

FOKUS: CYBERSPACE

Sosiale medier, samfunns- politisk deltagelse og kontroll

KARI STEEN-JOHNSEN

Ph.d. forsker II, Institutt for samfunnsforskning
kari.steen-johnsen@samfunnsforskning.no

BERNARD ENJOLRAS

Ph.d., forskningsleder, Institutt for samfunnsforskning
bernard.enjolras@samfunnsforskning.no

DAG WOLLEBÆK

Ph.d., forsker II, Institutt for samfunnsforskning
dag.wollebak@samfunnsforskning.no



Utviklingen av Internett og av sosiale medier har sammensatte samfunnsmessige konsekvenser og reiser nye spørsmål når det gjelder sikkerhet og kontroll, både virtuelt og i det virkelige liv. På den ene siden gjør sosiale medier det mulig for flere å delta i det offentlige ordskiftet og uttrykke sine meninger om politikk og samfunn. Sosiale medier kan bidra til rask og kraftfull mobilisering av en befolkning, og dermed til nye muligheter for å opponere mot et lands myndigheter. På den andre siden kan sosiale medier sette radikale grupper i stand til å organisere seg og utveksle synspunkter i langt sterkere grad enn tidligere. I forbindelse med terrorangrepet 22. juli 2011 spilte terroristens Internett-aktivitet en viktig rolle for hvordan angrepet ble forstått i Norge og i verden for øvrig.

I denne artikkelen tar vi utgangspunkt i at fremveksten av sosiale medier skaper nye dilemmaer der samfunnets interesser kan stå i motsetning til individenes sivile rettigheter, særlig rettigheter knyttet til personvern og ytringsfrihet. Nettopp fordi sosiale medier skaper nye muligheter for sivil deltagelse, mobilisering og organisering både *innenfor* og *som motsetning til* den rådende samfunnsorden, reiser utviklingen spørsmål om balansen mellom statlig kontroll og individuell frihet.

Sett fra statens side vil dilemmaene knyttet til sosiale medier arte seg forskjellig, avhengig av hva slags forfatning staten hviler på og hvilken kontroll

en stat ønsker å utøve med borgernes sivile og politiske aktiviteter. I denne artikkelen kommer vi til å konsentrere oss om samfunn med en demokratisk forfatning, med Norge som case. Vi vil først redegjøre for hvordan digitale nettverk endrer betingelsene for sivil deltagelse, mobilisering og organisering generelt. Deretter drøfter vi de spenningene dette reiser mellom sikkerhetsbehov og sivile rettigheter for både medborgere og myndigheter. Til slutt drøfter vi synet på forholdet mellom sikkerhet og sivile rettigheter i den norske befolkningen etter 22. juli, basert på spørreundersøkelser som ble gjennomført like før og rett etter terrorhandlingene, ni måneder etter, samt etter at Gjærv-kommisjonen hadde presentert sin rapport. Selv om tiden etter 22. juli var en svært spesiell periode i norsk historie, var det også en periode der spenningen mellom sikkerhet og sivile rettigheter ble særlig tydelig.

Sosiale medier og potensialet for samfunnspolitisk deltagelse

Sosiale medier (som Facebook, Twitter eller YouTube) er en spesiell kategori av digitale nettverk. En viktig grunn til at sosiale medier har blitt oppfattet som revolusjonerende, er kombinasjonen av ulike interaktive og nettverksbaserte kommunikasjonsmuligheter innenfor en predefinert og brukervennlig digital arkitektur. En måte å oppfatte sosiale medier på er å forstå dem som et sett av innebygde handlingsmuligheter – det vanskelig oversettbare begrepet *affordances* (boyd & Ellison 2007). Det er disse innebygde handlingsmulighetene som gjør det mulig å bruke sosiale medier til å organisere seg og drive politisk aktivitet, samt å spre informasjon til andre brukere. Sosiale medier tilbyr dermed nye digitaliserte muligheter for å produsere, registrere og spre informasjon som ikke var til stede i Internetts første fase (web 1.0) (O'Reilly 2007).

Et grunnleggende kjennetegn ved sosiale medier er at de kobler sammen individer innenfor digitale nettverk og danner broer mellom det lokale og det globale. I et digitalisert nettverkssamfunn har verden blitt en «*liten verden*» (Barabási 2002). Det vil si at hver nettbruker med få tastetrykk kan nå andre brukere. Når individer er koblet sammen i et nettverk, vil de kunne påvirke hverandres atferd og beslutninger. *Informasjonskaskader* er en sosial prosess som inntreffer når individer som tar beslutninger er i stand til å observere andres beslutninger for så å dra slutninger på grunnlag av disse. Sosiale mediers nettverksbaserte «*liten-verden*»-struktur er godt egnet til å skape informasjonskaskader fordi brukere lett kan observere hva deres forbindelser gjør, trekke slutninger og ta avgjørelser på basis av disse observasjonene som så sprer seg videre gjennom nettverkene deres. Sosiale mediers innebygde handlingsmuligheter, og nettverksfunksjon har ledet mange, både forskere og andre, til en antagelse om at sosiale

medier vil gi borgere nye muligheter til å ytre seg og å mobilisere til politisk handling i det offentlige rom (Hirzalla et al. 2011; Shirky 2008; Dahlgren 2005). Den arabiske våren tydeliggjorde at Facebook og Twitter var effektive redskaper for å nå og samle store menneskemengder raskt, spesielt i fravær av en fri presse (Khondker 2011). Applikasjoner slik som YouTube og Bambuser¹ har også vist seg viktige i forhold til å dokumentere overgrep begått av myndigheter og å formidle dette til et globalt publikum.

Også i etablerte demokratier som det norske kan sosiale medier spille en rolle i å mobilisere til samfunnsdeltagelse. I studier vi har gjennomført av bruk av sosiale medier og ulike former for samfunnsengasjement,² viser det seg at Facebook er blitt en like viktig kilde til informasjon om demonstrasjoner som massemediene (Enjolras, Steen-Johnsen & Wollebæk 2012). Dette gjelder for store deler av befolkningen, opp til 54 år. Vi finner også at Facebook ser ut til å tilby en alternativ struktur til det etablerte organisasjonssamfunnets strukturer når det gjelder å nå frem med informasjon om demonstrasjoner. Et spesielt interessant trekk ved mobilisering gjennom Facebook er at de som nås er yngre, og de har lavere inntekt enn de som mobiliseres gjennom personlig kontakt eller gjennom massemedier. Vi ser dermed tegn til at sosiale medier kan bidra til å utjevne sosioøkonomisk betingede forskjeller i deltagelse (Enjolras, Karlsson, Steen-Johnsen & Wollebæk 2013).

Men samtidig som den sosiale dimensjonen ved digitale nettverk skaper nye muligheter for medborgernes sosiale og politiske engasjement, åpnes også nye muligheter for myndighetene til å overvåke individer og samfunnet. Det oppstår dermed en potensiell spenning mellom det som oppfattes som samfunnets sikkerhetsbehov og muligheten for å utøve kontroll på den ene siden og beskyttelsen av individenes sivile rettigheter på den andre. Hva som er samfunnets sikkerhetsbehov og hvilke tiltak som er legitime, vil til enhver tid være gjenstand for politisk diskusjon. Avhengig av hva som defineres som legitime sikkerhetsbehov og virkemidler, vil det oppstå spenninger i forhold til rettigheter til personvern og ytringsfrihet. Nedenfor skal vi utdype denne spenningen nærmere.

Spenningen mellom sikkerhetsbehov og sivile rettigheter

Fremveksten av sosiale medier fører med seg en forvitring av skillet mellom offentlig og privat informasjon og kommunikasjon. Dette reiser nye

-
1. Bambuser er en mobilapplikasjon som gjør det mulig å streamere filmopptak live til et nettsted, og dermed for eksempel dokumentere overgrep til et globalt publikum mens det skjer. Se bambuser.com.
 2. Dette er del av den samme undersøkelsen som vi redegjør for i den empiriske delen av denne artikkelen.

spørsmål knyttet til personvern. På tross av at personvern – «retten til å være for seg selv» – er et grunnleggende trekk ved det å være et menneske, er både definisjon og forståelse av begrepet et omstridt tema både innenfor filosofi (Nissenbaum 2010) og psykologi (Joinson & Paine 2007). Når det gjelder spørsmålet om hvordan digitale nettverk påvirker personvern, mener vi at det er informasjonsdimensjonen og den ekspressive dimensjonen som er de mest relevante. Informasjonsdimensjonen ved personvernet gjelder individets rett til å bestemme og kontrollere hvilken informasjon som skal formidles til hvem. Den ekspressive dimensjonen dreier seg om retten til å beskytte en sfære hvor individet kan uttrykke seg uten å være underkastet myndighetenes eller andres sosialt press og kontroll.

Digitalisering har ført til teknologisk utvikling ikke bare når det gjelder kommunikasjon, som beskrevet ovenfor, men også når det gjelder verktøy som kan brukes for å fange opp og digitalisere informasjon (digitalt fotografi, lydopptak) samt digitale nettverksoverføringsmekanismer som gjør det mulig å fange opp og overvåke all kommunikasjon. Kombinert med veksten i datalagringskapasitet og databeregningskraft, fører disse teknologiske verktøyene til utvidede muligheter for sporing og overvåkning av individenes handlinger og kommunikasjon. Dette blir spesielt utfordrende for personvernet når vi kobler det til demokratiseringen som har skjedd av formidling, publisering, overføring og offentliggjøring av informasjon. Mens disse mulighetene tradisjonelt var avgrenset til massemediene, har digitaliseringen ført til en allmenngjøring av disse tekniske mulighetene. Samtidig er mange offentlige arkiver tilgjengelige for alle gjennom digitale nettverk. Kombinasjonen av lett tilgjengelig datakraft, brukernes mangel på kunnskap om effekter av deres handlinger på digitale nettverk og nye sosiale praksiser og normer når det gjelder avsløring av privat informasjon, kan true personvernet.

Ytringsfrihet og sensur

Digitalisering og sosiale medier har bidratt til å utvide mulighetene for fri ytring av ideer og politiske meninger betraktelig. Samtidig gir digital teknologi nye muligheter for informasjonskontroll, filtrering og sensur. Sosiale medier og digitale nettverk utfordrer dermed balansen mellom individuelle rettigheter og offentlige regler som garanterer og regulerer ytringsfrihet. De har gitt mer makt til borgere mange steder og har bidratt til autoritære regimers fall, som i den arabiske våren, men bidrar også til å true eller begrense ytringsfriheten (Morozov 2011; MacKinnon 2012).

Det kinesiske regimets håndtering av og kontroll med Internett gir et eksempel på hvilke muligheter for myndighetskontroll som eksisterer. Innhenting av data fra online samtaler mellom borgerne benyttes for å

identifisere sosiale og politiske problemer med den hensikt å forebygge og kontrollere sosial og politisk uro. I tillegg praktiserer kinesiske myndigheter en sofistikert form for Internett-sensur. For det første er det kinesiske Internett beskyttet av den «store brannmuren» som blokkerer tusenvis av uønskede websider. Dette er mulig fordi det kinesiske Internett er koblet til det globale Internett gjennom et begrenset antall «dører», noe som gjør innholdsfiltrering enkelt. For det andre tvinges Internett-leverandørene til å redigere og slette alle former for uønsket innhold som er publisert på deres plattformer. Internett-selskaper utøver dermed sensur på vegne av staten, samtidig som 500 millioner kinesere har tilgang til en «desinfisert» versjon av Internett.

Det kinesiske eksemplet er langt fra enestående. I Tyrkia blokkerte myndighetene i 2011 tilgangen til ca. 120 000 nettsider som inneholder ett av 138 ord de definerte som «støtende», blant annet «naked», «gay», med ambisjonen om å skape et *halal*-Internett.³ Mange ser dette som et forsøk på å venne befolkningen til sensur av nettet som senere vil ramme politisk innhold. Også i vestlige land er ytringsfriheten i økende grad truet. Samtidig som Tyrkia vedtok sitt *halal*-Internett, arbeidet David Cameron for å blokkere Facebook og Twitter, fordi de ble brukt til å organisere opptøyene i London.⁴

En mer konstant trussel er myndighetenes implementering av overvåkningssystemer på Internett, rettferdiggjort ut fra sikkerhetshensyn og behovet for å bekjempe terrorismen. Den amerikanske kryptologiske etterretningsorganisasjonen National Security Agency (NSA) opererer for eksempel et internasjonalt spionavlyttingssystem kalt «Echelon», som kan motta tre milliarder elektroniske transmisjoner daglig og som filtrerer informasjon som inneholder suspekte ord. Det amerikanske FBI bruker en programvare kalt «Carnivore» som skanner de digitale nettverkene og muliggjør avlytting av den enkeltes kommunikasjon, brukeridentifisering, samt lokalisering og identifisering av alle kontaktene til en konkret bruker.

Et annet trekk med relevans for ytringsfrihetsspørsmålet dreier seg om privatisering av det offentlige rom. Private tjenesteleverandører som Google, Facebook, Twitter, Apple osv. har mulighet til å regulere og sensurere det som publiseres på deres plattform gjennom bruksregler og policy. Disse har til hensikt å beskytte brukere fra mobbing, men kan være strengere enn lovene som regulerer ytringsfriheten i et demokratisk samfunn. I dette ligger at de utøver justis uten noen former for rettssikkerhet eller mulighet til appell. Et eksempel er at en Facebook-konto automatisk sten-

3. http://news.monstersandcritics.com/europe/news/article_1635954.php/Turkey-moves-to-ban-domain-names-containing-indecent-language.

4. <http://www.computerworlduk.com/news/public-sector/3296574/cameron-considers-blocking-bbm-facebook-and-twitter-for-alleged-rioters/>.

ges dersom nok brukere går sammen om å rapportere om at innholdet bryter med retningslinjene. Slik masserapportering er blitt brukt for å fjerne uttalelser fra meningsmotstandere (Tjomlid 2012).

Utviklingen medfører en risiko for at sosiale medieplattformer utvikler en form for kontroll som er i strid med demokratiske grunnprinsipper og menneskelige rettigheter. Ifølge Morozov (2011) bidrar den digitale utviklingen til å mektiggjøre ikke bare demokratiske aktivister, men også demagoger, diktatorer og terrorister. Den samme tvetydigheten ser ut til å prege utviklingen av private sosiale medieplattformer: sosiale medier kan ha en demokratiserende effekt, men innebærer en konsentrasjon av makt og kontrollmuligheter i hendene på få private aktører og interesser.

Sikkerhet og aksept for Internett-overvåkning i Norge etter 22. juli

Hvordan stiller så den norske befolkningen seg til kontroll og overvåkning av Internett? Med 22. juli-hendelsene opplevde man for første gang et større terrorangrep på norsk jord. I denne sammenhengen ble terroristens Internett-aktivitet og dens betydning for hendelsene debattert i offentligheten. Internett-aktiviteten berørte ulike sider ved terrorhandlingene, blant annet innkjøp av ingredienser til bomben og publiseringen av et manifest som skulle grunnngi handlingene og anspre likesinnede i andre land. Dette var et eksempel på Morozovs (2011) poeng om at Internett ikke bare virker demokratiserende, men også kan fungere som verktøy for terrorisme.

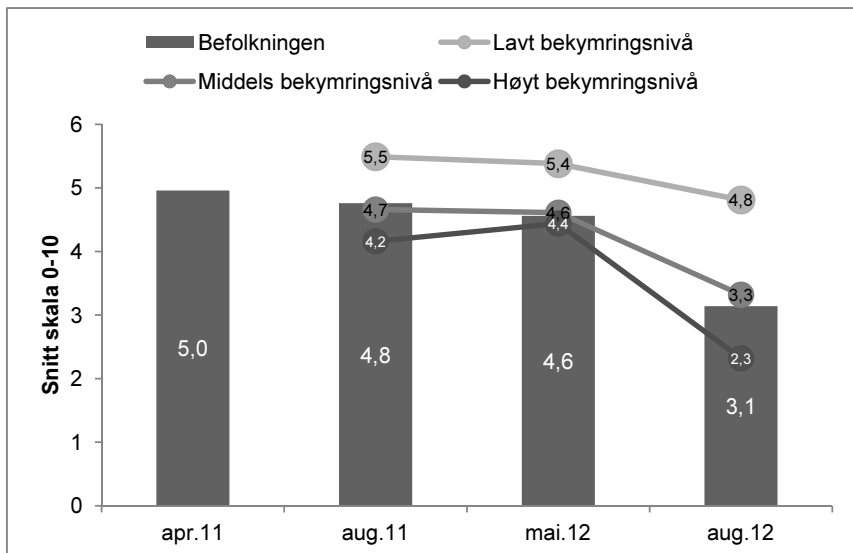
I mars og april 2011 gjennomførte vi en befolkningsundersøkelse om bruk av sosiale medier, tillit og sivilt og politisk engasjement i Norge. Deler av den samme undersøkelsen ble gjentatt i begynnelsen av august 2011. Undersøkelsen ble gjennomført på nytt i april/mai 2012 og i august/september 2012, etter at 22. juli-kommisjonen hadde lagt frem sin rapport. Vårt datamateriale gir oss dermed mulighet til å sammenlikne befolkningens holdninger og atferd på fire ulike tidspunkter: før terrorhendelsene (for enkelhets skyld referert til som april 2011), etter terrorhendelsene (august 2011), åtte måneder etter terrorhendelsene (mai 2012) og 13 måneder etter terrorhendelsene og to uker etter offentliggjøring av 22. juli-kommisjonens konklusjoner (august 2012).⁵

5. For hvert av disse tidspunktene har vi et datamateriale som består av to deler. Den første delen er et representativt utvalg Internett-brukere (ca. 1000 individer). Dette er representativt for den delen av befolkningen over 16 år som bruker Internett i større eller mindre grad, det vil si *Internett-befolkningen*. Den andre delen er et panel av brukere av sosiale medier, der de samme individene har blitt intervjuet på alle fire tidspunkter. 2128 personer er intervjuet på minst tre av tidspunktene, mens 641 er intervjuet alle fire gangene. For mer informasjon om undersøkelsen, se rapporten «Har rosetoget gått?» (Wollebæk mfl. 2012).

Norge har over tid skilt seg ut i internasjonal sammenligning med høy grad av tillit til medmennesker og tillit til myndighetene (Catterberg & Moreno 2005; Wollebæk & Segard 2011). Samtidig har nordmenn gitt forholdsvis sterk støtte til kontroll og overvåking som ledd i forebygging mot terror. I en studie fra 2009 viste Rykkja, Lægred og Fimreite at det var et komplekst forhold mellom ulike former for tillit og støtte til myndighetskontroll. De konkluderte med at den relativt høye støtten til myndighetskontroll i Norge måtte forklares med kombinasjonen av opplevd lav terrortrussel, fravær av tidligere erfaring med terrorisme i Norge og høy tillit til myndighetene (Rykkja mfl. 2011).

Ut fra denne forklaringsmodellen var det rimelig å tenke seg at 22. juli-terroren ville skape endringer i nordmenns forhold til myndighetskontroll; ved å endre befolkningens vurderinger av trusselnivået og ved å skape endringer i tillit til myndighetene. Figur 1 viser endringer i synet på et spørsmål vi stilte i alle fire undersøkelsene, det vil si både før og etter terrorangrepene, nemlig i hvor stor grad man mener myndighetene bør ha mulighet til å overvåke kommunikasjon på Internett for å forebygge alvorlig kriminalitet. Dette standpunktet ble satt opp mot alternativet «Internett bør være mest mulig fritt for overvåking fra myndighetene».

Figur 1: Syn på overvåking av Internett. Gjennomsnitt på skala 0–10 og prosent



NOTE: Skala: «Det er nødvendig for myndighetene å overvåke kommunikasjon på Internett for å forebygge alvorlig kriminalitet» (0) vs. «Internett bør være mest mulig fritt for overvåking fra myndighetene» (10). Estimatene for befolkningen som helhet er basert på befolkningsutvalget. Estimatene for personer med ulik grad av bekymring er basert på panelet og befolkningsutvalget kombinert for å få store nok undergrupper.

Figuren viser et klart stemningsskifte i befolkningen etter 22. juli-kommisjonens rapport. Befolkningen så ut til å ville gi myndighetene betydelig større fullmakter i retning av mer overvåkning. Hele 72 prosent plasserte seg nærmere overvåkingsstandpunktet enn fritt Internett-standpunktet i august 2012, mens andelen var 49 prosent i mai. Dette stemningsskiftet var i stor grad drevet av at de som var bekymret for terror ønsket at myndighetene skulle stramme inn kontrollen. Personene vi klassifiserte med «høyt bekymringsnivå» beveget seg to hele punkt på skalaen fra 0–10, og plasserte seg i gjennomsnitt på 2.4.⁶ De som i liten grad var bekymret for terror, endret ikke syn på spørsmålet om overvåkning av Internett i samme grad. Resultatene viste også at når respondentene ble bedt om å veie behovet for kontroll mot individuelle rettigheter, beveget tyngdepunktet i august 2012 seg klart i retning av økt kontroll og overvåkning for å beskytte befolkningen mot terror.

Diskusjon og konklusjon

I denne artikkelen har vi pekt på noen spenninger mellom sivile rettigheter og kontroll i lys av digitalisering og fremveksten av sosiale medier. På den ene siden kan fremveksten av sosiale medier bidra til å gi økt tilgang for flere både til det offentlige ordskiftet og til å organisere seg og mobilisere til politisk handling. På den andre siden utfordrer sosiale medier sivile rettigheter knyttet til personvern og ytringsfrihet. Vi har pekt på at digitaliseringen gir økte muligheter til å samle informasjon om enkeltindivider og overvåke deres aktivitet. Disse mulighetene kan utnyttes både av statlige myndigheter og for kommersielle formål. Digitaliseringen gir også økte muligheter til å sensurere innhold på nett, noe både stater og kommersielle selskaper benytter seg av.

Spenningen mellom sivile rettigheter og kontroll med Internett reiser flere sett av problemstillinger for et demokratisk samfunn. Blant de viktigste er hvordan borgerne forholder seg til sine rettigheter og hvilke forventninger de retter mot sine myndigheter i forhold til å ivareta disse rettighetene. Basert på vår undersøkelse av forholdet til kontroll og overvåkning av Internett blant norske borgere etter 22. juli, kan det synes som om det finnes svake motkrefter til slik kontroll. Disse resultatene er i tråd med funn fra tidligere undersøkelser av holdninger i den norske opinionen (Rykkja

6. Svar på spørsmålene: Hvor bekymret er du for at Norge skal bli rammet av nye, store terrorangrep? Og: Hvor bekymret er du for at du selv og din familie skal bli rammet av nye, store terrorangrep? Med «høyt bekymringsnivå» mener vi her at de i gjennomsnitt sier de er «nokså bekymret» eller høyere på de to spørsmålene som er analysert. Dette utgjør 13 prosent av befolkningen på det siste målepunktet. De som er klassifisert med «lavt bekymringsnivå» har maksimalt svart «ikke særlig bekymret» på ett av de to spørsmålene. Dette er 19 prosent av befolkningen.

mfl. 2011), men funnene våre indikerer at tyngdepunktet i opinionen gikk ytterligere i retning av mer kontroll og overvåkning etter presentasjonen av 22. juli-kommisjonens rapport.

Hvordan skal vi forklare disse svake motkreftene til økt myndighetskontroll i et demokratisk samfunn som Norge? Vi finner to ulike mekanismer som hovedsakelig trekker i retning av økt myndighetskontroll. Den viktigste av disse er bekymringsmekanismen: 22. juli-kommisjonens rapport førte til et høyere bekymringsnivå enn det ellers ville vært, noe som skapte økt aksept for kontroll og overvåkning. Den andre mekanismen er knyttet til statsvennligheten og den høye systemtilliten i det norske samfunnet. Denne har to motstridende effekter. På den ene siden demper den frykt, og dermed støtte til kontroll og overvåkning, fordi den styrker troen på myndighetenes evne til å beskytte. Sammen med den høye generaliserte tilliten – tiltroen til at andre mennesker stort sett vil deg vel – har denne tilliten bidratt til at fryktnivået fortsatt tross alt er lavt i Norge i sammenlikning med andre samfunn som har opplevd liknende hendelser. På den annen side gjorde den høye systemtilliten at mange i mindre grad så problematiske sider ved statlig kontroll og overvåkning. De som hadde høy tillit til myndighetene, hadde også høy tillit til at de kunne treffe de nødvendige tiltakene for å beskytte mot terror. Dette trekker i retning av å gi myndighetene utvidede fullmakter til å utøve mer kontroll.

Studien av den norske befolkningens holdninger til kontroll av Internett og mer generelt til kontroll og overvåkning etter 22. juli understreker at disse holdningene henger nær sammen med et kompleks av andre faktorer, slik som den mellommenneskelige tilliten som finnes i et samfunn, tillit til myndighetene og opplevd fare for nye terrorangrep. Sammenhengene blir enda mer komplekse når vi legger til at det ikke bare er staten som utøver kontroll på Internett, men også kommersielle selskaper. Et viktig spørsmål dreier seg om reguleringen av kommersielle selskapers makt, og hvordan borgerne som konsumenter og brukere av tjenester agerer. Heller ikke på dette feltet synes borgerne å kjempe for sine sivile rettigheter. Det er illustrerende at samtidig som tre av fire i vår undersøkelse har en Facebook-konto, er det bare en av ni som svarer at de har «stor» eller «svært stor» tillit til firmaet Facebook. 42 prosent har liten eller ingen tillit. For Googles del har 18 prosent stor tillit, mens 30 prosent har liten eller ingen tillit.⁷

Det er et paradoks at de fleste av oss frivillig legger igjen store mengder informasjon hos mektige institusjoner vi ikke kjenner oss særlig sikre på

7. De øvrige svarer «verken eller» – 46 prosent for Facebook og 52 prosent for Google. Dette er et spørsmål en stor andel ikke har klare meninger om. Ungdom har større tillit til både Facebook og Google: Blant de under 25 har 19 prosent tillit til førstnevnte og 29 prosent til sistnevnte (mot 10 og 16 prosent av de over 25).

vil forvalte den på en ansvarlig måte. Det er også interessant at motkref-
tene til statlig overvåkning av Internett er såpass svake i den norske opini-
onen. Vi tror en viktig grunn til dette er at kompleksiteten som kjenneteg-
ner digital kommunikasjon (både den fysiske infrastrukturen og måten
den fungerer på) er lite gjennomsiiktig for sluttbrukeren. De fleste mang-
ler kunnskap for å kunne gjøre informerte valg. Samtidig mangler Inter-
nett en effektiv lovgivning (på internasjonalt nivå) som kan beskytte bru-
kerens rettigheter. Cyberspace er i stor grad et uregulert rom rettslig sett.
Dette rommet åpner for medborgernes sosiale og politiske handlinger,
men også for terrorister, autoritære regjeringer og sikkerhetsmyndigheter.

Litteratur

- Barabási, A. L. (2002) *Linked*. London: Penguin Books.
- boyd, D. & K. Crawford (2011) Six provocations for big data. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*. Oxford: Oxford Internet Institute.
- boyd, D. & N. B. Ellison (2007) Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13 (1): 210–230.
- Brandtzæg, P. & M. Lüders (2009) Privat 2.0: Person- og forbrukervern i den nye medievirkeligheten. SINTEF-Rapport.
- Catterberg, G. & A. Moreno (2005) The individual bases of political trust: Trends in new and established democracies. *International Journal of Public Opinion Research*, 18 (1): 31–48.
- Dahlgren, P. (2005) The Internet, public spheres, and political communication: Dispersion and deliberation. *Political Communication*, 22 (2): 147–162.
- Enjolras, B., K. Steen-Johnsen & D. Wollebæk (2012) Social media and mobilization to offline demonstrations: Transcending participatory divides? *New Media & Society, Online first*.
- Enjolras, B., R. Karlsen, K. Steen-Johnsen & D. Wollebæk (2013) *Liker – liker ikke. Sosiale medier og samfunnsengasjment*. Oslo: Cappelen Damm.
- Granovetter, M. (1973) The strength of weak ties. *American Journal of Sociology*, 78: 1360–1380.
- Hirzalla F, L. van Zoonen & J. de Ridder (2011) Internet Use and Political Participation: Reflections on the Mobilization/Normalization Controversy. *Information Society* 27 (1): 1–15.
- Joinson, A. N. & C. B. Paine (2007) Self-disclosure, privacy and the Internet. I A. N. Joinson, K. McKenna, T. Postmes & U. Reips (red.) *Oxford Handbook of Internet Psychology*. Oxford: Oxford University Press.
- Khondker, H. H. (2011) Role of the New Media in the Arab Spring. *Globalizations*, 8 (5): 675–679.
- MacKinnon, R. (2012) *Consent of the networked. The worldwide struggle for internet freedom*. New York: Basic Books.
- Morozov, E. (2011) *The net delusion: The dark side of internet freedom*. New York: Public Affairs.

- Nissenbaum, H. (2010) *Privacy in context. Technology, policy and the integrity of social life*. Stanford: Stanford University Press.
- O'Reilly, T. (2007) What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *Communications & Strategies*, 65 (1): 17–37.
- Rykkja, L., P. Læg Reid & A. L. Fimreite (2011) Attitudes towards anti-terror measures: The role of trust, political orientation and civil liberties support. *Critical Studies on Terrorism*, (4): 2.
- Shirky, C. (2008) *Here Comes Everybody. The Power of Organizing Without Organizations*. New York: Penguin Books.
- Sunstein, C. (2001) *Republic.Com*. Princeton/Oxford: Princeton University Press.
- Tjomlid, G. (2012) *Tjomlid.com*. Alternativbøllene slår til igjen: Blokkert fra Facebook. Tilgjengelig på <http://tjomlid.com/2012/12/10/alternativbollene-slar-til-igjen-blokkert-fra-facebook/>. Lesedato 29.01.2012.
- Wollebæk, D. & S. B. Seggaard (red.) (2011) *Sosial kapital i Norge*. Oslo: Cappelen Damm Akademisk.
- Wollebæk, D., B. Enjolras, K. Steen-Johnsen & G. Ødegård (2012) Ett år etter 22. juli. Har rosetoget gått? *Rapport fra Senter for forskning på sivilsamfunn og frivillig sektor* (Vol. 2012:005: 81). Oslo: Senter for forskning på sivilsamfunn og frivillig sektor.