



Bak den norske overvåkingsdebatten

Behind the Norwegian surveillance debate

Guro Flinterud

Forsker, Forskningsavdelingen, Politihøgskolen

guro.flinterud@phs.no

Jon Strype

Førsteamanuensis, Forskningsavdelingen, Politihøgskolen

jon.strype@phs.no

Heidi Mork Lomell

Professor, Institutt for kriminologi og retts sosiologi, Universitetet i Oslo

h.m.lomell@jus.uio.no

Sammendrag

Hvordan resonnerer deltakerne i overvåkingsdebatten over sitt ståsted, og er debatten så polarisert som den fremstår i avisspaltene? Vi har intervjuet personer som jobber med overvåking eller deltar i det offentlige ordskiftet om deres ståsted i debatten. Funnene både bekrefter og utfordrer polariseringen i det offentlige ordskiftet. Vi finner en grunnleggende forskjell i hva som anses som den største trusselen: myndighetenes overvåking eller kriminelle og terrorister? Med andre ord, er myndighetene en garantist for eller tvert imot en trussel mot befolkningens frihet og sikkerhet? Intervjuobjektene er enige om hva slags samfunn de vil ha, men ikke om hva som skal til for å oppnå et slikt samfunn, og hvilken rolle myndighetene spiller. Funnene viser hvordan en polarisert debatt utspiller seg i et relativt harmonisk og tillitsbasert samfunn.

Nøkkelord

Overvåking, Digitalisering, Debatt, q-metodologi

Abstract

How do participants in the surveillance debate reflect on their positions, and is the debate as polarized as it appears in the newspaper columns? We have interviewed people who work with surveillance or participate in public debate about their positions in the debate. Our findings both confirm and challenge the impression of polarization in public debate. We find a fundamental difference in what appears as the greatest threat: is it the authorities, or criminals and terrorists? In other words, are the authorities a guarantor for, or, on the contrary, a threat to the freedom and security of the people? There is consensus regarding what kind of society one wants, but not regarding what it takes to create such a society, and what role authorities play. Our findings show how a polarized debate plays out in a relatively harmonic and trust-based society.

Keywords

Surveillance, Digitalization, Debate, Q-methodology

Innledning

Det siste tiåret har det vært tre store saker som har aktualisert statens tilgang til overvåking i den norske samfunnsdebatten: implementeringen av EUs datalagringsdirektiv (EU-direktiv 2006), innføringen av dataavlesning som metode (Straffeprosessloven, 2016, § 216 o-p) og forslaget om å innføre tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, tidligere kjent som digitalt grenseforsvar, i forbindelse med ny lov om Etterretningstjenesten (Forsvarsdepartementet, 2020). Alle disse sakene dreide seg om å på ulike måter utvide myndighetenes overvåkingsmuligheter i det digitale rom. De kom som følge av terrorhendelser, men også som følge av en teknologisk utvikling som utvider mulighetene for overvåking langt forbi det som tidligere har vært mulig. Overvåkingsdebatten er som sådan ikke bare en debatt om grensene for hvor langt inn i personsfæren vi vil tillate myndighetene å gå, men også en debatt som søker å definere disse grensene på en tilsynelatende grenseløs digital arena.

Med utgangspunkt i media og offentlig debatt fremstår overvåkingsdebatten som svært polarisert (Flinterud, 2020). Selv innlegg som omhandler viktigheten av å balansere sikkerhet og personvern, faller gjerne tungt ned på den ene eller andre siden, og det er lite rom for reell tvil i det offentlige ordskiftet. Det kan se ut til at utsagn fra de to sidene av debatten—for eller mot økt overvåking—ikke egentlig debatterer den aktuelle metoden, men i stedet presenterer to vidt forskjellige beskrivelser av nåtiden, både når det gjelder problemdefinisjon og løsninger (Flinterud, 2020). I denne artikkelen søker vi å komme bak den polariserte overflaten, ved å vende oppmerksomheten mot de som jobber med tematikken i praksis eller deltar i det offentlige ordskiftet, og hvordan de oppfatter og artikulere dilemmaene rundt overvåking og digitalisering. Vi har intervjuet personer med bakgrunn fra politi og etterretning, politikk, IT, media og jus med fokus på hvordan de stiller seg til argumentene i overvåkingsdebatten. Intervjuene er del av et komparativt forskningsprosjekt med formål å utforske hvordan myndighetenes overvåking på nett reguleres, debatteres og forstås i Norge, Finland og Storbritannia.¹ Intervjuene er utformet etter q-metodologi (se for eksempel Watts & Stenner, 2012), en induktivt rettet kombinasjonsmetode [mixed method] som gir oss både kvantitative og kvalitative resultater å basere analysen på². Spørsmålet vi stiller i denne artikkelen er: Hvordan resonnerer interessentene over sitt ståsted i debatten, og i hvilken grad gjenfinner vi polariseringen fra det offentlige ordskiftet i intervjuene?

Overvåking som trussel eller beskyttelse?

Statens behov for å samle informasjon om innbyggerne har en lang historie, og overvåking er uløselig knyttet til moderne statsdannelse (Giddens, 1985; Rule, 1973). Dagens overvåkings-systemer har vokst frem med utviklingen av nasjonalstaten, og særlig med byråkratiseringen som fulgte industrialiseringen fra midten av 1800-tallet. Myndighetene har et grunnleggende – mange vil hevde umettelig – behov for å samle informasjon.

I Norge har debatter om myndighetenes overvåking vært knyttet til historiske skandaler. Et eksempel er deportasjonen av jødiske borgere under andre verdenskrig, muliggjort av navne- og adresselister fra det norske politiet og Nasjonal samlings statistiske kontor (Søbye,

1. <https://sites.dundee.ac.uk/eyes-online-project/>

2. Et dokumentasjonsnotat (Flinterud og Strype, 2020) med bakgrunnsinformasjon, et tidlig working paper fra studien, samt datafil fra den kvantitative analysen, er tilgjengelig på <https://phs.brage.unit.no/phs-xmlui/handle/11250/2600751>

1998). Lund-kommisjonens avsløring av myndighetenes inngående overvåking av norske kommunister i etterkrigstiden er et annet eksempel (Lund, 1996, se også Wyller, 1997). Til tross for slike skandaler finner vi en tilsynelatende urokkelig tillit til myndighetene i Norge (Kleven, 2016). Flere studier har vist at et flertall i befolkningen gir sin tilslutning til myndighetenes overvåking hvis det øker sikkerheten (se for eksempel Friedewald, Burgess, Čas, Bellanova, & Peissl, 2017).

Hva de som selv jobber med tematikken mener er i mindre grad studert. En studie av britiske og amerikanske etterretningsoffiserer viser at når de vurderer proporsjonaliteten i sine overvåkingssystemer, argumenterer de nesten utelukkende ut fra om metoden er godkjent av lovgiverne eller ikke (Cayford & Pieters, 2018). Studien peker for øvrig på det store behovet for kunnskap om hvordan de ulike interessentene argumenterer for sine posisjoner. Vår studie søker å bidra til kunnskapsbasen på dette lite utforskede området ved å spesifikt fokusere på subjektiviteten i interessentenes argumentasjon.

Teknologisk utvikling har gjennom tidene ført med seg nye og mer effektive måter å samle og oppbevare informasjon om befolkningen, som igjen har ført til diskusjoner om grensene mellom å beskytte og å kontrollere befolkningen. Mulighetene for digital overvåking som har oppstått de siste tiårene, må leses inn i denne sammenhengen, som et eksempel på hvordan nye verktøy aktualiserer en mer grunnleggende debatt om hva slags samfunn vi vil leve i. I tillegg har flere argumentert for at terroren i USA 11. september 2001 fungerte som en terskelhendelse som forsterket og spisset til risikoargumentasjon globalt samt flyttet tyngdepunktet i overvåkingsdebatten fra å handle om å beskytte seg mot myndighetene til å søke beskyttelse av myndighetene (se for eksempel Massumi, 2010; Lyon, 2003). Også i Norge har vi sett at terrorhendelser har blitt en viktig ramme for diskursen rundt overvåking, og flere lovendringer har kommet som en direkte følge av terror (Husabø & Bruce, 2009). Hvorvidt disse endringene følger av en økt reell risiko eller en tilspisset retorikk knyttet til risiko er en viktig del av overvåkingsdebatten.

Befolkningens syn på overvåking, personvern og menneskerettigheter er i endring (Goold & Lazarus, 2007; Hudson, 2003; Friedewald m.fl., 2017). Det er flere tendenser til det mange betegner som et paradigmeskifte i vår oppfatning av menneskerettighetenes rolle og funksjon i samfunnet (Lomell, 2006, 2014). Myndighetenes overvåking kan forstås både som en trussel mot og beskyttelse av individer. Mens det tidligere var vanlig å plassere overvåking som en potensiell trussel mot individer, er det en økende tendens til at man definerer overvåking som en beskyttelse av individene – mot kriminalitet og terror (Stein, 1996). Denne tendensen ser vi både i Norge og internasjonalt, og disse tendensene kommer også til overflaten i overvåkingsdebatten.

Menneskerettighetserklæringene ble utformet i en tid da den største faren for menneskers frihet og trygghet ble ansett å være en totalitær og/eller en autoritær stat. I dag er det mange som ser saken i et annet lys. Mange mener at myndighetene ikke gjør nok for å forebygge og forhindre alvorlig kriminalitet og terror, de overvåker for lite, ikke for mye (Günther, 2013). Fremveksten av risikosamfunnet med et økt fokus på ulike trusler og farer som truer menneskene forsterker dette. Oppfatningen blant stadig flere er at myndighetene bør gjøre mer for å beskytte sine innbyggere (Ramsay, 2012; Simon, 2007).

Staten gis i stadig større grad rollen som en aktør med en konstitusjonell plikt til å beskytte borgerne. Beskyttelse mot kriminalitet og terror blir slik en menneskerett, en fundamental eller grunnleggende rettighet på nasjonalt nivå. Staten pålegges en plikt til å beskytte befolkningen mot kriminalitet og terror på sitt territorium.

David Murakami Wood har påpekt at debatter om og definisjoner av overvåkingssamfunnet må forstås som historisk, geografisk og kulturelt situert (Wood, 2009). Debatten vi

tar utgangspunkt i har en helt spesifikk geografisk lokalisering i en nasjonalstat med en helt spesifikk historie, og er situert i en spesifikk tid hvor digitale teknologier er i rask fremvekst parallelt med et endret trusselbilde – opplevd eller reelt. Den norske overvåkingsdebatten har vokst frem gjennom en kombinasjon av samspill med allierte og grensedragninger mot andre stater, og den har derfor trekk som er særegne for Norge, samtidig som den har likheter med andre lands debatter. Det som kjennetegner overvåking i Norge på 2010-tallet, er at myndighetenes tilganger er strengt regulert og kontrollert samtidig med at lovgivningen stadig utvides – primært i kjølvannet av terrorhendelser i Norge eller andre land. I tillegg er det en nasjon hvor alle innbyggere er registrert i et folkeregister, og som i stor grad er i ferd med å digitalisere velferdstjenestene, hvilket medfører en radikal økning i gjenfinnbare data om innbyggerne (Schartum, 2010). Samtidig er det norske samfunnet preget av høy tillit til myndighetene (Kleven, 2016). Den norske overvåkingsdebatten kan derfor karakteriseres som en polarisert debatt som finner sted i et relativt harmonisk og tillitsbasert samfunn med høy grad av digitalt registrerte data om innbyggerne. I tillegg virker terrortrusselen og diskursen rundt den direkte inn på debatten.

Overvåkingsdebatten som aktualisering av «matter out of place»

Som vi har sett dreier mye av den vitenskapelige teoretiseringen av overvåking seg om hva overvåking gjør; hvilke effekter, tilsiktede eller utilsiktede, kan økt overvåking føre med seg? Det vi vil bidra med i denne artikkelen er en dypere forståelse for hvordan fenomenet forstås og tolkes av de som jobber med tematikken til daglig. Et særtrekk ved overvåkingsdebatten er at den aktualiseres av den teknologiske utviklingen. De som jobber med tematikken snakker ikke bare om overvåking som metode, de snakker også med utgangspunkt i sine spesifikke perspektiver om hvordan teknologiene som gjør det mulig å overvåke påvirker og endrer samfunnet. Vi hevder at debatten om overvåking i dag dreier seg om å forhandle fram nye grensedragninger for hva som skal regnes som rett og galt i det digitale samfunnet, både moralsk og juridisk.

Dette perspektivet vil utdypes med utgangspunkt i Mary Douglas' begrep «matter out of place»³, som fremhever at det som regnes som farlig eller urent i et samfunn, er det som ikke enkelt kan klassifiseres i det gjeldende klassifikasjonssystemet (Douglas, 2002). Begrepet er hentet fra Douglas' bok *Purity and Danger. An Analysis of Concepts of Pollution and Taboo* (Douglas, 2002), og danner en grunnsten i argumentet for at alle samfunn, både det hun kaller «primitive» og «moderne», har det til felles at de innfører eksplisitte og implisitte regler for å skape orden i samfunnet. Man kan si at disse reglene danner en symbolsk orden som styrer hva som blir vurdert som rent og urent, hva som er greit å gjøre, og hva som ikke er greit å gjøre. I samfunn preget av religiøs styring, som de mange stammesamfunnene Douglas studerte, defineres disse reglene oftest gjennom tabuer. Det som ikke er greit å gjøre blir uttrykt gjennom religiøse forbud, og knyttet til urenheter. Douglas sitt nyskapende argument var å påpeke at de samme mekanismene gjør seg gjeldende i moderne, sekulære samfunn, men med andre uttrykk. Selv om vestlige samfunn i dag ikke styres av religiøse tabuer, finnes det fortsatt behov for å definere grenser for hva som er greit og ikke. Disse grensene defineres ofte på bakgrunn av samfunnets symbolske orden, altså ting vi *tror på*. Sekulære samfunn tror gjerne på objektivitet og vitenskapelighet, men når samfunnet settes

3. Vi bruker det engelske begrepet gjennomgående i artikkelen. Dette fordi det etter vår mening ikke er mulig å oversette på en måte som dekker betydningen og samtidig trer like tydelig frem som et analytisk begrep.

under press blir det tydelig at dette ikke er gitte størrelser, men uttrykk for tolkning. Samfunnets symbolske orden trer tydeligere frem når det skjer noe i samfunnet som gjør at grensene mellom rent og urent, lovlig og ulovlig, ikke lenger fremstår som selvsagte, men heller virker splittende innad i samfunnet.

I vår sammenheng vil nye teknologiske overvåkingmuligheter fremstå som eksempler på elementer som setter vår felles forståelse av samfunnets regler på prøve. Det som ikke enkelt lar seg klassifisere, kan forstås som en trussel mot samfunnet. Douglas (2002) skriver «[...] ideas about separating, purifying, demarcating and punishing transgressions have as their main function to impose system on an inherently untidy experience» (s. 5). Prinsipper knyttet til personvern gjør seg sterkt gjeldende i lovgivning og regelverk om overvåking i vestlige demokratier som Norge. Et lands lovgivning er eksempel på en klassifisering som er grunnleggende for et sekulært samfunn, som rammer inn myndighetenes makt ovenfor befolkningen og gjør at tilværelsen oppfattes oversiktlig, og rettfærdig. Vi har definert en grense for urettmessig bruk av makt fra myndighetene, og overtramp dømmes ved lov. Loven fungerer slik tabuene gjorde i primitive samfunn, den speiler samfunnets verdier, samtidig som den opererer som en rettesnor for befolkningen som gjør at overtrampene også fordømmes moralsk av befolkningen.

Teknologiske nyvinninger bidrar imidlertid til å sette det etablerte klassifikasjonssystemet på prøve. Digitalisering av både den private og offentlige sfæren har ført med seg en stortiltet produksjon av data, som gjør at det vi sier og gjør i stadig mindre grad er flyktig; vi kan rekonstrueres både i tid og rom, som form og innhold. Vi har alle en «digital dobbeltgjenger», et begrep som uttrykker at vi i økende grad lever så påkoblet at sporene etter levd liv kan rekonstrueres som mer eller mindre nøyaktige avspeilinger som eksisterer og utvikler seg i tilknytning til, men samtidig uavhengig fra individene (Haggerty og Ericson, 2000). David Lyon har tatt til orde for at vi lever i en overvåkingskultur, hvor overvåking har blitt et integrert aspekt ved vår levemåte (Lyon, 2018). Dette fordi overvåking, eller potensialet for overvåking, er en sentral bestanddel av det digitale: Teknologien vi har blitt helt avhengig av, setter spor som kan observeres i sanntid og gjenfinnes i ettertid. Dette setter klassifikasjonene knyttet til overvåking under press i dagens samfunn; grensene må defineres på nytt. Polariseringen i det offentlige ordskiftet om overvåking antyder at det er uenighet om hvordan grensene skal dras opp; hva forstås egentlig som «matter out of place» i dagens digitaliserte samfunn – terrortrusselen eller overvåkingstrusselen?

Metode

Deltakerne i studien ble rekruttert med tanke på å få et så bredt utvalg som mulig blant personer med spesialkunnskap innenfor ulike aspekter ved myndighetenes tilgang til digital overvåking. Vi startet med å identifisere hvilke sektorer vi ville finne relevante informanter fra: politi/etterretning, offentlige organer, politikk, privat sektor/teknologibransjen, frivillige organisasjoner, akademia og samfunnsdebattanter. Vi brukte media til å identifisere personer som var aktive i offentlig debatt, og deretter snøballmetoden for å finne interesser som jobber med tematikken, men som ikke nødvendigvis er synlige i det offentlige ordskiftet.⁴

4. En anonymisert oversikt over informanter og yrkestilhørighet er tilgjengelig i dokumentasjonsnotatet (Flinterud og Strype, 2020).

rer. Utvalget bestod av 6 kvinner og 19 menn, hvorav de fleste falt innenfor aldersgruppene 40-49 (12) og 50-59 (9). Én deltaker var i aldergruppen 20-29, mens de resterende 3 var i alderen 30-39. Ettersom de primære utvalgskriteriene var at dette skulle være eksperter på feltet, og at de skulle representere en bredde, vurderte vi det slik at det ikke var faglig forsvarlig å etterstrebe en jevn kjønns- og aldersfordeling. Vi mener fordelingen i kjønn og alder i utvalget speiler den kjønns- og aldersfordelingen vi finner i den aktuelle gruppen.

Selv om det ikke har vært utført Q-metodologiske studier av overvåkingsdebatten, viser for eksempel en studie av debatten knyttet til automatisert grensekontroll i Schengen hvilket potensiale Q-metodologi har til å få frem interessenters felles utgangspunkt og uenigheter (Lehtonen & Aalto, 2017). For en kort beskrivelse av Q-metodologi, se dokumentasjonsnotatet (Flinterud og Strype, 2020).

Q-studien besto av flere deler. Første skritt var å definere *concourse* (Watts & Stenner, 2012, s. 34), som i vårt tilfelle kan beskrives som alle påstander som til sammen dekker de gjeldende posisjonene i overvåkingsdebatten. Påstandene i studien ble hentet fra offentlige dokumenter knyttet til lovforslaget om endringer i straffeprosessloven, rapport og høringsvar knyttet til digitalt grenseforsvar, samt alle relevante medieoppslag fra de største nasjonale og regionale norske avisene tilgjengelige i Retriever, fra januar 2009 til oktober 2017.

Neste skritt var å gjøre et utvalg av påstander til bruk i Q-sorteringene. Studien er del av et større, internasjonalt prosjekt, og utvalget av påstander ble derfor gjort i samarbeid med forskere fra Finland og Storbritannia. Hvert lands forskere utviklet egne sett (*concourses*) før vi møttes og diskuterte oss frem til et sett med 45 påstander som vi mente dekket debatten i alle de tre landene på en god måte.⁵ Med dette settet av påstander fikk hvert land inkludert påstander som ble vurdert som helt sentrale i den nasjonale debatten, samtidig som ingen måtte inkludere noe som virket helt irrelevant. Alle deltakerne ble bedt om å vurdere utvalget av påstander etter sorteringsøvelsen, og samtlige sa de kjente igjen den norske debatten ut fra påstandene.

Deltakerne i studien gjennomførte først en sorteringsøvelse (Q-sortering). Deretter fulgte et kvalitativt intervju med utgangspunkt i sorteringen og påstandene.

I sorteringsøvelsen ble deltakerne bedt om å sortere en bunke med kort med de utvalgte påstandene i forhold til hverandre på et gitt skjema, fra mest enig til mest uenig. Skjemaet vi brukte hadde 11 kolonner, markert fra -5 til +5, med 0 i midten. I tråd med Q-metodologien var formatet bestemt på forhånd, slik at det skulle legges 2 kort på de to ytterste søylene, 3 kort på -4 og +4, 4 på -3 og +3, 5 på -2, -1, +1 og +2, og 7 på 0. Hver deltaker ble dermed tvunget til å se påstandene i forhold til hverandre heller enn å ta stilling til hver påstand for seg. Sorteringen ble så notert ned.

Q-faktoranalysen ble i vår studie gjennomført ved hjelp av kommandoen *qfactor* (Akhtar-Danesh, 2018) i statistikkprogrammet Stata. Datamatriksen som ble analysert besto av de 25 informantenes sortering av de 45 påstandene, der påstandenes plassering i sorteringen var tilordnet verdiene -5 til 5.

Vi vurderte mulige faktorløsninger på grunnlag av flere kriterier: Kaisers kriterium, dvs. å kun trekke ut faktorer med eigenvalue over 1, inspeksjon av scree plot og Horns parallellanalyse (Horn, 1965). Vi åpnet også for å gjøre en kvalitativ vurdering av hvorvidt faktorene som framkommer i analysen er teoretisk interessante, dersom det var flere potensielle løsninger basert på de statistiske kriteriene.

5. Alle påstandene er tilgjengelige i dokumentasjonsnotatet (Flinterud og Strype, 2020).

Ved hjelp av *qfactor* identifiserte vi typiske Q-sorteringer for hver faktor (Watts & Stenner, 2012, s. 140; Størksen, 2012, s. 568). For en teknisk beskrivelse av hvordan typiske Q-sorteringer konstrueres og tolkes, se Watts & Stenner (2012, s. 129-141).

I det påfølgende intervjuet ble deltakerne bedt om å kommentere sorteringen, og å diskutere påstander som deltakerne selv mente det var viktig å snakke om. Det ble gjort opptak av denne delen av intervjuet, og opptakene ble transkribert. Den kvalitative delen av intervjuet tok vanligvis rundt 60 minutter.

Med Q-metodologien fikk vi altså både et kvantifiserbart materiale gjennom sorteringen, og et kvalitativt materiale gjennom samtalen i etterkant av sorteringen. Gjennom det kvantitative materialet fikk vi dermed en overordnet beskrivelse av posisjonene i debatten, mens det kvalitative materialet bidro til en dypere forståelse av dynamikken i posisjonene. Metoden muliggjorde dermed en forståelse av de ulike nivåene i debatten som ikke ville tredd like tydelig fram med en ren kvantitativ eller kvalitativ tilnærming.

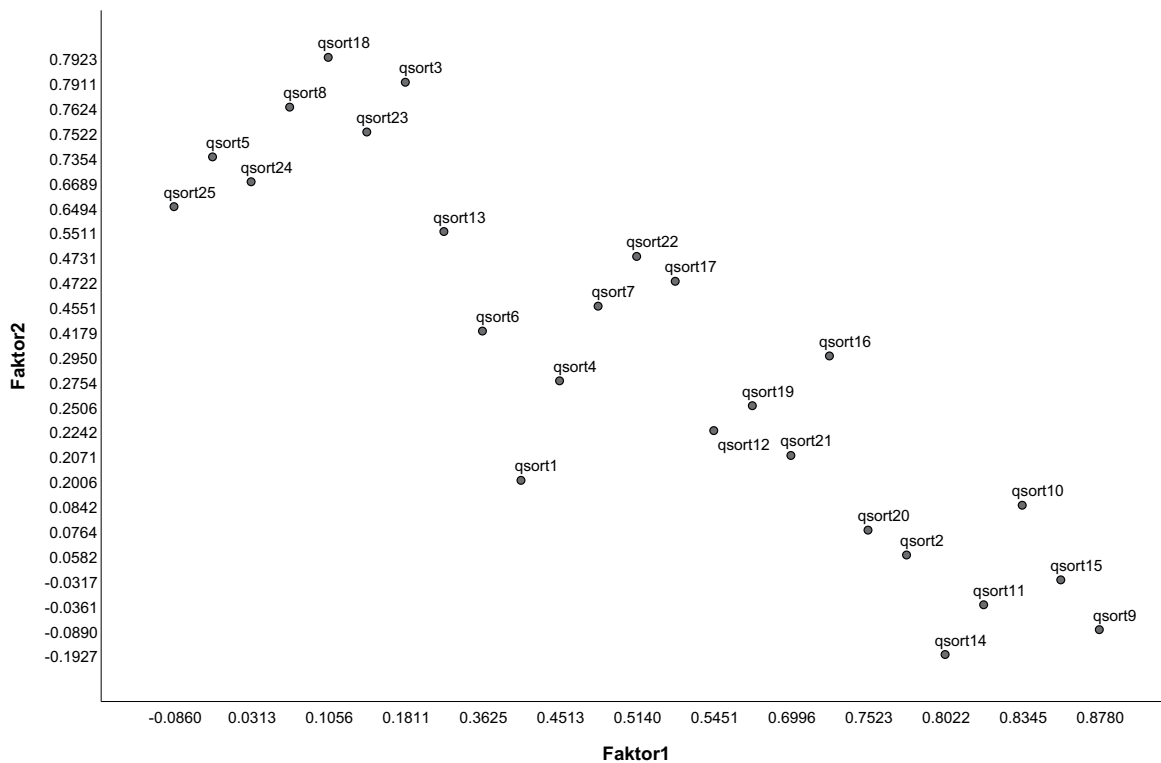
Resultater

Fra Q-sorteringer til faktorer

Det første spørsmålet vi ønsket svar på, var hvor mange faktorer vi med rimelighet kunne dele de 25 Q-sorteringene inn i. Vi gjennomførte en første faktoranalyse (itererte prinsipalfaktorer, IPF) med de 25 sorteringene som input-variabler i analysen. Alle kriterier (Kaisers kriterium, scree plot og Horns parallellanalyse) pekte tydelig i retning av å velge en tofaktorløsning. Ettersom q-metodologi åpner for å bruke det kvalitative materialet for å danne et bedre bilde av faktorene, gikk vi til de definerende påstandene for å se om det innholdsmessig var grunnlag for å ta med en tredje, svak faktor. Vi så imidlertid at de påstandene som dataanalysen løftet frem som definerende for den tredje faktoren, ikke uttrykte noe meningsinnhold som skilte denne tydelig fra de to andre faktorene. Vi konkluderte derfor med at det ikke var hensiktsmessig å se på løsninger med flere enn to faktorer.

Vi gjennomførte deretter en endelig faktoranalyse med to faktorer og varimax-rotasjon. Figur 1 viser hvordan hver av de 25 Q-sorteringene lader på faktor 1 og faktor 2.⁶ Det framgår av figur 1 at noen Q-sorteringer er tydelig plassert i faktor 1 eller faktor 2, mens andre sorteringer i mindre grad har en entydig plassering. I tillegg til q-sorteringene som lader på enten faktor 1 eller faktor 2 var det tre sorteringer som ladet på begge faktorer, og som derfor er utelatt fra analysen. Disse befinner seg visuelt midt i figur 1, med kodene qsort22, qsort7 og qsort17. Vi ser altså at selv om resultatet av faktoranalysen peker mot to faktorer, så befinner q-sorteringene seg langs et kontinuum, hvorav flere befinner seg nær midtpunktet.

6. Se også faktormatrisen i tabell A1 i dokumentasjonsnotatet (Flinterud og Strype, 2020)



Figur 1: Faktorladningsplott: Q-sorteringenes faktorladninger på henholdsvis faktir 1 og faktor 2.

Fra faktorer til gruppenes typiske Q-sorteringer: polarisering og konsensus
 Ved hjelp av faktoranalysen delte vi sorteringene inn i to faktorer, som er uttrykk for dis-
 tinkle klasser av synspunkter. Vi konstruerte deretter typiske Q-sorteringer for hver faktor,
 som beskrevet tidligere. Figurene 2 og 3 viser de to faktorenes typiske Q-sorteringer.⁷

-5	-4	-3	-2	-1	0	1	2	3	4	5
11	9	2	8	7	6	29	3	4	16	1
37	22	15	21	12	10	33	19	5	18	14
	25	23	24	31	13	36	26	17	38	
		34	30	35	20	40	42	41		
			39	45	27	43	44			
					28					
					32					

Figur 2: Factor array, faktor 1.

7. Tabell A2 i dokumentasjonsnotatet viser i tillegg z-skårene som korresponderer til verdiene i de typiske sorte-
 ringene.

-5	-4	-3	-2	-1	0	1	2	3	4	5
24	2	3	15	1	4	8	23	6	5	14
30	21	13	18	11	9	22	34	10	7	16
	29	19	20	17	12	37	39	28	38	
		35	26	27	25	41	44	31		
			33	32	36	43	45			
					40					
					42					

Figur 3: Factor array, faktor 2.

Det er viktig å minne om at de aggregerte, typiske Q-sorteringene ikke er identiske med de enkelte informanternes sorteringer, men snarere uttrykker det som er typisk for hver klasse av synspunkter. Når vi snakker om «faktorer», viser vi til den typiske sorteringen som ble generert av q-faktoranalysen. Beskrivelsen av hva som kjennetegner hver faktor, sier noe om den meningsstrukturen informantene argumenterer innenfor, men det sier ikke noe om hvordan hver enkelt informant argumenterer. Enkeltinformantenes argumentasjon kommer først til syne i analysen av de kvalitative intervjuene, hvor vi forsøker å nyansere og skape en dypere forståelse for argumentasjonen innad i de to klassene av synspunkter.

Det sentrale standpunktet i den første faktorens typiske Q-sortering er at menneskerettigheter, ytringsfrihet og et sikkert internett opprettholdes ved å begrense myndighetenes tilgang til digital kommunikasjon og informasjon. Vi finner også frykt for at videre tilganger til digital kommunikasjon kan svekke tilliten både til myndigheter og teknologi, og dermed føre til at befolkningen bevisst unngår å søke opp informasjon eller å ytre seg i frykt for å havne urettmessig i myndighetenes søkelys. Påstander som omtaler det gjeldende forslaget for Digitalt Grenseforsvar, slik som «37. Den preventive effekten av et digitalt grenseforsvar veier opp for de antatte finansielle og samfunnsmessige kostnadene» og «9. Et digitalt grenseforsvar er en nøyaktig og pålitelig måte å avdekke informasjon om hittil ukjente trusler mot rikets sikkerhet» er sortert mot mest uenig»⁸. Hovedsakelig dreier den sentrale posisjonen seg om å sørge for at folk har tillit til at de kan leve en beskyttet tilværelse også i det digitale rom, og en beskyttet tilværelse forstås her som frihet fra å bli urettmessig overvåket av myndighetene. Viktigheten av kunnskapsrike og uavhengige godkjennings- og kontrollorganer og åpne demokratiske prosesser står sentralt, og potensielle utilsiktede og negative konsekvenser av overvåking vektlegges framfor tilsiktede effekter som forebygging og bekjempelse av kriminalitet og terror.

I den andre faktorens typiske Q-sortering fremheves viktigheten av at overvåkingspraksiser ikke skal være diskriminerende, og at menneskerettigheter skal gjelde likt på alle områder av livet, både online og offline. Her settes imidlertid disse påstandene i sammenheng med at vi vil få et tryggere samfunn dersom myndighetene får bedre tilgang til den digitale sfæren,

8. På tidspunktet for intervjuer var ikke Forsvarsdepartementets forslag til ny etterretningslov publisert, og intervjuobjektene tok dermed stilling til forslaget slik det forelå i rapporten «Digitalt Grenseforsvar» fra Lysne II-utvalget (Lysne m.fl., 2016).

som «7. Å utvide myndighetenes tilgang til kommunikasjon på nett vil gjøre samfunnet tryggere for borgerne» og «10. Dagens kriminalitets- og trusselbilde gjør det nødvendig å utvide myndighetenes tilgang til overvåking i cyberspace». I likhet med den første sorteringen ligger hovedfokus på å skape trygghet i det digitale rom, men her er det myndighetene som skaper denne tryggheten. Tilliten til myndighetene avspeiles også i påstandene som sorteres mot mest uenig, som at de ikke er enige i at myndighetene får alt de ber om uavhengig av debatten. I motsetning til den første sorteringen, hvor det uttrykkes frykt for hva myndighetenes overvåking kan gjøre med tilliten i befolkningen, ser vi her en sterk tro på myndighetenes evne til å holde på og bygge tillit og trygghet gjennom å bruke overvåkingsmetoder for å bekjempe og forhindre kriminalitet. Det legges også i større grad vekt på påstander som omhandler praktiske hensyn, som at det er stor forskjell på å overvåke metadata og innholdsdata når det gjelder inngrep i personvern, og at det å overvåke i det digitale rom ikke skiller seg fundamentalt fra den overvåkingen som skjer på andre måter. Sett i sammenheng uttrykker påstandene som er vektet høyt, enten mot enig eller uenig, et standpunkt som aksepterer økt overvåking i det digitale rom, samtidig som man er opptatt av at praksisen rammes inn på en forsvarlig måte, både juridisk og moralsk.

Samtidig som faktoranalysen identifiserte to klasser av synspunkter med distinkte kjennetegn, er kanskje det mest slående resultatet at det er betydelig overlapp, i den forstand at det er påstander som plasseres ganske likt i begge sorteringer. Dette gjelder særlig påstander som sorteres mot «mest enig»-siden. De sentrale enighetene dreier seg om grunnleggende prinsipper i et moderne, demokratisk samfunn: «16. Det er essensielt at alle mennesker gis de samme grunnleggende rettighetene på nett som de har i livet ellers», «14. Målrettingen av overvåkingsmetoder må ikke være av diskriminerende art, med andre ord, den må ikke være basert på etnisitet, religion, meninger, tilhørighet til en sosial gruppe eller andre personlige faktorer uten en rimelig grunn», og «38. For å sikre fullstendig demokratisk kontroll må de som fører tilsyn med og kontrollerer etterretningstjenestene ha tilstrekkelig kunnskap og teknisk kompetanse til å forstå etterretningstjenestenes tilganger og aktiviteter». Dette viser at aktørene tross uenighet debatterer ut fra en felles plattform, man er enig om hva slags samfunn man vil ha. Det man ikke er enig om er hva som skal til for å oppnå et slikt samfunn, og hvilken rolle myndighetene spiller i denne sammenhengen. Både enigheten og uenigheten kan forstås som uttrykk for hvordan aktørene forstår myndighetenes rolle, som garantist for eller trussel mot et fritt, demokratisk samfunn der grunnleggende menneskerettigheter beskyttes og respekteres. Posisjonene i debatten illustrerer to ulike tilnærminger til spørsmålet.

Før vi går videre, er det på sin plass med noen kritiske refleksjoner om bruk av Q-metodologi i studien. Et grunnleggende diskusjonspunkt er validiteten til grupperingene som framkommer i Q-faktoranalysen. Hvor mange faktorer man trekker ut av materialet, vil påvirke hva som kjennetegner innholdet i faktorene. Vi har imidlertid holdt oss strengt til den klassiske faktoranalysens kriterier for å velge faktorløsning, og basert på disse kriteriene var det entydig støtte til å dele materialet i to grupper av synspunkter. Et annet kritisk punkt er hvorvidt det er statistisk sunt å utføre en faktoranalytisk studie med så få som 25 personer. Her er det imidlertid nødvendig å huske på at det er påstandene, og ikke personene, som er enheter i Q-faktoranalysen. N er altså 45 i vår studie. Et siste spørsmål dreier seg om selve Q-sorteringsøvelsen. Ettersom formatet for sortering av kortene er gitt, kan man spørre seg om dette kan gi et godt bilde av subjektivitet. Dette kom også opp i intervjuene hvor flere påpekte at den endelige fordelingen av påstander i skjemaets ytterste kolonner (-5 og +5) ville kunne variere i ulike kontekster. Likevel mente de at hovedbildet i fordelingen ville holdt seg stabilt. Det er dermed lite sannsynlig at disse justeringene ville flyttet noen av deltakerne over i en annen faktor. Det tvungne Q-formatet kan imidlertid også ha fordeler. Når deltakeren tvinges til å

rangere påstandene i forhold til hverandre i Q-sorteringen, kan nyanser komme til syne som ikke alltid kommer fram i en spørreskjemabasert holdningsundersøkelse hvor hver påstand vurderes isolert. Vi har i vår studie brukt mer tid på de kvalitative intervjuene i etterkant av sorteringen enn det som er vanlig i en q-metodologisk studie. Dette har gitt oss et større materiale å tolke gruppering av synspunkter ut fra, og også større forståelse for argumentasjoner i overvåkingsdebatten. Gjennom denne kombinerte vektleggingen av kvalitative og kvantitative analyser vokser et komplekst landskap av argumenter frem, som på ulike måter balanserer enighet og uenighet.

Diskusjon

Ulike forståelser av «matter out of place»

Både dokumentanalysen og intervjuene fremhever at informantene i vår studie tar utgangspunkt i ulike forståelser av hva som er «matter out of place», hva som skaper uorden og dermed er «farlig», for å bruke Douglas' terminologi. Informantene som argumenterer for økt overvåking, definerer primært terror og kriminalitet som «matter out of place». For denne gruppen er det radikaliserte og kriminelle som skaper uorden i systemet, og deres befatning med teknologi som myndighetene ikke har tilgang til forsterker denne uordenen. Argumentasjonen er at samfunnet blir farligere på grunn av den teknologiske utviklingen, men det er ikke overvåkingsteknologien i seg selv som skaper uorden i samfunnet—det er det kriminaliteten og terroren som gjør. Teknologien i seg selv vil være et positivt tilskudd dersom den ble en del av politiet og etterretningstjenestenes verktøykasse. Dette underbygges blant annet i at denne gruppen er enig i påstandene «7. Å utvide myndighetenes tilgang til kommunikasjon på nett vil gjøre samfunnet tryggere for borgerne» og «28. Teknologien utvikler seg så raskt at myndighetene og lovgivningen ikke klarer å holde tritt», kombinert med at de er mer uenige i påstanden «1. Sikkert internett er et grunnleggende verktøy i et fritt og demokratisk samfunn. Produkter og tjenester som støtter opp om denne sikkerheten bør ikke settes på spill ved at produsenter bes om å overlevere dekrypteringsnøkler». Teknologien fremstår her som et gode i hendene på myndighetene—hvis myndighetene hadde fulgt bedre med i utviklingen, og hatt tilgang til kommunikasjon på nett, så ville samfunnet vært tryggere. De er samtidig uenige i at å overlevere dekrypteringsnøkler setter nettsikkerhet på spill. Lest som en metode myndighetene kan bruke for å få tilgang til kommunikasjon på nett, fremstår utlevering av dekrypteringsnøkler som en måte å trygge samfunnet.

Dette poenget understrekes i mange av intervjuene fra denne gruppen, men her fremheves det også at dette ikke er noe man bør ta lett på. En sier for eksempel:

hvis mistanken er der og dataene er utilgjengelig fordi det er brukt kryptering, og et selskap besitter den nøkkelen, og domstolen har besluttet at dette er data politiet skal få tilgang i, så mener jeg at du må kunne pålegge de utlevering av krypteringsnøkkel for å få tilgang til den informasjonen som domstolen har besluttet at myndighetene skal ha.

En annen uttrykker det slik:

[...] og det er nødvendig rett og slett noen ganger å ha muligheten til å bruke metoder effektivt ved å få den typen nøkler fra leverandør. Men etter rettslig behandling og alle rettsikkerhetsgarantier ivaretatt osv. Så er problemet med en del av de dekrypteringsnøkklene at hvis du først gir den fra deg så har de på en måte tilgang til alt. Og det gjør det mer krevende, men jeg mener i utgangspunktet at det må være greit.

Det er med andre ord et nødvendig onde som beskrives i intervjuene. Påstanden om dekrypteringsnøkler er heller ikke ukontroversiell for de som assosieres med denne gruppen. En av informantene sier friskt: «Jeg er usikker på om jeg har troen på dekrypteringsnøkler som skal overleveres fra produsenten, for det kommer bare til å bite oss i ræva lengre frem». Denne informanten har en mer teknologisk inngang til problemstillingen, og trekker frem at når en slik nøkkel blir frigitt er det stor sjanse for at den havner i hendene på uvedkomne. Informanten konkluderer med at det beste nok er å ikke tillate bruken av dekrypteringsnøkler, og sier «vi taper nok litt på det, men jeg tror vi vinner mer på sikt».

Til tross for at informantene over ender på ulikt standpunkt i denne konkrete saken, argumenterer de alle innenfor den samme logikken. Utgangspunktet deres er at terrorister og kriminelle opererer i skjulte rom på internett, og at politi og etterretning trenger tilgang der for å stoppe dem. Ifølge denne argumentasjonen destabiliserer den teknologiske utviklingen samfunnet gjennom at kriminelle tar den i bruk umiddelbart, mens myndighetene må gjennom strenge prosesser før de får ta den i bruk. Teknologien er som sådan ikke «matter out of place» i et større perspektiv, den er bare «matter currently misplaced». Ved å følge de fastlagte strukturene i det norske demokratiet, først med generell godkjenning av metoden gjennom lov, deretter godkjenning av den enkelte sak ved domstolskjennelse, vil stabiliteten i samfunnet re-etableres. Det som virkelig er «matter out of place» i denne argumentasjonen er kriminalitet og terror. Hele utgangspunktet for overvåkingsdebatten sett fra denne gruppens argumentasjon er at kriminalitet og terror ikke har noen plass i vårt klassifikasjonssystem. Argumentasjonen knyttes primært til å finne løsninger for å fjerne avviket, og mer sekundært til overvåkingsteknologiens utilsiktede effekter. Dette gjenspeiles godt i utsagnet om at vi ved å avstå fra å be selskaper om dekrypteringsnøkler kanskje taper på kort sikt, men vinner på lang sikt. Til tross for at denne informanten mener vi må avstå fra å bruke akkurat denne type teknologi, så er ordene «tape» og «vinne» primært knyttet til å bekjempe kriminalitet og terror.

Informantene som assosieres med et ønske om begrenset overvåking definerer derimot overvåkingen i seg selv som «matter out of place». Denne gruppen slutter seg til påstanden som advarer mot å frigi dekrypteringsnøkler, sammen med påstanden «Muligheten for at man kan bli overvåket på nett fører til selvsensur og frykt. Dette vil i siste instans virke ødeleggende på demokratisk debatt og tankens frihet». Begge disse påstandene sorteres mot uenig av den andre gruppen. Isolert sett tar påstanden om dekrypteringsnøkler utgangspunkt i at teknologien i seg selv har en iboende mulighet for å destabilisere cybersikkerhet. Dette hensynet er ikke del av argumentasjonen til de to første informantene sitert over. I det tredje sitatet over er dette perspektivet en del av meningsinnholdet, men det er ikke grunnleggende for argumentasjonen. Forskjellen i argumentasjon blir tydeligere når man går til intervjuene i gruppen som mener overvåking bør begrenses. Én formulerer sammenhengen mellom de to påstandene over slik:

Jeg bare henviser til høringsuttalelsen fra Direktoratet for e-helsetjenester til digitalt grenseforvar, som jo ikke har noe med cyberangrep og terrorisme og så videre å gjøre, men som sier folk kommer til å slutte å registrere sine helsedata hvis de ikke vet hvem som kan spionere på det.

Sitatet illustrerer et gjennomgående poeng i denne gruppens argumentasjon, nemlig at dette dreier seg om mer enn terrorisme og kriminalitet. Overvåkingsteknologier rammes inn som noe som vil gjennomsyre alle deler av samfunnet og få konsekvenser på tvers av sektorer. Denne argumentasjonen etablerer overvåkingsteknologiene som i seg selv «matter out of place». Det er overvåkingsteknologien som representerer et avvik. Teknologiene skifter

ikke status avhengig av hvem som bruker dem, de er i seg selv potensielt skadelige, og må derfor begrenses. Selv om den grunnleggende forståelsen av overvåkingsteknologi som et onde er felles for argumentasjonen i denne gruppen, kommer det frem mer balanserte avveininger i intervjuene enn det som antydes i det offentlige ordskiftet. En informant reflekterer over problematikken slik:

Intensjonen, når politiet sier at vi får ikke tilgang fordi du har kryptert telefonen din og de trenger å etterforske, intensjonen er jo god. Det er bare det at, når jeg for eksempel sier at «no fucking way» at det skal være en bakdør der, så er ikke det for at politiet ikke skal få etterforske deg når det behovet er der. Det er for konsekvensen for sikkerheten og stabiliteten på resten, på de tjenestene vi har som ligger som fundament for samfunnet. Og det er nettopp det det handler om.

Utdraget eksemplifiserer hvordan denne gruppen vender fokuset bort fra det å forhindre kriminalitet. Den grunnleggende forståelsen de som vil begrense overvåking bygger sin argumentasjon på, er at dette dreier seg ikke primært om kriminalitet og terror, det dreier seg om teknologi og overvåkingens konsekvenser for tillit og frihet.

Der påstanden om dekryptering eksplisitt viser til cybersikkerhet, peker påstanden om selvsensur og frykt på nedkjølingseffekten. Grunnlaget for teorier om nedkjølingseffekt er nettopp at frykten for overvåking vil føre til at befolkningen, eller spesifikke grupper, vil slutte å ytre seg eller bruke digitale verktøy for å lete opp informasjon, i frykt for å havne urettmessig i politiets søkelys. Teorien peker på hvordan slike mekanismer kan føre til en forvitring av demokratiet (Schauer, 1978). Påstanden om nedkjølingseffekten, i kombinasjon med påstanden om dekryptering, gir et sterkt uttrykk for at gruppen som argumenterer for begrenset overvåking fremhever viktigheten både av tillit til at teknologien er trygg, og til at det er restriksjoner på muligheten for å bruke teknologien mot befolkningen. Dette uttrykker et ønske om å holde teknologien i sjakk, å sørge for at bruken tilpasses vårt moralske klassifikasjonssystem.

Hvordan påstanden om nedkjølingseffekten snakkes om i intervjuene avspeiler også utgangspunktet informantene argumenterer ut fra. De som vil begrense overvåking uttrykker tydelig at de kjenner til det teoretiske begrepet og forskningen rundt det, en sier for eksempel: «Spørsmålet om selvsensur og frykt er en realitet, i hvert fall de undersøkelsene jeg har sett på området. Men foreløpig, av det jeg har sett, så er det først og fremst et problem for utsatte grupper». Mange i denne gruppen nyanserer bildet ved å vise til innskrenkingen av demokratiet i land som Tyrkia, Polen og Ungarn i nyere tid, eller å vise til historiske eksempler som hendelser i DDR og andre totalitære stater. De kontekstualiserer bekymringen med eksempler på hva som kan skje dersom myndighetene får videre tilganger, og i mindre grad opp mot faktiske hendelser i Norge i dag. Det er allikevel tydelig at argumentasjonen er knyttet til hva teknologien potensielt kan gjøre, uavhengig av brukerens intensjon.

Argumentasjonen rundt nedkjølingseffekt fra de som ønsker økt overvåking viser tydelig at de har kriminalitet, og ikke teknologi, som utgangspunkt. En påpeker:

Jeg vil mene det er motsatt, fordi at nå vil folk la være å delta i debatten på nett fordi det ikke er noe kontroll der. Det er bare å være kvinnelig, politisk debattant, for eksempel, og så gå ut på nett og skrive en artikkel, så gjør du det en gang og så lar du være fordi du får så mye tilbake.

En annen sier «Jeg er jo godt vant med å gjøre vurderinger av utsagn på nett hvor folkeskikken ikke er på plass». Ut fra denne logikken snus hele ideen om nedkjølingseffekt på hodet.

Når utgangspunktet for debatten er at internett er et kontrollfritt rom hvor myndighetene ikke har tilgang, tolkes andre dynamikker inn i denne påstanden, som at vanlige mennesker som sprer negative kommentarer fører til en nedkjølingseffekt på nett ettersom myndighetene ikke er til stede der. Der hvor den akademiske teorien om nedkjølingseffekten påpeker den panoptiske effekten, altså at man lar være å gjøre noe på grunn av frykten for at man *kan* være under oppsyn av myndighetene, viser argumentasjonen i denne gruppen til en mer praktisk og erfaringsbasert effekt knyttet til samhandling mellom privatpersoner. Netthets er et reelt problem i dagens samfunn, og de som jobber med å bekjempe netthets, ser en nedkjølingseffekt som følge av at myndighetene *ikke* ser det som skjer der. Dette er en annen mekanisme enn påstanden i utgangspunktet var ment å vise til, men resultatet tydeliggjør hvordan sakskomplekset i debatten gis ulike meninger etter hvilket perspektiv debattantene fortolker situasjonen fra. Det viser også til den grunnleggende forskjellen mellom det å fremme behovet for beskyttelse *mot* eller beskyttelse *av* myndighetene.

Tilsynelatende enighet

Med utgangspunkt i påstandene som er sortert langt fra hverandre i de to typiske sorteringene, finner vi tydelige motsetninger mellom de to gruppene. Som vi har sett underbygger argumentasjonen i det kvalitative materialet uenigheten mellom gruppene. Det at enkelte sentrale påstander allikevel er sortert likt i begge gruppene, som nevnt over, tilsier at det allikevel ligger en felles, overordnet klassifisering til grunn for debatten. Som nevnt over er informantene i stor grad enige om viktigheten av menneskerettigheter, og kritiske til å diskriminere individer på bakgrunn av gruppetilhørighet. På påstandsnivå uttrykker disse begrepene et felles ståsted på tvers av informantene. Går vi inn i hvordan forståelsen av begrepene blir artikulert i intervjuene, finner vi imidlertid tydelige spor av utviklingen som skisseres tidligere i artikkelen, nemlig brytningen mellom å vurdere myndighetene som henholdsvis de som skal beskytte oss, og dem vi bør beskyttes mot.

Når det gjelder påstanden «16. Det er essensielt at alle mennesker gis de samme grunnleggende rettighetene på nett som de har i livet ellers», sier for eksempel en informant fra gruppen som vil begrense overvåking at dette er en av få påstander som er et tydelig «argument[er] imot overvåking, eller logikk[er] mot overvåking, eller som kan bidra til en refleksjon om at vi kanskje ikke skal overvåke så mye». I gruppen som ønsker økt tilgang til overvåking forstås påstanden imidlertid i en helt annen kontekst:

[...] (D)et er nå et av de store problemene, at man har mangelfull normdanning på internett. Og realiteten er at folk opplever ikke å ha samme rettighetene på nett som ellers, i forhold til beskyttelse da. Og det foregår utrolig mye handlinger der som ellers ikke ville ha skjedd. Og det ... det mangler man jo instrumenter til å ... til å håndheve, da.

Rettigheter er med andre ord et begrep som overordnet kategoriseres som en viktig verdi i vårt samfunn. Alle er enige om at like rettigheter er grunnleggende for et fritt samfunn, og at det innebærer at man har med seg rettighetene sine også når man ferdes i det digitale rom. Hva rettigheter innebærer er imidlertid ikke entydig. Den første informanten argumenterer helt tydelig fra et implisitt ståsted som sier at dette gjelder retten til å ikke bli overvåket. Den andre informantens utdypning synliggjør en posisjon som ikke bare uttrykker at han tolker begrepet «rettighet» som retten til å bli beskyttet mot ytre farer, men også at dette standpunktet knyttes til manglende normer i det digitale rom. Denne informantens begrunnelse uttrykker helt spesifikt at dette for ham dreier seg om å etablere normer for hvordan vi bruker ny teknologi. Det at internett oppfattes som et kontrollfritt rom, er fra dette standpunktet

forbundet med tap av retten til å bli beskyttet av myndighetene, som veier tyngre enn et potensielt tap av retten til å være anonym på nett.

Informanten som mente denne påstanden er et tydelig argument mot overvåking, tar også utgangspunkt i teknologi og normer når standpunktet utdypes, men her handler det ikke om å kontrollere og stoppe gråsonepåførsel, som spredning av negative kommentarer. Her er det i stedet myndighetenes manglende teknologiske forståelse som er det potensielle problemet. Informanten sier:

Man får en opplevelse av at de ikke ville sagt de samme tingene, ment de samme tingene hvis de [ikke gjaldt] digitalt. Mens fordi at det digitale er der, så tenker de at 'ah, her er det så mye å ta av, her', man er på en måte villig til å gjøre det fordi at overvåkingen i realiteten er usynlig. Mens mye av det som tas opp ville man ikke foreslå i en ikke-digital setting.

Problemet, slik denne informanten forstår det, er med andre ord ikke nødvendigvis at vi må beskyttes mot myndighetene fordi de har dårlige hensikter, men at vi må beskyttes mot myndighetene fordi de ikke ser konsekvensene av hva de gjør. Det er tydelig at informanten mener de på nåværende tidspunkt ikke har god nok teknologiforståelse til å se rekkevidden av å tillate overvåking på nett. Det grunnleggende for denne argumentasjonen er at myndighetenes manglende forståelse for teknologiutvikling kan føre til overtramp, ikke at myndighetenes manglende tilstedeværelse på digitale kanaler fører til dårligere beskyttelse.

Påstanden om like rettigheter online og offline inviterer spesifikt til å vurdere overvåking i det digitaliserte samfunnet, og tydeliggjør hvordan informantenes argumentasjon er en del av en større forhandling om å definere det digitale inn i et allerede etablert begrepssystem for å snakke om overvåking. Det blir også tydelig at begrepet «rettigheter» tolkes ulikt, på den ene siden som retten til å bli beskyttet av myndighetene på nett, og på den andre siden, retten til å slippe innsyn fra myndighetene på nett.

Den andre påstanden det er enighet om på tvers av gruppene, går inn i mer generelle prinsipper: «14. Målrettingen av overvåkingsmetoder må ikke være av diskriminerende art, med andre ord, den må ikke være basert på etnisitet, religion, meninger, tilhørighet til en sosial gruppe eller andre personlige faktorer uten en rimelig grunn». Påstanden inviterer til å reflektere over hvordan overvåking på nett foregår, men den aktualiserer også et sentralt argument som brukes for å legitimere overvåking, nemlig terrortrusselen. Selv om de aller fleste er enige i grunnprinsippet, er det også mange informanter, fra begge grupper, som nyanserer med å påpeke at dette også er et spørsmål som må vurderes ut fra det generelle trusselbildet. En sier for eksempel: «så er det mye større grunn til å overvåke de som har vært fremmedkrigere i Tyrkia som tilhører en annen etnisitet ... som er likere etnisk og religiøst enn mange andre grupper i samfunnet». Dette utsagnet kommer fra en informant som i hovedsak vil begrense overvåking, og illustrerer hvordan intervjuene bringer frem kompleksiteten i avveiningene som ligger bak standpunktene om å ønske mer eller mindre overvåking. Informanten er generelt kritisk til å ta i bruk de overvåkingsmulighetene som ligger i dagens teknologi, men mener allikevel at dette prinsipielle standpunktet må vike for mer presserende og dagsaktuelle hensyn, som trusselbildet knyttet til internasjonal terror.

Refleksjonene knyttet til denne påstanden dreier seg i stor grad om politiet og etterretningstjenestenes evne og vilje til å gjøre de rette vurderingene, med andre ord er påstandens andre del, som spesifiserer «uten rimelig grunn», et viktig premiss. På tvers av de to gruppene kan man lese en underliggende tiltro til myndighetenes evne til å vurdere hva som er rimelig grunn. Argumentasjonen rundt denne vurderingen knyttes i stor grad til trusselbildet, og særlig terrorplanlegging. Det er kun et par informanter som holder fast ved tekno-

logidiskursen i denne sammenheng, og dermed løfter et kritisk perspektiv: Hvordan kan vi være sikre på at den «rimelige grunnen» er rimelig? En informant påpeker: «Selv i de systemene som skal være nøytrale, så har man tydelige fordommer på hvem det er som begår den type kriminelle handlinger, og hvordan man da bygger opp det». De to informantene knytter problematikken særlig til algoritmestyrt overvåking av data, som kan få store negative konsekvenser for enkeltpersoner til tross for at trusselbildet gir gode grunner for å målrette mot religion, nasjonal tilhørighet eller reisemønster. Det vi ser i refleksjonene rundt enkeltpåstanden om diskriminering er at grensegangen innad i gruppene forflytter seg: Noen av de som i det store og hele argumenterer ut fra overvåkingsteknologi som «matter out of place», når i refleksjonen rundt gruppetilhørighet en grense hvor de aksepterer de potensielle ulempene for å forhindre større potensiell skade. Kun et fåtall holder fast ved perspektivet som tilsier at teknologien ikke bør brukes. Dette viser at posisjonene i debatten er flytende, og i stor grad kontekstavhengige. Til tross for at resultatet av studien viser to distinkte faktorer hvor utgangspunktet for argumentasjonen viser seg å være forskjellig, er det også et potensiale for bevegelse innad og mellom posisjonene, som sjelden kommer til syne i den offentlige debatten.

Avslutning

Resultatet av studien samsvarer overordnet med det bildet som tegnes i den offentlige debatten om overvåking, nemlig at tematikken er preget av polarisering. I den offentlige debatten finslipes argumentene slik at innleggene tar form av å bygge troverdighet for eget ståsted enten gjennom å utelate enhver usikkerhet knyttet til eget standpunkt, eller å aktivt så tvil om motstandernes argumentasjon ved å påpeke retoriske svakheter (Flinterud, 2019). At vi endte opp med to faktorer som innholdsmessig i hovedsak kunne identifiseres som argumenter for enten økt eller begrenset overvåking i det digitale rom, var som sådan ikke overraskende. I intervjuene, derimot, så vi at ståstedene balanseres og utbroderes. En-til-en-samtale ga mer rom for å balansere og utdype avveiningene som ligger bak standpunktene, og bidro til å skape en dypere forståelse av en debatt som fra utsiden kan fremstå som fastlåst og uløselig. Materialet gir et viktig innblikk i avveininger som i liten grad skinner gjennom i offentlig debatt.

Det mest påfallende resultatet var funnet av overlapp på enkelte sentrale påstander, til tross for at faktoranalysen viser to distinkte faktorer. På den ene siden tolker vi dette som et uttrykk for at debatten foregår i et fritt demokrati hvor det tross alt er bred enighet om en felles verdimelessig plattform. Uansett ståsted kan de fleste i det offentlige ordskiftet i Norge enes om universelle menneskerettigheter, ytringsfrihet og motstand mot diskriminering. Dette er begreper som overordnet kjennetegner vårt samfunns symbolske orden. På den annen side viser analysen av de kvalitative dataene at det ikke nødvendigvis er slik at personene innenfor de ulike faktorene snakker om det samme når de snakker om rettigheter og diskriminering. Vi fant blant annet en kjent distinksjon fra de senere års debatter knyttet til rettssikkerhet, hvor den ene gruppen argumenterte ut fra gjerningsmannens rettigheter og retten til å anses uskyldig til det motsatte er bevist, mens den andre gruppen argumenterte ut fra potensielle ofres rettigheter og retten til å bli beskyttet av staten mot kriminalitet og terror. Her trer den symbolske ordenens innholdsmessige tolkningsrom frem, i det to verdier i samfunnet settes opp mot hverandre, men vektet motsatt. Overordnet så vi at denne distinksjonen gjorde at de to gruppene argumenterte ut fra to forskjellige utgangspunkter. Mens den ene gruppen i hovedsak argumenterte med utgangspunkt i at økt overvåking vil kunne gjøre samfunnet mer ustabil, argumenterte den andre gruppen med at økt overvå-

king vil gjøre samfunnet sikrere. Det er med andre ord ikke de aktuelle metodene som sådan som debatteres, men heller hvilke konsekvenser digitaliseringen fører med seg, og hvordan de kan påvirke samfunnet som helhet.

Det er også verdt å reflektere over fordelingen av q-sorteringer innad i de to faktorene, som fremstår mer som spredt utover et kontinuum enn som tilhørende to motpoler. Spredningen antyder at det finnes balanserende stemmer i denne debatten, til tross for det overordnede inntrykket av polaritet. Dette underbygges i analysen av de kvalitative intervjuene, hvor vi finner både uenighet innad i faktorene, og tendenser til at informanter som lader på en faktor tar i bruk den andre faktorens språklige utgangspunkt når de kontekstualiserer enkeltpåstander. Selv om det overordnede bildet viser en debatt med to standpunkter og to tematiske utgangspunkter for å argumentere for sitt syn, så viser dataene også en underliggende fleksibilitet. Det som i tilspisset offentlig og mediert debatt fremstår som fastlåst og polarisert, får i vårt materiale mer preg av forhandling, med flere stemmer tydelig plassert i et balansepunkt. Bak den norske overvåkingsdebatten ser det ut til å være mer rom for kunnskapsbasert forhandling enn det som er tydelig på overflaten.

Referanser

- Akhtar-Danesh, N. (2018). qfactor: A command for Q-methodology analysis. *The Stata Journal*, 18(2), 432-446. DOI: <https://doi.org/10.1177/1536867x1801800209>
- Cayford, M. & Pieters, W. (2018). The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society*. 34(2), 88-103. DOI: <https://doi.org/10.1080/01972243.2017.1414721>
- Coogan, J. & Herrington, N. (2011). Q methodology: an overview. *Research in Secondary Teacher Education*, 1(2), 24-28.
- Douglas, M. (2002). *Purity and Danger. An Analysis of Concepts of Pollution and Taboo*. New York: Routledge Classics.
- EU-direktiv (2006). 24/EC of the European parliament and of the council. *Official Journal of the European Union*, 105 (54).
- Flinterud, G. (2020). 'Consequences for Society as a Whole': Narrating Technology in the Norwegian Media Debate on Online Surveillance. Sendt utgiver, under vurdering.
- Flinterud, G. og Strype, J. (2020) Dokumentasjonsnotat. <https://phs.brage.unit.no/phs-xmlui/handle/11250/2600751>
- Forsvarsdepartementet (2020). Lov om Etterretningstjenesten (etterretningstjenesteloven). Prop. 80 L (2019-2020).
- Friedewald, M., Burgess, J., Čas, J., Bellanova, R., & Peissl, W. (red.). (2017). *Surveillance, Privacy and Security*. London: Routledge. DOI: <https://doi.org/10.4324/9781315619309>
- Giddens, A. (1985). *The nation-state and violence*. Cambridge: Polity Press.
- Goold, B. J. & Lazarus, L. (Red.). (2007). *Security and Human Rights*. Oxford: Hart Publishing.
- Günther, K. (2013). Responsibility to Protect and Preventive Justice. I A. Ashworth, L. Zedner & P. Tomlin (Red.), *Prevention and the Limits of Criminal Law* (s. 69-90). Oxford: Oxford University Press.
- Haggerty, K.D. & Ericson, R.V. (2000). The Surveillant Assemblage. *British Journal of Sociology*, 51(4), 605-622. DOI: <https://doi.org/10.1080/00071310020015280>
- Horn, J. L. (1965). A rationale and test for the number of factors in factor analysis. *Psychometrika*, 30(2), 179-185. DOI: <https://doi.org/10.1007/bf02289447>
- Hudson, B. (2003). *Justice in the risk society. Challenging and re-affirming justice in late modernity*. London: SAGE Publications.

- Husabø, E. J. & Bruce, I. (2009). Fighting Terrorism through Multilevel Criminal Legislation. Security Council Resolution 1373, the EU Framework Decision on Combating Terrorism and their Implementation in Nordic, Dutch and German Criminal Law. Leiden: Martinus Nijhoff Publishers.
- Kleven, Ø. (2016). Nordmenn på tillitstoppen i Europa. *SSB: Samfunnsspeilet*, 2, 13-18.
- Lehtonen, P. & Aalto, P. (2017). Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States. *European Security*, 26(2), 207-225. <https://doi.org/10.1080/09662839.2016.1276057>
- Lomell, H. M. (2006). ' - Menneskerettigheter er vel og bra, men for hvem? Offeret eller gjerningsmannen?'. *Nordisk tidsskrift for menneskerettigheter*, 24(1), 59-73.
- Lomell, H. M. (2014). Forventinger om beskyttelse. I L. Hausken, S. R. Yazdani & T. K.-. Haagenen (Red.), *Fra terror til overvåking. Overvåking i Norge, et kritisk prospekt* (s. 39-62). Oslo: Vidarforlaget.
- Lund, K. (1996). Rapport til Stortinget fra kommisjonen som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere (Lund-rapporten).
- Lyon, D. (2003). *Surveillance after September 11*. Cambridge: Polity Press.
- Lyon, D. (2018). *The Culture of Surveillance. Watching as a Way of Life*. Cambridge: Polity Press.
- Lysne, O., Grytting, T., Jarbekk, E., Lunde, E., & Reusch, C. (2016). Digitalt grenseforsvar (DGF): Lysne II-utvalget.
- Massumi, B. (2010). The Future Birth of the Affective Fact: The Political Ontology of Threat. I: A. Bryant and G. Pollock, (red.), *Digital and Other Virtualities: Renegotiating the Image* (s.79-92). London: I.B.Tauris..
- Ramsay, P. (2012). *The insecurity state: vulnerable autonomy and the right to security in the criminal law*. Oxford: Oxford University Press.
- Rule, J. B. (1973). *Private lives and public surveillance*. London: Allen Lane.
- Schauer, F. (1978). Fear, Risk, and the First Amendment: Unravelling the 'Chilling Effect'. *Boston University Law Review*, 58, 685-732.
- Schartum, D. W. (red.) (2010). *Overvåking i en rettsstat*. Bergen: Fagbokforlaget.
- Simon, J. (2007). *Governing through crime. How the war on crime transformed American democracy and created a culture of fear*. New York: Oxford University Press.
- Stein, A. (1996). The Refoundation of Evidence Law. *Canadian Journal of Law and Jurisprudence*, 9. DOI: <https://doi.org/10.1017/s0841820900003477>
- Straffeprosessloven. (2016). Lov om rettergangsmåten i straffesaker (LOV-1981-05-22-25). Hentet fra: https://lovdata.no/dokument/NL/lov/1981-05-22-25/KAPITTEL_4-10#%C2%A7216p
- Størksen, I. (2012). Hva er Q-metodologi, og hvordan kan den brukes i psykologien. *Tidsskrift for norsk psykologforening*, 49(6), 566-570.
- Søbye, Espen (1998): Jødeforfølgelsene under den annen verdenskrig: Et mørkt kapittel i statistikkens historie? *Samfunnsspeilet* 4, 2-17
- Watts, S. & Stenner, P. (2012). *Doing Q methodological Research. Theory, Method & Interpretation*. Sage.
- Wood, D.M. (2009). The 'Surveillance Society': Questions of History, Place and Culture. *European Journal of Criminology*, 6(2), 179-194. DOI: <https://doi.org/10.1177/1477370808100545>
- Wyller, T. C. (1997). Rikets sikkerhet – og demokratiets: refleksjoner over Lund-kommisjonens rapport. *Nytt norsk tidsskrift*, 14, 3, 203-215.