# Dokumentasjonsnotat for «Taking surveillance apart? Accountability and Legitimacy of Internet Surveillance and Expanded Investigatory Powers» WP 2: Stakeholders articulating surveillance and privacy

Innhold

[Anonymisert oversikt over informanter og yrkestilhørighet 2](#_Toc38889445)

[En kort beskrivelse av Q-metodologi 3](#_Toc38889446)

[Referanser 3](#_Toc38889447)

[Påstander sortert i Q-intervjuene 4](#_Toc38889448)

[STATA-syntaks (krever installasjon av *qfactor* i STATA) 6](#_Toc38889449)

[Tabell A1. Rotert faktorladningsmatrise 7](#_Toc38889450)

[Tabell A2. Z-skårer og korresponderende verdier i de typiske sorteringene 8](#_Toc38889451)

«Taking Surveillance Apart? Accountability and Legitimacy of Internet Surveillance and Expanded Investigatory Powers» er et internasjonalt samarbeidsprosjekt mellom Politihøgskolen i Norge, Politihøgskolen i Finland, universitetet i Dundee og universitetet i Edinburgh. Prosjektet ledes av universitetet i Dundee.

Dokumentasjonsnotatet samler resultater fra den norske studien av hvordan interessenter i overvåkningsdebatten artikulerer sine standpunkter. For nærmere informasjon om studien, ta kontakt med Guro Flinterud, guro.flinterud@phs.no.

Se også prosjektets nettside: <https://sites.dundee.ac.uk/eyes-online-project/>

## Anonymisert oversikt over informanter og yrkestilhørighet

Informantene i studien er lovet anonymitet. Yrke er derfor oppgitt i overordnede kategorier.

**Offentlig sektor** = Ansatte i statlige eller kommunale virksomheter som jobber direkte med overvåkningstematikk

**Interesseorganisasjon** = Ansatte som jobber for ulike typer organisasjoner hvor statlig overvåkning er et sentralt tema

**Politietaten** = Ulike typer ansatte på ulike nivåer i politietaten og PST, også ansatte uten politifaglig utdanning.

**Politikk** = Politikere som jobber med temaer knyttet til statlig overvåkning

**Akademia** = Ansatte i Universitets- og høgskolesektoren, ulike fagbakgrunner

**Privat sektor** = Ansatte i teknologibransjen og advokatbransjen med arbeidsoppgaver som er relevant for overvåkningstematikk

|  |  |
| --- | --- |
|  | **Yrkeskategori** |
| qsort1 | Offentlig sektor |
| qsort2 | Interesseorganisasjon |
| qsort3 | Politietaten |
| qsort4 | Interesseorganisasjon |
| qsort5 | Politietaten |
| qsort6 | Offentlig sektor |
| qsort7 | Akademia |
| qsort8 | Politikk |
| qsort9 | Interesseorganisasjon |
| qsort10 | Offentlig sektor |
| qsort11 | Akademia |
| qsort12 | Privat sektor |
| qsort13 | Privat sektor |
| qsort14 | Privat sektor |
| qsort15 | Privat sektor |
| qsort16 | Interesseorganisasjon |
| qsort17 | Politikk |
| qsort18 | Politietaten |
| qsort19 | Politikk |
| qsort20 | Akademia |
| qsort21 | Offentlig sektor |
| qsort22 | Politietaten |
| qsort23 | Politietaten |
| qsort24 | Politietaten |
| qsort25 | Politietaten |

## En kort beskrivelse av Q-metodologi

Q-metodologi er en forskningsmetode som gir både kvantitative og kvalitative data. Metoden tar sikte på å skape dypere forståelse av mønstre av enkeltstandpunkter hos individer heller enn å avdekke hvordan holdninger fordeler seg mellom individer i en befolkning (Coogan & Herrington, 2011, s. 24). Metoden blir i dag ofte brukt for å kartlegge holdninger blant interessenter til et spesifikt tema, og kan særlig være et godt verktøy for å fange nyansene i saker som framstår som polariserte (Lehrer & Sneegas, 2018).

Forskningsprosessen i Q-metodologi er delt i flere hoveddeler:

Forskeren identifiserer først studiens «concourse», som kan defineres som universet av mulige påstander om et tema (Watts & Stenner, 2012, s. 34). Den vanligste framgangsmåten for å identifisere dette universet av påstander er gjennom analyse av alle tilgjengelige dokumenter om det valgte temaet, hvor forskeren noterer seg alle mulige utsagn om problematikken.

Deretter jobbes det med å tematisere påstandene til man til slutt står igjen med 40-60 påstander som representerer de mest sentrale aspektene ved debatten. Disse 40-60 påstandene utgjør Q-utvalget (McKeown & Thomas, 2013, s.3).

Neste del av prosessen er Q-intervjuet. Dette intervjuet består av to deler, en sorteringsøvelse (Q-sortering) hvor intervjuobjektet får utdelt en bunke kort med de utvalgte påstandene som skal sorteres i forhold til hverandre fra mest enig til mest uenig, og deretter et kvalitativt intervju med utgangspunkt i sorteringen og påstandene.

Resultatene fra sorteringen analyseres ved hjelp av Q-faktoranalyse. Til forskjell fra ordinær faktoranalyse som identifiserer strukturer i et variabelsett, innebærer Q-faktoranalyse å finne underliggende grupperinger av individer (Q-sorteringer) i studien (McKeown & Thomas, 2013, s. 51). Med andre ord: Q-faktoranalyse søker å identifisere grupperinger av Q-sorteringer som ligner hverandre. Det som da framtrer kan ses som generaliserte synspunkter i grupper (McKeown & Thomas, 2013, s. 7).

Faktoranalyse innebærer, både i tradisjonell forstand og innen Q-metodologien, å gjøre en del valg for å finne den mest hensiktsmessige faktorstrukturen i et datamateriale. Det helt sentrale valget dreier seg hvor mange faktorer som kan og bør trekkes ut av datamaterialet. Watts & Stenner (2012) understreker at selv om det i den Q-metodologiske faktoranalysen er få riktige og gale valg, trenger forskeren «a simple desire to find a sound and workable solution that (…) is methodologically and statistically, as well as theoretically, acceptable» (Watts & Stenner, 2012, s. 96).

Det siste skrittet i den kvantitative delen av analysen innebærer å identifisere typiske Q-sorteringer for hver faktor (Watts & Stenner, 2012, s. 140; Størksen, 2012, s. 568). Denne operasjonen kan utføres av statistikkprogrammet og resulterer i sorteringer med samme format som de individuelle sorteringene, men som representerer det som er typisk for sorteringene innad i hver faktor. For en teknisk beskrivelse av hvordan typiske Q-sorteringer konstrueres, se Watts & Stenner (2012, s. 129-141).

### Referanser

Coogan, J. & Herrington, N. (2011). Q methodology: an overview. *Research in Secondary Teacher Education*, *1*(2), 24-28.

Lehrer, N. & Sneegas, G. (2018). Beyond polarization: using Q methodology to explore stakeholders’ views on pesticide use, and related risks for agricultural workers, in Washington State’s tree fruit industry. *Agriculture and human values, 35*(1), 131-147.

McKeown, B., & Thomas, D. B. (2013). *Q methodology* (Vol. 66). Sage publications.

Watts, S. og Stenner, P. (2012) *Doing Q methodological Research. Theory, Method & Interpretation.* Sage Publishers.

## Påstander sortert i Q-intervjuene

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.
2. Forespørsler om informasjon fra politiet og etterretningstjenestene er en urimelig byrde for internett-tilbydere.
3. Data fra overvåkning på nett bør slettes umiddelbart etter at saken er avsluttet, og bør ikke brukes til andre formål enn det ble samlet inn for.
4. Nye overvåkningsmetoder innføres gradvis, hvilket skjuler totaliteten av endringene over tid.
5. Overvåkningsmetodene som er mest inngripende i privatlivet, slik som dataavlesning, bør være forbehold den mest alvorlige kriminaliteten eller alvorlige trusler mot rikets sikkerhet.
6. For sikre verdifull informasjon om trusler mot rikets sikkerhet må vi styrke vårt internasjonale samarbeid.
7. Å utvide myndighetenes tilgang til kommunikasjon på nett vil gjøre samfunnet tryggere for borgerne
8. Radikaliserte som står i fare for å bli voldelige bør identifiseres gjennom sin atferd på nett, og kommunikasjonen deres bør overvåkes.
9. Et digitalt grenseforsvar er nøyaktig og pålitelig måte å avdekke informasjon om hittil ukjente trusler mot rikets sikkerhet
10. Dagens kriminalitets- og trusselbilde gjør det nødvendig å utvide myndighetenes tilgang til overvåkning i cyberspace.
11. Hvis du ikke har noe å skjule, trenger du heller ikke bekymre deg for myndighetenes overvåkning.
12. Vi bør kun dele og motta etterretning fra land som følger FNs menneskerettighetskonvensjon.
13. Tradisjonelle (offline) overvåkningsmetoder har avslørt hva mennesker gjør, mens tilgang til kommunikasjon i det digitale rom avslører hva mennesker tenker. Det er en fundamental forskjell i hvor inngripende de to handlingene er.
14. Målrettingen av overvåkningsmetoder 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.
15. Til tross for gjeldende privilegier bør også kommunikasjonen til yrker som journalist, advokat og lege bli gjenstand for overvåkning dersom de kommuniserer med mennesker som utgjør en fare for rikets sikkerhet.
16. Det er essensielt at alle mennesker gis de samme grunnleggende rettighetene på nett som de har i livet ellers.
17. Hvis vi øker den digitale overvåkningen som følge av terrorhandlinger, svekker vi de idealene terroristene går til angrep på.
18. 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.
19. Vi må begrense hvilke tilganger til overvåkning vi tillater dagens myndigheter å ha, fordi vi ikke kan kontrollere hvordan disse tilgangene kan bli brukt av fremtidige myndigheter.
20. Etterretningstjenestene har for stor tiltro til effektene av å overvåke av digital kommunikasjon.
21. Å overvåke grensekryssende nettverkskommunikasjon er mer akseptabelt enn å overvåke innenlandskommunikasjon.
22. Digitalt grenseforsvar er basert på filtrering av data mot spesifikt angitte parametere før det sendes til analyse, derfor er det målrettet overvåkning, ikke masseovervåkning.
23. Media har for stor innflytelse på folkeopinionen når det gjelder overvåkning på nett.
24. De statlige myndighetene vil få de tilgangene de vil ha uavhengig av debatten.
25. Det gjeldende forslaget om Digitalt grenseforsvar treffer den rette balansen mellom sikkerhet og personvern.
26. Inngrepet i personvernet skjer allerede når data samles inn og lagres, det trenger ikke å bli sett på.
27. Kriminelle vil alltid finne måter å omgå overvåkning på nett, for eksempel ved å flytte til internett-tilbydere i andre, mindre regulerte land.
28. Teknologien utvikler seg så raskt at myndighetene og lovgivningen ikke klarer å holde tritt.
29. Hvis befolkningen synes det er greit at personvernet innskrenkes til fordel for sikkerhet, så er det fordi de ikke fullt ut forstår hvorfor personvern er så viktig i den digitale tidsalder.
30. Det er ingen forskjell mellom innholdsdata og metadata når det gjelder inngrep i personvernet.
31. I saker som gjelder rikets sikkerhet bør lovgivningen knyttet til overvåkning på nett bestemmes av vårt eget storting, ikke av overnasjonale organer, som EU.
32. Borgere bør informeres i etterkant hvis deres kommunikasjon på nett har blitt sett på, lagret eller brukt i etterforskning.
33. Stordataanalyse av kommunikasjon på nett vil føre til dårlige avgjørelser om individer gjennom feilvurderinger og antagelser.
34. Data fra internett bør lagres av tilbyderne i 12 måneder slik at potensialet for etterforskning er utnyttet til fulle.
35. Målrettet overvåkning blir masseovervåkning hvis den også fanger opp data fra individer som ikke kommuniserer direkte med den mistenkte.
36. Publikum bør informeres om utbredelse og utfall av overvåkning på nett tilstrekkelig ofte og detaljert, for å opprettholde publikums tillit til politi og myndigheter og unngå mistanke om at overvåkningen er mer vidtrekkende enn den faktisk er.
37. Den preventive effekten av et digitalt grenseforsvar veier opp for de antatte finansielle og samfunnsmessige kostnadene
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.
39. Uavhengige kontrollmekanismer er en bedre måte å beskytte rettighetene våre, enn å forsøke å begrense eller fjerne tilganger fra myndighetene.
40. Lovgivningen knyttet til etterretning og digital overvåkning er så tvetydig og fragmentert at den er vanskelig å forstå og åpen for bred fortolkning.
41. Domstolene bør foreta en selvstendig og uttømmende vurdering for hver begjæring om tilgang til overvåkning, og ikke kun legge begjærende myndighets vurdering til grunn.
42. Godkjenningsprosesser i forbindelse med søk i et digitalt grenseforsvar bør ikke bare involvere dommeren og en representant fra e-tjenesten, men også en uavhengig representant som skal ivareta hensynet til allmennheten, for å sikre at rettighetene og interessene til de som plasseres under overvåkning blir opprettholdt.
43. Godkjenning av bruk av spionprogramvare bør inkludere en analyse av mulig skade som programmet kan gjøre på datasystemet eller prosessen det kontrollerer, i tillegg til en troverdig beskrivelse av hvordan programmet kan fjernes uten å medføre fare.
44. Personale på alle nivåer i etterretningstjenesten bør være garantert en anonym og uavhengig rettslig kanal for å rapportere misbruk av tvangsmidler, som ikke vil medføre en risiko for dem selv eller rikets sikkerhet.
45. Godkjenningsprosessene knyttet til overvåkning på nett kan medføre risiko ved at viktig etterforskning eller etterretning hindres eller forsinkes.

## STATA-syntaks (krever installasjon av *qfactor* i STATA)

Generell syntaks:

 qfactor varlist [if] [in] , nfactor(#) [extraction(string)

 rotation(string) transpose(string) statement(string)

 score(string) esize(string) bipolar(string)]

(se help qfactor for oversikt over opsjoner)

Q-analyse: kun defaultopsjoner og 2 faktorer:

qfactor qsort1 qsort2 qsort3 qsort4 qsort5 qsort6 qsort7 ///

qsort8 qsort9 qsort10 qsort11 qsort12 qsort13 qsort14 ///

qsort15 qsort16 qsort17 qsort18 qsort19 qsort20 qsort21 ///

qsort22 qsort23 qsort24 qsort25 , nfactor(2)

Horns parallel-analyse: (Horn, 1965)

fapara, pca reps(10)

## Tabell A1. Rotert faktorladningsmatrise

|  |  |  |
| --- | --- | --- |
| **Q-sort nr.** | **F1** | **F2** |
| 9 | **0.8780** | -0.0890 |
| 15 | **0.8496** | -0.0317 |
| 10 | **0.8345** | 0.0842 |
| 11 | **0.8041** | -0.0361 |
| 14 | **0.8022** | -0.1927 |
| 2 | **0.7700** | 0.0582 |
| 20 | **0.7523** | 0.0764 |
| 16 | **0.7252** | 0.2950 |
| 21 | **0.6996** | 0.2071 |
| 19 | **0.5895** | 0.2506 |
| 12 | **0.5451** | 0.2242 |
| 17 | 0.5435 | 0.4722 |
| 22 | 0.5140 | 0.4731 |
| 7 | 0.4757 | 0.4551 |
| 4 | **0.4513** | 0.2754 |
| 1 | **0.4424** | 0.2006 |
| 18 | 0.1056 | **0.7923** |
| 3 | 0.1811 | **0.7911** |
| 8 | 0.0425 | **0.7624** |
| 23 | 0.1113 | **0.7522** |
| 5 | -0.0008 | **0.7354** |
| 24 | 0.0313 | **0.6689** |
| 25 | -0.0860 | **0.6494** |
| 13 | 0.2584 | **0.5511** |
| 6 | 0.3625 | 0.4179 |

## Tabell A2. Z-skårer og korresponderende verdier i de typiske sorteringene

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Utsagn nr.** | **zscore1** | **F\_1** | **zscore2** | **F\_2** |
| 1 | 1,440 | 5 | -0,375 | -1 |
| 2 | -1,050 | -3 | -1,670 | -4 |
| 3 | 0,755 | 2 | -0,827 | -3 |
| 4 | 1,070 | 3 | -0,267 | 0 |
| 5 | 1,210 | 3 | 1,560 | 4 |
| 6 | 0,425 | 0 | 1,200 | 3 |
| 7 | -0,407 | -1 | 1,470 | 4 |
| 8 | -0,615 | -2 | 0,342 | 1 |
| 9 | -1,620 | -4 | -0,286 | 0 |
| 10 | -0,048 | 0 | 1,370 | 3 |
| 11 | -1,970 | -5 | -0,391 | -1 |
| 12 | -0,091 | -1 | 0,039 | 0 |
| 13 | 0,115 | 0 | -1,130 | -3 |
| 14 | 1,700 | 5 | 1,910 | 5 |
| 15 | -1,470 | -3 | -0,807 | -2 |
| 16 | 1,380 | 4 | 1,920 | 5 |
| 17 | 0,955 | 3 | -0,655 | -1 |
| 18 | 1,410 | 4 | -0,752 | -2 |
| 19 | 0,737 | 2 | -0,840 | -3 |
| 20 | 0,030 | 0 | -0,803 | -2 |
| 21 | -0,697 | -2 | -1,160 | -4 |
| 22 | -1,630 | -4 | 0,589 | 1 |
| 23 | -1,050 | -3 | 0,749 | 2 |
| 24 | -0,894 | -2 | -1,910 | -5 |
| 25 | -1,570 | -4 | -0,122 | 0 |
| 26 | 0,717 | 2 | -0,692 | -2 |
| 27 | 0,096 | 0 | -0,464 | -1 |
| 28 | 0,238 | 0 | 1,140 | 3 |
| 29 | 0,552 | 1 | -1,140 | -4 |
| 30 | -1,000 | -2 | -2,010 | -5 |
| 31 | -0,471 | -1 | 0,881 | 3 |
| 32 | 0,315 | 0 | -0,375 | -1 |
| 33 | 0,493 | 1 | -0,819 | -2 |
| 34 | -1,420 | -3 | 0,727 | 2 |
| 35 | -0,092 | -1 | -0,848 | -3 |
| 36 | 0,474 | 1 | 0,007 | 0 |
| 37 | -1,650 | -5 | 0,457 | 1 |
| 38 | 1,360 | 4 | 1,490 | 4 |
| 39 | -0,659 | -2 | 0,857 | 2 |
| 40 | 0,427 | 1 | -0,366 | 0 |
| 41 | 1,080 | 3 | 0,535 | 1 |
| 42 | 0,663 | 2 | -0,031 | 0 |
| 43 | 0,490 | 1 | 0,293 | 1 |
| 44 | 0,726 | 2 | 0,590 | 2 |
| 45 | -0,447 | -1 | 0,626 | 2 |