet markedsføring.

Programvaren brukes over hele verden, og har rundt 200 kunder bare i Storbritannia. Partier og organisasjoner får dermed tilgang til både data og kraftige verktøy uten å være eksperter på området.

Automatiserte kontoer

Automatiserte kontoer på sosiale medier, også kalt bot-er, gjør det mulig å publisere svært mange innlegg på kort tid. I forbindelse med valg har man særlig sett bot-er som sprer villende informasjon og falske nyheter.

Første halvår i 2018 slettet Twitter over 200 millioner kontoer, mistenkt for spam eller ulovlig automatisering.

Frem mot det svenske valget i 2018 var det en kraftig økning i bot-er på Twitter som delte politisk innhold. Det meste av dette innholdet kom fra nettsteder som publiserte falske nyheter.

FORSLAG TIL SPILLEREGLER

I både Canada og Storbritannia diskuteres nye spilleregler for digital valgkamp. Teknologirådet har foreslått at norske partier vurderer følgende punkter:

Åpenhet og merking

Partiene må være åpne om hvordan de bruker data, og merke annonser på nett og i sosiale medier. Merkingen kan inneholde informasjon om hvor mye penger som har blitt brukt, og hvem som er målgruppen. Politiske reklamer bør lagres i et arkiv.

Handlingsregel for data og penger

Partiene bør i fellesskap avklare hvilke typer data det er greit å bruke til å målrette politisk reklame, og om det skal innføres en grense for hvor mye penger som kan brukes på digital markedsføring.

Valgkamprevisjon

Partiregnskapene må spesifisere hvor mye penger som brukes på digital markedsføring og hvordan de er brukt. Det bør innføres datarevisjon for å sjekke at data kun brukes til det formålet de er innhentet for.

Fra valgkamp til manipulering

I Norge er politisk markedsføring regulert. Politisk reklame på TV er forbudt, begrunnet i at fjernsyn har stor gjennomslagskraft, kan gi et skjevt bilde av kompliserte spørsmål og kan favorisere ressurssterke partier.

På nett er det derimot fritt frem for politisk reklame. Nyere studier viser at annonsering på sosiale medier har stor effekt på velgere, og partiene flytter stadig større andel av markedsføringsbudsjettene sine over på digitale flater.

Global industri

I 2017 ble det avslørt at selskapet Cambridge Analytica hadde fått tilgang til data om 87 millioner Facebook-brukere. Cambridge Analytica bistod Donald Trump i hans valgkamp, og markedsførte seg med psykologisk profilering av brukerne.

Det er over 250 selskaper som spesialiserer seg i bruken av persondata i valgkamp. Selv om det er eksemplene fra USA og Storbritannia som har fått mest oppmerksomhet, viser eksempler fra Frankrike, Brasil, Kenya og India hvordan selskaper som Cambridge Analytica jobber over hele verden.

I etterkant av Brexit-avstemningen er det satt i gang undersøkelser av hvordan persondata blir brukt for å påvirke velgere. Britiske Information Commissioner har allerede gitt flere bøter for ulovlig håndtering og bruk av persondata.

Et selskap som gir råd til gravide og småbarnsforeldre hadde for eksempel solgt data om en million av sine brukere til en datamegler. Disse dataene ble senere brukt av Labour for å persontilpasse politisk reklame til nybakte mødre før valget i 2017.

Fri meningsdanning?

Nyhetsstrømmen på sosiale medier styres av algoritmer. Vi får ser det algoritmen tror vil engasjere oss: temaer vi er interessert i, holdninger vi er enig i eller innlegg fra venner vi kommuniserer mye med. Innlegg som skaper engasjement via delinger, kommentarer og «likes» spres hurtig videre.

Slik kan det skapes filterbobler, som gjør at vi sjelden utsettes for holdninger som utfordrer egne synspunkt. Dette kan forsterke eksisterende holdninger, og skape større avstand til andre grupper. Når man stadig får bekreftet sine egne meninger, er det lett å tro at disse holdningene er vanligere og mer utbredt enn de faktisk er – såkalte ekkokamre.

Målrettet markedsføring kan også bidra til dette. «Dark ads» er annonser som kun vises til målgruppen. Det vil si at partier kan velge hvilke budskap de vil fremme til hvilke personer, uten at andre har innsyn i hva som skjer. Ulike personer og grupper kan dermed få ulikt inntrykk av et partis budskap.

Desinformasjon

De digitale verktøyene for markedsføring er globale og lett tilgjengelige. Det åpner for at utenlandske aktører kan bruke samme metoder og teknologi som partiene for å påvirke velgere, uten å gi seg til kjenne. Selv om det er vanskelig å anslå den konkrete effekten, viser flere granskninger at omfanget av påvirkningskampanjer er betydelig.

Ekstern påvirkning

Flere rapporter har slått fast at det russiske Internet Research Agency (IRA) brukte sosiale medier til å påvirke amerikanske velgerne. Fra 2013 og frem til i dag har IRA nådd millioner av amerikanere via Facebook, Instagram og Twitter. IRA ble drevet som et profesjonelt digitalt reklamebyrå, med egne logoer, personaer og typografi.

Selv om IRAs aktiviteter har blitt avslørt, har ikke aktiviteten stoppet. Særlig på Instagram har russiske kontoer økt aktiviteten etter valget i 2016, og forsøker å skape engasjement rundt politikkområder som nasjonal sikkerhet, og temaer som er særlig viktige for unge velgere.

I India har desinformasjon spredt via WhatsApp ført til flere voldelige hendelser. I motsetning til i USA, spres ikke desinformasjon fra utenlandske aktører, men fra nasjonale miljøer. Fordi WhatsApp er kryptert, kan ikke brukerkontoer og grupper overvåkes og slettes på samme måte som på Facebook og Twitter, og det er vanskelig å finne ut hvem som står bak.

Det er trolig IRAs aktiviteter i USA som er det mest kjente eksemplet, men det er identifisert påvirkningskampanjer i mange land. Det er særlig tre strategier som går igjen:

Passivisering

Russiske IRA fokuserte mye av sin innsats på å påvirke afroamerikanere til å ikke bruke stemmeretten sin. Innleggene oppfordret til boikott av valget, og oppga uriktig informasjon om prosedyrene for å registrere seg som velger.

Skape konfrontasjoner og polarisering

I forkant av det indiske valget i 2018 ble det delt store mengder bilder av falske avisoverskrifter i grupper på WhatsApp, som prøvde å skape polarisering mellom hinduer og muslimer. Særlig ble Kongresspartiet forsøkt fremstilt som anti-hindu.

I mai 2016 organiserte russiske IRA en demonstrasjon og samtidig en motdemonstrasjon om samme tema, via Facebook-gruppene «Heart of Texas» og «United Muslims of America».

Spredning av falske nyheter

Før det svenske valget i 2018 ble det opprettet Twitter bot-er som delte falske nyheter. Det var stor aktivitet, noe som førte til at innholdet fikk stor spredning, og det ble likt og delt videre av vanlige brukere. En kartlegging viser at svenske Twitter-brukere er i Europa-toppen når det gjelder deling av desinformasjon.

Tiltak mot manipulering

Etter de siste års avsløringer har det blitt satt i gang ulike tiltak for å unngå manipulering av velgere.

Selvregulering for internettgigantene

Etter oppfordring fra EU-kommisjonen har de største internettselskapene og aktører fra annonsørmarkedet skrevet en "Code of practice on disinformation". Målet er å skape større åpenhet om politiske annonser (bl.a. avsender og finansiering), forhindre misbruk av boter og prioritere troverdig informasjon i brukernes nyhetsstrøm.

Twitter, Facebook og Google har alle begynt å merke politisk markedsføring, slik at brukerne lettere skal kunne skille mellom reklame og annet innhold.

Både Twitter og Facebook har opprettet arkiv for politiske annonser. For å hindre utenlandsk påvirkning har Facebook i tillegg satt restriksjoner på kjøp av politisk reklame, slik at kun nasjonale aktører kan annonsere.

Dette har imidlertid skapt utfordringer i EU, da mange institusjoner driver valgkamp på tvers av landegrenser i forkant av EU-valget. I praksis kan EU-kommisjonen kun fremme informasjon om valget til innbyggere i Belgia, siden kommisjonen ligger i Brussel.

Selskapene jobber også for å bedre kunne oppdage og slette automatiserte kontoer som sprer ulovlig innhold. Fra januar til mars 2019 identifiserte Twitter rundt 40 millioner kontoer som spam eller ulovlige automatiserte kontoer. Bare i mars 2019 slettet Google en million Youtube-kanaler for brudd på reglene for spam, villedende innhold og svindel.

Lovbestemt ansvar

Flere land, blant annet Tyskland, Frankrike og Italia, har tatt juridiske skritt for å tydeliggjøre sosiale medie-selskapenes ansvar for innholdet som publiseres og deles på deres plattformer. Lovendringer stiller blant annet krav til responstid for fjerning av ulovlig innhold og gjør det mulig å bøtelegge aktører som ikke følger opp. I Tyskland skal ulovlig innhold fjernes innen 24 timer. Kritikk har blant annet handlet om at også lovlig innhold, som for eksempel satire, fjernes i prosessen, og at ytringsfriheten dermed kan innskrenkes.

Cyberforsvar for demokratiet

EU har opprettet et varslingssystem slik at medlemslandene raskt skal kunne dele informasjon hvis de oppdager forsøk på valgmanipulering, og samles om en felles respons.

I Sverige utredes det om en ny myndighet skal ha ansvar for å utvikle landets psykologiske forsvar. Australia og flere andre land har opprettet egne enheter i sine forsvar som skal beskytte landets velgere mot påvirkning utenfra.

Informasjon og bevisstgjøring

Flere satser på å bevisstgjøre velgerne:

- Faktasjekkere, som faktisk.no, vurderer nyhetssaker og utspill, og kan bidra til å avsløre desinformasjon og falske nyheter.
- Troverdighetsverktøy, som Le Décodex og NewsGuard, undersøker nettaviser og andre kilder. De ser om nettstedene tidligere har publisert desinformasjon, og gir en score på om siden er troverdig eller ikke.
- Myndigheten för samhällsskydd och beredskap (MSB) i Sverige har skrevet en håndbok om hvordan desinformasjon kan identifiseres og møtes. Håndboken er oversatt og tatt i bruk i flere land.

Forfattere: Tore Tennøe / Marianne Barland

Kontakt: post@teknologirådet / www.teknologiradet.no

Teknologirådet gir råd til Stortinget og regjeringen om ny teknologi