PÅ NETT MED PUBLIKUM

Hvordan smarttelefonen og sosiale medier
gir nye muligheter for norsk politi

Teknologirådet

PÅ NETT MED PUBLIKUM

– HVORDAN SMARTTELEFONEN OG SOSIALE MEDIER GIR NYE MULIGHETER FOR NORSK POLITI

ISBN 978-82-92447-68 – 0 (trykket utgave)
ISBN 978-82-92447-69 – 7 (elektronisk utgave)

Rapport nr. 2 2014
Utgitt: Oslo, august 2014
Omslag: Birgitte Blandhoel
Trykk: ILAS Grafisk
Elektronisk publisert på: www.teknologiradet.no

FORORD

Norsk politi går en svært spennende tid i møte. Svakheter og mangler som ble avdekket i kjølvannet av 22. juli 2011, har gitt oss et solid grunnlag for utformingen av fremtidens politi. Nå er norsk politi inne i en omfattende og historisk viktig endringsprosess.

Mye har skjedd i samfunnet for øvrig siden politiet sist var gjenstand for så omfattende endringer. I dag har 3 av 4 nordmenn en smarttelefon. Vi har den med oss overalt og bruker den til å dele tekst, bilder, video og ikke minst kommunisere med hverandre på sosiale medier. (Og selvfølgelig også til å ringe!).

Denne rapporten tar for seg de muligheter dette gir oss på beredskapsfeltet. Hvordan kan nettverket av publikums smarttelefoner brukes til å styrke politiets situasjonsforståelse når det virkelig gjelder? Kan vi få et tettere samspill mellom politi og publikum? Hvilke valg må vi ta for å ivareta balansen mellom sikkerhet og åpenhet?

I ekspertgruppen har vi hatt med oss:

- *Gise Hannemyr*, universitetslektor, Institutt for informatikk, UiO
- *Håkon Wium Lie*, CTO, Opera Software (og medlem i Teknologirådet)
- *Silvija Seres*, CEO, TechnoRocks (og medlem i Teknologirådet)
- *Inger-Marie Sunde*, førsteamanuensis, Politihøgskolen

Teknologirådets prosjektledere Hilde Lovett og Robindra Prabhu har ledet prosjektet, som er delfinansiert av Justis- og beredskapsdepartementet.

Teknologirådet skal gi uavhengige råd til Stortinget og øvrige myndigheter i viktige teknologispørsmål, og legge til rette for en åpen, offentlig debatt om viktige dilemmaer. Denne rapporten er den første i en serie på tre rapporter som utforsker hvordan ny teknologi kan endre politiarbeidet, men også utfordre grensene mellom sikkerhet og åpenhet. Vi håper denne rapporten kan bidra til en offensiv og nyansert debatt om politiets nye muligheter.

Tore Tennøe
Direktør, Teknologirådet

INNHOLD

1. SAMMENDRAG OG ANBEFALINGER 6

1.1 DET DIGITALE SAMSPILLET MELLOM POLITI OG PUBLIKUM 7

1.2 POLITIET MÅ UTNYTTE AT DE FLESTE HAR EN SMARTTELEFON 8

1.3 SOSIALE MEDIER SOM INFORMASJONSKILDE FOR POLITIET 12

2. POLITIETS NYE MULIGHETER 15

2.1 PUBLIKUM ER VILLIGE TIL Å DELE 16

2.2 POLITISK AKTUALITET 17
2.2.1 22. juli-kommisjonen 17
2.2.2 Politianalysen 18
2.2.3 Justiskomitéens innstilling til terrormeldingen 18

2.3 MÅL OG AVGRENSNINGER FOR RAPPORTEN 19
2.3.1 Tre rapporter om teknologi i politiet 19
2.3.1 Avgrensninger 20

3. DIGITALE NØDMELDINGER OG TIPS 21

3.1 STYRKET SITUASJONSFORSTÅELSE 23
3.1.1 Digitale bilder: Mer informasjon 23
3.1.2 Bildemosaikk: bedre oversikt 25
3.1.3 GPS: Presis lokalisering 26
3.1.4 Kartlegging: Forstå situasjonsforløpet 27
3.1.5 Bevegelse av store menneskemengder 28

3.2 ET NYTT SAMSPILL MELLOM POLITI OG PUBLIKUM 30

3.3 112 SOM APP: EN NY KONTAKTFLATE MOT PUBLIKUM 31
3.3.1Tilrettelegging for smarttelefon 32
3.3.2 Tidligere og pågående tiltak i politiet 33

3.4 HÅNDTERING AV INFORMASJONSFLOMMEN 35
3.4.1 Vil politiet klare å ta i mot og bruke informasjonen? 35
3.4.2 Er det plass i nettet? 37
3.4.3 Manipulert informasjon 38

3.5 KRAV TIL INFORMASJONSHÅNDTERING 39

3.5.1 Håndtering av personsensitiv informasjon 39
3.5.2 Anonymisering 39

3.6 PERSONVERN OG ÅPENHETSHENSYN 40
3.6.1 Håndtering av overskuddsinformasjon 40
3.6.2 Et nytt overvåkningsregime? 41

4. POLITIET I SOSIALE MEDIER 44

4.1 PASSIV TILSTEDEVÆRELSE: OVERVÅKING AV SOSIALE MEDIER 47
4.1.1 Tidlig varsling 47
4.1.2 Situasjonsforståelse: raskt overblikk 50
4.1.3 Identifisere nye vitner 50
4.1.4 Eksempel: 22. juli 2011 på Twitter 51

4.2 AKTIV TILSTEDEVÆRELSE: KOMMUNIKASJON MED PUBLIKUM 54
4.2.1 Korrigere informasjon 54
4.2.2 Engasjere publikum 57
4.2.3 Forutsetninger for god dialog gjennom sosiale medier 60

4.3 UTFORDRINGER OG BEGRENSNINGER 61
4.3.1 Kan politiet stole på sosiale medier? 61
4.3.2 Verifisere og kvalitetssikre 62

4.4 PERSONVERN OG ÅPENHET 63
4.4.1 Eksponering og forhåndsdømming 63
4.4.2 Personsensitiv informasjon 64
4.4.3 Får vi en nedkjølingseffekt? 64
4.4.6 Retningslinjer for politiet på sosiale medier 69

5. REFERANSELISTE 72

Dokumenter fra nasjonale myndigheter 72
Publikasjoner 73
Omtalte nettsider 73

1. SAMMENDRAG OG ANBEFALINGER

Nordmenn er på verdenstoppen i bruk av smarttelefonen og sosiale medier. Denne infrastrukturen drar ikke politiet nytte av i dag. Publikum kan være en kilde til detaljert og oppdatert informasjon som kan gi politiet bedre situasjonsforståelse og beslutningsgrunnlag ved ulykker og kriminalitet.

Norsk politi er inne i sin viktigste og mest omfattende moderniseringsprosess i nyere tid. Både rapporten fra 22. juli-kommisjonen[1] og Politianalysen[2] gir grundige beskrivelser av tilstanden i norsk politi, og begge er tydelige på at en bedre utnyttelse av IKT og moderne teknologi er en viktig "nøkkel til bedre beredskap i fremtiden"[3].

Nå skal norsk politi endres og rustes for fremtidens utfordringer, og dokumenterte svakheter skal utbedres. "Endringsprogrammet" skal følge opp forbedringstiltak som har blitt lagt frem i kjølvannet av 22. juli. "Merverdiprogrammet" skal gi norsk politi det nødvendige IKT-løftet som gjør organisasjonen til en moderne informasjonsvirksomhet.

[1] NOU 2012:14, "Rapport fra 22. juli -kommisjonen"
[2] NOU 2013:9, "Ett politi – rustet til å møte fremtidens utfordringer"
[3] NOU 2012:14, "Rapport fra 22. juli-kommisjonen", s. 455

1.1 DET DIGITALE SAMSPILLET MELLOM POLITI OG PUBLIKUM

Den overordnede målsettingen for endringsarbeidet er å gi politiet bedre forutsetninger for å løse sine oppgaver og levere bedre polititjenester til publikum. Samtidig er teknologien med på å endre publikums forventninger til politiet.

I løpet av få år har ny teknologi forandret måten vi kommuniserer med hverandre på. Smarttelefonen er blitt uunnværlig for svært mange, og sosiale medier er en viktig arena i det offentlige ordskiftet. Folk kommunisere gjennom bilder, video og tekst. Med det følger også en forventning om at kontakten med politiet skal kunne skje gjennom de teknologiske verktøyene vi bruker til daglig, på en måte som også utnytter de mange mulighetene teknologien tilbyr.

Dette har konsekvenser for hvordan fremtidens nærpoliti vil kunne kommunisere og samhandle med publikum. I dag skjer denne kommunikasjonen hovedsakelig via taleanrop. Samtidig har publikum aldri vært bedre rustet til å bistå politiet med viktig informasjon, som i sin tur kan gi:

- **Kortere responstid**, gjennom tilgang til presis stedsangivelse og rettidig informasjon fra publikum.
- **Bedre situasjonsforståelse,** gjennom bl.a. bilder og video fra publikum, som særlig kan bidra til å styrke situasjonsforståelsen før politiet selv er på stedet. Dette gir i sin tur **forbedret responskvalitet**, og bedre forutsetninger for god **samhandling og koordinering** politiet og nødetatene imellom.
- **Tettere kontakt med publikum**, gjennom en bredere kontaktflate mot publikums digitale hverdag.

Smarttelefonen og sosiale medier er sammen sterke endringsdrivere i samfunnet, og gir opphav til nye informasjonskilder som politiet kan ha stor nytte av. Samtidig må nye muligheter veies opp mot hensynet til personvernet og mulige konsekvenser for et fritt og åpent samfunn. Det blir viktig å trekke grensene for hvor langt politiet skal få gå i bruken av slik informasjon.

Denne rapporten tar sikte på å dekke en blindsone i de endringsprosesser som alt er iverksatt, og forhindre at publikum forblir en uforløst ressurs. Samtidig

søker rapporten hele tiden å veie nye muligheter opp mot hensynet til åpenhet og personvern.

1.2 POLITIET MÅ UTNYTTE AT DE FLESTE HAR EN SMARTTELEFON

Publikum har med seg telefonen overalt og er ofte først på åstedet. Smarttelefonen er ikke bare en telefon, men også en datamaskin med en rekke sensorer. Dermed kan publikum levere detaljert digital informasjon til politiet tett opp til en hendelse, i form av f.eks. bilder, video og tekst med presis tids- og stedsangivelse.

Digitale nødmeldinger og tips er en naturlig modernisering av dagens talebaserte nødtelefon. Slik kan publikum bidra til å styrke politiets situasjonsforståelse og gi viktige opplysninger som ville kunne gått tapt i en muntlig beskrivelse. Samtidig utvider smarttelefonen mulighetene for samhandling mellom politi og publikum både før og etter en hendelse har inntruffet

For publikum kan digital informasjon fra smarttelefonen brukes i minst tre ulike sammenhenger:

- **"Føre var"**: Muligheten til frivillig deling av bl.a. presise lokasjonsdata med nødetatene gir publikum helt nye måter å redusere risiko for egen sikkerhet, både når man er alene (f.eks. på fjelltur) eller befinner seg på steder med mange mennesker.

- **"Rop om hjelp"**: Når ulykken først er ute, og tale er uaktuelt eller vanskelig, åpner smarttelefonen for kommunikasjon gjennom bl.a. tekst, bilder og video. Samtidig kan viktig informasjon som lokasjon og helsedata oversendes nødetatene automatisk.

- **"Øyenvitne"**: Er publikum vitner til en hendelse kan bilder, video og lydopptak raskt og enkelt dokumentere situasjonen og situasjonsforløpet.

Når mange bidrar med slike data, kan den samlede informasjonsmengden sammenstilles på svært interessante måter som bl.a. kan gi politi- og nødetater:

- hurtig tilgang til kritisk viktig informasjon
- bedre og mer presis oversikt over en situasjon
- muligheten til å kartlegge og følge situasjonsforløpet mens hendelsen utfolder seg og kommunisere med publikum på stedet underveis

Både isolert betraktet og satt i større sammenheng, kan informasjon fra publikum være med på å styrke situasjonsforståelsen der det skjer, når det skjer. Ettersom de fleste bruker smarttelefonen i hverdagen, er det både nyttig og viktig å koble dette eksisterende sensornettverket til politiets- og nødetatenes systemer.

Teknologirådet anbefaler derfor at det legges til rette for at publikum skal kunne sende digitale nødmeldinger og tips i Norge, og at politiet bruker slik informasjon i sitt arbeid. Det innebærer noen tekniske utfordringer, men krever også klare retningslinjer for informasjonshåndtering og bruk. Det er viktig at et nytt samspill mellom politi og publikum ikke bidrar til et utilsiktet overvåkningsregime.

Det bør utvikles en nød-app for smarttelefoner i Norge

Nødetatene bør tilby en offentlig nød-applikasjon for smarttelefoner og andre mobile enheter som gjør det enkelt og trygt for publikum å rapportere hendelser til nødetatene. Det må være mulig å dele presis stedsinformasjon, samt å kommunisere via tale, tekst, direktemelding (”instant messaging”), bilder og video. Det bør også vurderes om applikasjonen automatisk skal kunne sende inn profildata med for eksempel navn, medisinsk informasjon, pårørende og deres kontaktopplysninger.

Politiet må kunne ta i mot og behandle digitale nødmeldinger og tips fra publikum, med informasjon i form av bl.a. bilder, video og GPS-posisjon

I dag foregår all kommunikasjon mellom publikum og nødmeldesentralene via taleanrop. I en nødsituasjon er det ikke tilrettelagt for å sende inn digital informasjon som bilder, video og GPS-posisjon til nødetatene. Samtidig viser Teknologirådets spørreundersøkelse at 77 prosent sier seg villig til å dele bil-

der og video fra mobilen for å styrke politiets situasjonsforståelse i en hendelse[4].

For at både politi og publikum skal kunne dra nytte av en offentlig nød-app, er det viktig at pågående fornyingsprosesser som skal levere nye IKT-systemer til politiet og nødetaten er tilrettelagt for mottak, behandling og bruk av digitale nødmeldinger og tips fra publikum.

Justis- og beredskapsdepartementet har besluttet at SMS-varsling skal innføres for døve og hørselshemmede innen utgangen av 2014, med mulig utvidelse for hele befolkningen. Varslingstjenesten skal knyttes til nødnettleveransen.

En slik tjeneste er et steg i riktig retning, men ambisjonen må være en mye bredere utnyttelse av de mange mulighetene publikums smarttelefoner gir beredskapsarbeidet. Dette betyr at nødmeldesentralene må være rustet til å ta i mot, behandle og bruke også annen digital informasjon fra publikum, som f.eks. GPS-lokasjon, bilder og video. Det er viktig at nødnettleveransen ikke begrenser mulighetene for slik informasjonsdeling og samhandling mellom politi og publikum på sikt.

Justis- og beredskapsdepartementet bør redegjøre for hvordan de nye IKT-løsningene ved nødetatenes sentraler skal tilpasses for å støtte andre former for kommunikasjon med publikum enn tale og SMS, slik som f.eks. chat, bilder, video og lydopptak.

Tilrettelegging for mottak av slik informasjon må ikke bare ses i lys av en nødmeldetjeneste, men også gi publikum anledning til å styrke politiets situasjonsforståelse gjennom digitale tips ved behov. Det er viktig at arbeidet med å avklare hvilke tilpasninger som er nødvendige gjøres så tidlig som mulig og ikke utsettes til etter en eventuell ferdigstillelse av nødnettet.

Digitale nødmeldinger og tips må være gratis, tilgjengelig for alle, og ha prioritet i nettet

Det er viktig at en nye nødmeldetjenester gjøres tilgjengelig og anvendbare for alle. Bred tilgjengelighet hos publikum er også en forutsetning for at politiet

[4] Spørreundersøkelse med 100 respondenter i aldersgruppen 15 år og oppover gjennomført av Norstat i mars 2014 på oppdrag fra Teknologirådet for å undersøke publikums holdninger til kommunikasjon og informasjonsdeling med politiet gjennom smarttelefonen og sosiale medier.

skal høste gevinst i form av styrket situasjonsforståelse ved både mindre og større hendelser.

SMS-varsling skal innføres for døve og hørselshemmede i Norge innen utgangen av 2014. Det er viktig at selv en slik begrenset utvidelse av nødmeldetjenesten ikke bare gjøres tilgjengelig for døve og hørselshemmede.[5] Digital kommunikasjon med nødetatene gjennom f.eks. SMS, chat, bilder og video er en nyttig tjeneste for alle og bør derfor gjøres åpen for hele befolkningen.

På samme måte som nødanrop i dag er gratis, bør også digitale nødmeldinger og tips være gratis å sende.[6] Digitale nødmeldinger må også gis tilstrekkelig prioritet i nettet.

Politiet må utvikle klare retningslinjer for hvordan og hvor lenge digitale meldinger fra publikum skal kunne brukes

Digitale meldinger fra publikum er frivillig sendt og inneholder lukket informasjon som kun er tiltenkt politiet. Samtidig kan bilder eller video inneholde mer informasjon enn avsenderen er klar over.

Når publikum får anledning til å sende digitale nødmeldinger og tips til politiet, vil politiet kunne få en mye større informasjonsrikdom enn i dag. Slik digital informasjon vil også enklere kunne søkes i, sammenstilles og analyseres av datamaskiner enn dagens taleanrop fra publikum. For at politiet skal kunne opprettholde en høy tillit hos publikum, er det viktig med klare retningslinjer for bruk av innsendt informasjon. Retningslinjene bør være åpent tilgjengelige og svare på følgende spørsmål:

- Hvordan sikres innholdet i nødmeldinger og tips mot utilsiktet bruk, både ved innsending og ved lagring?
- Hvilke elementer av en melding lagres og hvor lenge lagres de?
- Hvordan kan meldingene brukes videre og kobles til annen informasjon, og hvor lenge skal dette kunne gjøres før meldingene slettes?
- Hvordan brukes overskuddsinformasjon?

---

[5] http://www.tv2.no/2014/06/11/nyheter/nodnett/5687506

[6] "Anrop til nødetatenes nødmeldingstjeneste bør kunne foretas uten vederlag og uten bruk av mynt, kort, kode eller annet tilgangsmiddel." Ekomloven: http://www.lovdata.no/all/tl-20030704-083-002.html#2-6

Gjennom en slik åpen og transparent avtale med publikum kan politiet skape tillit til at personvernet og rettssikkerheten til både avsender og personer som er identifiserbare i nødmeldingene blir ivaretatt.

1.3 SOSIALE MEDIER SOM INFORMASJONSKILDE FOR POLITIET

Nordmenn er aktive brukere av sosiale medier. Hele 80 prosent oppgir å være medlem av et sosialt nettverk[7], samtidig som 65 prosent av norske nettbrukere oppgir at de bruker sosiale medier i løpet av en dag.[8] Sosiale nettsteder blir et stadig viktigere kommunikasjonsmedium for folk, også i det offentlige ordskiftet. Som terrorangrepene 22. juli 2011 også viste, sprer informasjon seg raskt i sosiale medier, og en god del av den er åpen for alle – også for politiet.

Mange kommersielle aktører har fått øynene opp for mulighetene som ligger i sosiale medier, og det utvikles stadig nye verktøy for innsamling og analyse av store mengder slik informasjon. Dette åpner også nye muligheter for politiet.

Ved større og mindre hendelser kan delvis automatisert overvåking av sosiale medier gi politiet et verdifullt tilskudd til situasjonsforståelsen. En markant aktivitetsøkning på sosiale medier kan også være et varsel om at noe er i ferd med å skje. I Nederland har politiet tatt i bruk verktøy som automatisk skanner store mengder informasjon på Twitter, og ved hjelp av algoritmer henter ut og sorterer informasjon som kan være relevant for nødetatene ved større hendelser hvor publikum ofte er først på stedet og tett på det som skjer.[9]

Sosiale medier er ikke bare en ny informasjonskilde for politiet, men gir også nye muligheter for tettere samarbeid med publikum og å engasjere dem i sitt arbeid. Sosiale medier kan også bidra til bedre forståelse av hvordan publikum opplever politiet og av hva som opptar dem.

Flere politistasjoner i Norge bruker allerede sosiale medier, men primært som en informasjonskanal mot publikum. Teknologirådet anbefaler at bruken av

[7] TNS Gallup for Teknologirådet og Datatilsynet, januar 2013
[8] Norsk mediebarometer 2013, Statistisk Sentralbyrå (2014)
[9] http://www.newscientist.com/blogs/onepercent/2012/04/making-twitter-make-sense-for.html

åpne sosiale medier i politiet utvides, slik at de også fungerer som en informasjons- og kommunikasjonskanal inn til politiet.

Samtidig må det foreligge tydelige målsettinger og retningslinjer for politiets aktivitet i åpne sosiale medier, hvis ikke kan det i verste fall føre til en uheldig nedkjølingseffekt.

Politiet bør overvåke åpen informasjon i sosiale medier

Automatiserte dataprogrammer som overvåker informasjon i sosiale medier gir unike muligheter for tidlig varsling og styrket situasjonsforståelse, særlig ved større hendelser. Sammen med digitale nødmeldinger og tips fra publikum, samt politiets egne feltrapporteringer, vil informasjon i sosiale medier være et svært viktig bidrag til politiets samlede situasjonsbilde.

I en tidlig fase bør politiets overvåkning og analyse begrense seg til aggregert informasjon i sosiale medier, og ikke brukes til å identifisere individer i etterforskning. Formålet med overvåkingen bør være å styrke situasjonsforståelsen ved hendelser eller kartlegge publikums holdninger eller fra tilbakemeldinger knyttet til politiets arbeid.

Denne begrensningen kan revurderes når politiet har opparbeidet tilstrekkelig erfaring og kompetanse i analyse og bruk av informasjon i sosiale medier.

Videre bør politiets bruk av sosiale medier utvides slik at disse fungerer som en plattform for å engasjere publikum i politiets daglige arbeid, særlig arbeid som gjøres i lokalmiljøet. Det legger til rette for et tettere samarbeid med publikum, som i sin tur kan gi politiet mer målrettet informasjon og tilbakemeldinger ved behov, både ved akutte hendelser og i mer langsiktig arbeid.

Politiet må ha klare retningslinjer for å unngå nedkjølingseffekt

Politiets overvåking og tilstedeværelse i sosiale medier kan oppleves som en begrensing på fri utfoldelse i disse kanalene.

Det er derfor viktig at politiets daglige overvåking av sosiale medier kun involverer informasjon som også er allment tilgjengelig for andre samfunnsaktører, og at virksomheten er forankret i et tydelig definert skille mellom åpen og lukket informasjon.

Det finnes mange ulike sosiale medier, og disse opererer på ulike måter. Twitter-meldinger er f.eks. tilgjengelig for alle med internettilgang, mens Facebook krever pålogging. Informasjonen kan både bevisst og ubevisst deles med alle, mange eller få. Samtidig er den allmenne oppfatning av hva som er offentlige og private rom i digitale medier i stadig forandring.

For å unngå at politiet tilstedeværelse i sosiale medier resulterer i en uønsket nedkjølingseffekt som påvirker folks naturlige omgang med disse mediene, behøves en utredning av hvor disse skillelinjene går med særlig fokus på bruk av slik informasjon i justissektoren.

Videre er det viktig at politiets bruk av sosiale medier forankres i en tydelig strategi for hele etaten. Formålet med politiets bruk av sosiale medier må være tydelig definert og fulgt opp med klare retningslinjer for riktig bruk. Retningslinjene bør bl.a. svare på følgende og åpent deles med publikum:

- Hvilke sosiale medier som til enhver tid overvåkes og til hvilke formål.
- Hvilke metoder som brukes i overvåkningen, og en klarering av om sammenhengen mellom formål og metode proporsjonal og nødvendig.
- Hvordan og hvor lenge innsamlet informasjon lagres.
- Hvordan informasjonen kan brukes og sammenstilles med annen informasjon.
- Hvilke redaksjonelle mekanismer har politiet for å beskytte personvernet når publikum aktivt engasjeres i en sak.

2. POLITIETS NYE MULIGHETER

"Det er skyting på Utøya. Lillesøstera mi er der og ringte hjem nå."
Fredag 22.07 – 17:41:10. Frk Tirill.

Dette var den første Twitter-meldingen fra Utøya etter at skytingen startet. Ungdom som befant seg på Utøya mens skytingen pågikk, sendte tekstmeldinger til familie og venner, til og med direkte til regjeringsmedlemmer. De brukte sosiale medier for å fortelle om sin egen situasjon og for å få informasjon om de andre på øya.[10]

En god politirespons er avhengig av rettidig og presis informasjon fra hendelsen. Publikum er gjerne først på åstedet og de har med seg smarttelefonen overalt. En eller flere smarttelefoner vil derfor høyst sannsynlig befinne seg i nærheten av de fleste hendelser. Publikum kan sende tekst, bilder, lyd- og videoopptak fra omgivelsene. Dette er informasjon som kan hjelpe politiet i deres arbeid, på vei til åstedet, og i den videre oppfølgningen av situasjonen.

Publikums smarttelefon er en ressurs som politiet ikke utnytter i dag. De siste ti årene har smarttelefonen gitt opphav til en ny situasjon, hvor folk kommuniserer og deler informasjon på helt nye måter. Samtidig har utviklingen in-

[10] 22. juli-kommisjonen hadde dialog med 185 personer som var på Utøya under skytingen om deres bruk av sosiale medier det første døgnet etter terroraksjonen. 37 personer svarte at de var aktive på sosiale medier mens skytingen pågikk; NOU 2012: 14; 22. julikommisjonens rapport, s. 277.

nen IKT gjort det enklere å håndtere store datamengder og gjøre komplekse analyser på digital informasjon. Denne rapporten beskriver hvordan denne utviklingen kan forandre og forsterke det tradisjonelle samspillet mellom politi og publikum. Mer enn noen gang kan publikum aktivt brukes som ressurs for å gi mer politikraft. Det kan få stor betydning for hvordan politiet vil jobbe i fremtiden.

Samtidig som teknologien gir nye muligheter, reiser den også sentrale spørsmål knyttet til personvern og åpenhet. Det er viktig å trekke opp grensene for hvor langt politiet skal kunne gå i sin utnyttelse av nye muligheter, samt vurdere hvilke videre utilsiktede konsekvenser ny teknologi kan ha for folk og samfunn.

2.1 PUBLIKUM ER VILLIGE TIL Å DELE

Nordmenn viser vilje til å dele informasjon med politiet. 63 prosent av oss ønsker å bidra med bilder og video fra hendelser, og en like stor andel ønsker å motta forespørsler fra politiet om observasjoner fra stedet der de befinner seg. 92 prosent ønsker å samarbeide med politiet for å hindre lovbrudd, for eksempel ved hærverk i nabolaget. [11]

I en undersøkelse foretatt av Teknologirådet i samarbeid med Datatilsynet, sa over 60 prosent seg helt eller delvis enig i påstanden om at både politi og sikkerhetsmyndigheter bør kunne bruke åpen informasjon fra sosiale medier, blogger og andre internettjenester til forebygging og etterforskning, mens nærmer 20 prosent var helt eller delvis uenig.[12]

I forbindelse med arbeidet med denne rapporten har Teknologirådet gjennomført en spørreundersøkelse med 1000 respondenter i aldersgruppen 15 år og oppover for å undersøke publikums holdninger til kommunikasjon og informasjonsdeling med politiet gjennom smarttelefonen og sosiale medier. Undersøkelsen bekrefter delingsviljen i befolkningen, men viser samtidig at publikums forhold til politiets tilstedeværelse på og bruk av sosiale medier er

[11] Iversen og Dahl (2010), *"Politi 2.0: Kan sosiale medier bidra til økt dialog og samhandling mellom politi og publikum?"*, s 11

[12] Spørreundersøkelse gjort i forbindelse med Personverndagen 2014. Undersøkelsen ble gjennomført av Opinion Perduco via webpanel i november 2013. Til sammen 1501 innbyggere i alderen 15 år og oppover deltok i undersøkelsen.

noe mer nyansert. Resultatene fra undersøkelsen er presentert som diagrammer på ulike steder i rapporten.

2.2 POLITISK AKTUALITET

Politiet er inne i en rask og omfattende endringsprosess. Terrorangrepene 22. juli 2011 har bidratt til å akselerere denne prosessen. Endringene innebærer forandringer i alt fra struktur og organisering til teknologiutnyttelse og fornyelse av arbeidsverktøy og metoder. Flere pågående og kommende prosjekter vil være premissgivende for fremtidens politi.

Samtidig har informasjonsrevolusjonen og digitaliseringen forandret det norske samfunn på grunnleggende måter. Disse endringene har vært med på å forandre arbeidsprosesser i mange ulike informasjonsvirksomheter de siste årene. Politiet er en informasjonstung virksomhet, og det er både naturlig og nødvendig å vurdere hvordan disse endringene vil gi politiet nye muligheter og utfordringer i årene fremover.

2.2.1 22. JULI-KOMMISJONEN

Rapporten fra 22. juli-kommisjonen ga et detaljert øyeblikksbilde av situasjonen i norsk politi. Et viktig budskap i rapporten var at potensialet i moderne IKT ikke var tilstrekkelig utnyttet[13] og at vi forøvrig befinner oss i en teknologirevolusjon som norsk politi må bli en del av[14].

Kommisjonen erkjenner også at teknologien har endret samspillet mellom politi og publikum: kunnskapen om angrepene spredte seg hurtig til store deler av befolkningen ved hjelp av mobiltelefoner og sosiale medier. Den påpeker også at vi nå står overfor en helt ny og interessant situasjon, hvor bl.a. regjeringsmedlemmer får informasjon direkte fra ofre via SMS, telefon og sosiale medier mens en nasjonal krise pågår og skal håndteres[15].

[13] NOU 2012:14, Rapport fra 22. juli-kommisjonen, s16
[14] NOU 2012:14, Rapport fra 22. juli-kommisjonen, s336
[15] NOU 2012:14, Rapport fra 22. juli-kommisjonen, s454

I forlengelsen av dette skisserer kommisjonen løselig mulighetsrommet som bl.a. smarttelefoner åpner for politiet, uten å gå nærmere inn på hva dette betyr og hvilke konsekvenser det vil få for politi og samfunn:

> *"Mobiltelefoni og smarttelefon tilbyr også foto- og videokapasitet som politiet åpenbart vil kunne nyttiggjøre, ved å etablere systemer og programmer som kan samspille med teknologien."*[16]

2.2.2 POLITIANALYSEN

Politianalysen[17] følger opp med en grundig, helhetlig og godt dokumentert analyse av politiets organisering, styring og virksomhetsutøvelse. Også teknologi og teknologianvendelse er satt på dagsordenen. Analysen diskuterer utførlig viktige problemer knyttet til organiseringen og styringen av IKT i politiet.

Nærhet og tilgjengelighet til publikum er et tilbakevendende tema i analysen, men i denne sammenheng diskuteres teknologi først og fremst som et støtteverktøy som kan effektivisere tjenesteutøvelsen. Ulike informasjons- og selvbetjeningstjenester, slik som eksempelvis elektronisk søknadsbehandling og mulighet til å bestille time på internett, løftes som eksempler på teknologi om vil kunne lette kontakten med publikum.

I så måte følger ikke Politianalysen opp sporet fra 22. juli-kommisjonens rapport med en beskrivelse av mulighetsrommet som smarttelefoner, sosiale medier og nye informasjonskilder gir politiet. Det er en mangel ved Politianalysen som denne rapporten vil forsøke å bøte på.

2.2.3 JUSTISKOMITÉENS INNSTILLING TIL TERRORMELDINGEN

I Meld. St. 21 (2012–2013) *Terrorberedskap*[18] redegjør regjeringen Stoltenberg for sin oppfølging av rapporten fra 22. juli-kommisjonen. Her diskuteres utbredelsen av mobile enheter hos publikum og fremveksten av sosiale medier først og fremst som verktøy for radikalisering og terrorplanlegging. Mulighetene for et nytt samspill mellom politi og publikum blir ikke utforsket.

---

[16] NOU 2012:14, Rapport fra 22. juli-kommisjonen, s336
[17] NOU 2013:9, Ett politi – rustet til å møte fremtidens utfordringer
[18] Meld. St. 21 (2012-2013), Terrorberedskap – Oppfølging av NOU 2012:14 Rapport fra 22. juli-kommisjonen

Stortingets justiskomité påpeker disse manglene i Innst. 425 S til Stortinget 6. juni 2013[19]. En enstemmig komité "viser til mulighetene for å bruke stedsinformasjon, bilder og video fra publikum i nødsituasjoner og ved nødmeldinger. Komiteen mener det i en krisesituasjon er viktig med informasjonssystemer som raskt kan levere mest mulig korrekt, helhetlig og fullstendig situasjonsbilde."[20]

Denne rapporten ønsker å kartlegge og tydeliggjøre disse mulighetene, og samtidig diskutere utfordringer som knytter seg til teknologiutviklingen.

2.3 MÅL OG AVGRENSNINGER FOR RAPPORTEN

Teknologirådet vil i løpet av året utgi tre rapporter om hvordan utviklingen i samfunn og teknologi det siste tiåret har endret forutsetningene for politiarbeidet.

2.3.1 TRE RAPPORTER OM TEKNOLOGI I POLITIET

Denne rapporten er den første i serien, og har to hovedtemaer:

1. Smarttelefonen og hvilke muligheter den gir for samhandling med publikum.
2. Hvordan informasjon fra nye, åpne kilder, særlig sosiale medier, kan brukes til å styrke politiets situasjonsforståelse nært opp til en hendelse.

Neste rapport vil ta for seg hvordan prediktive analysemetoder kan brukes til å forutsi hvor og når kriminalitet finner sted, og hvordan de kan understøtte politiets forebyggende arbeid.

Den siste rapporten i serien handler om hvordan teknologi for informasjonsdeling kan tilrettelegge for at politiet får nødvendig, korrekt og tilpasset informasjon til rett sted og tid.

Teknologirådets konklusjoner bygger på erfaringer fra andre land, og en analyse av hvordan sentrale teknologiske utviklingstrekk vil prege politiets arbeidsmåter fremover.

[19] Innst. 425 S (2012-2013), Innstilling fra justiskomiteen om terrorberedskap, 6. juni 2013
[20] Innst. 425 S (2012-2013), Innstilling fra justiskomiteen om terrorberedskap, 6. juni 2013, s. 17

2.3.1 AVGRENSNINGER

Denne rapporten drøfter hvordan utbredelsen av smarttelefoner og andre mobile enheter i den norske befolkningen kan gi politiet anledning til å hente informasjon fra omgivelsene når noe skjer, der det skjer. Den vil i første rekke beskrive nye mulighetsrom for samspill mellom politi og publikum. Rapporten vil ikke utførlig diskutere krav til teknisk infrastruktur for å realisere disse mulighetene.

Videre befatter rapporten seg primært med politiets *operative* virksomhet. Den operative virksomheten til politiet er likevel både bred og mangfoldig. I videste forstand involverer dette alt fra forebygging og etterretning til orden, trafikk, operasjonssentraler, samt redning- og beredskapsarbeid. I arbeidet med rapporten er det derfor gjort en rekke avgrensninger. Rapporten vurderer ikke teknologi og informasjonsinnsamling som understøtter politiets etterforskning og straffesaksprosesser eller etterretningsarbeid som typisk hører under Politiets sikkerhetstjeneste (PST).

Forebygging, etterretning, beredskap, kriminalitetsbekjempelse og etterforskning er imidlertid aktiviteter som kan gå over i hverandre. Flere av elementene i rapporten vil derfor både ha relevans for andre virksomhetsområder i politiet, samt være nødvendige forutsetninger for å hente gevinst fra ny og fremtidig teknologi.

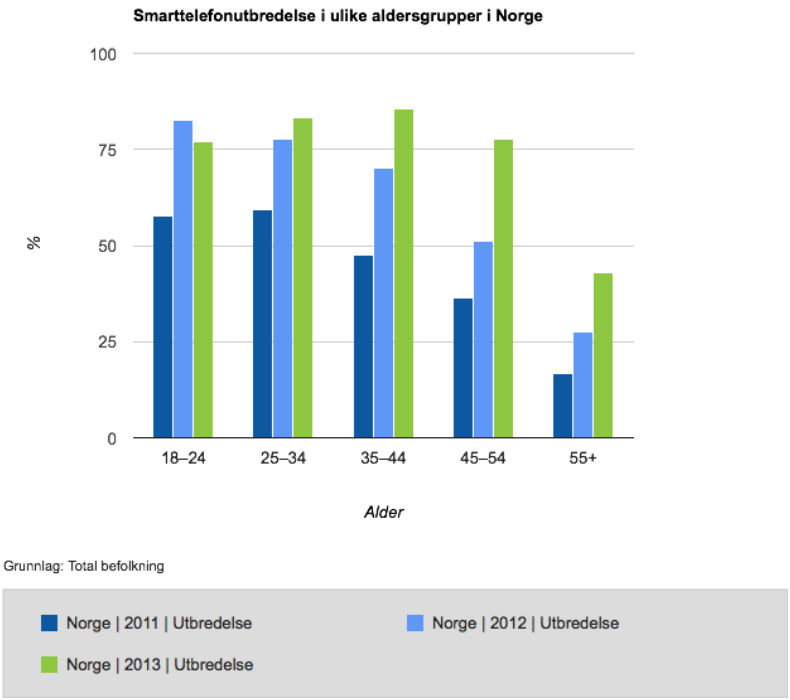
3. DIGITALE NØDMELDINGER OG TIPS

En smarttelefon er ikke bare en telefon. Å ringe er i dag kun den femte mest brukte funksjonen på mobiltelefonen (etter internettbruk og sosiale medier)[21]. Smarttelefonen er en avansert datamaskin med ulike sensorer, som også kan dele data over nettet. Kamera og mikrofon gjør at folk kan registrere omgivelsene nøyaktig med tid, sted, tekst, bilde-, lyd- og videoopptak. GPS og akselerometer kan brukes til presis stedsbestemmelse og til å måle bevegelse.

I dag har 3 av 4 nordmenn en smarttelefon i lommen[22]. Og mens den yngre delen av befolkningen ikke overraskende har vært raske til å ta i bruk smarttelefoner, viser Figur 1 at utbredelsen nå også tiltar i eldre alderssegmenter[23].

I praksis betyr dette at overalt hvor folk befinner seg, vil det også være små, avanserte datamaskiner med sensorer i form av smarttelefoner. På denne måten kan publikum betraktes som et sensornettverk som aktivt eller passivt kan bidra med informasjon som understøtter politiets operative virksomhet.

[21] Shane Richmond, "Smartphones hardly used for calls", The Telegraph, 29. juni 2012
[22] MedieNorge og TNS Gallup, http://www.medienorge.uib.no/statistikk/medium/ikt
[23] Google, "Our Mobile Planet", http://www.thinkwithgoogle.com/mobileplanet



Figur 1 Mobilutbredelse i ulike aldersgrupper i den norske befolkningen fra 2011 til 2013 (Kilde: "Our Mobile Planet", http://think.withgoogle.com/mobileplanet/).

Slike data fra publikum kan være nyttige for politiet på flere ulike måter. Blant annet kan de bidra til at politiet raskt får:

- mer detaljert informasjon via bilder og video og dermed en styrket situasjonsforståelse
- en presis stedsangivelse og mulighet til å lokalisere personer ved behov
- bedre oversikt over en hendelse ved å sammenstille bilder fra flere personer
- bedre forståelse av situasjonforløpet ved en større hendelse eller krise
- forståelse av bevegelsesmønsteret til større menneskemasser

Fordi informasjonen er digital, kan den behandles og sammenstilles med andre nødmeldinger i politiets datasystemer. Politiet vil kunne spare verdifull tid som i dag går med til manuell registrering og tolkning av informasjon i nødmeldinger. Det vil også kunne minske sannsynligheten for feil, og for at viktig informasjon blir oversett. Delautomatiserte prosesser kan sørge for at informasjonen behandles videre, sorteres, analyseres og deles mellom de relevante enheter i politiet uten tap av mening. Informasjonen kan på den måten bli nyttig og handlingsorientert for både operasjonssentral, patrulje og politistasjon.

For å tilrettelegge for en slik informasjonsinnsamling og for at politiet skal kunne håndtere informasjonsrikdommen på en skikkelig måte, må politiet innføre nye verktøy, metoder og retningslinjer for bruk. Samtidig reiser en slik informasjonsrikdom noen viktige og interessante spørsmål knyttet til personvern, åpenhet og om hvor mye vi ønsker at politiet til en hver tid skal kunne vite eller ha anledning til å få vite.

Både mulighetene og slike hensyn diskuteres nedenfor.

3.1 STYRKET SITUASJONSFORSTÅELSE

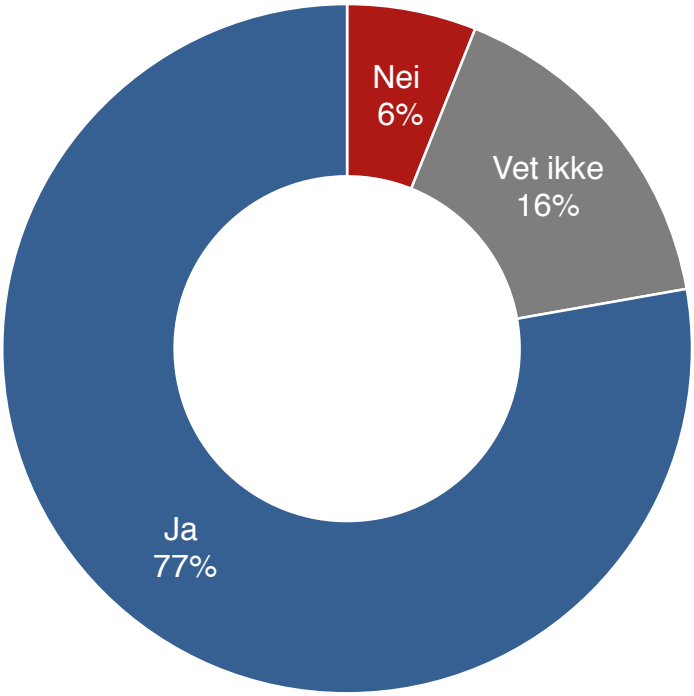
Tilgang til relevant informasjon tett opp til en hendelse er viktig for å etablere et korrekt situasjonsbilde – en felles forståelse av hva som skjer, når det skjer, hvor det skjer, hvem som er involvert, hvilken risiko det innebærer for mannskap og publikum, hvordan situasjonen kan utvikle seg, osv.

Smarttelefoner gir anledning til å bedre politiets situasjonsforståelse både før, under og umiddelbart etter en hendelse. Nedenfor gis ulike eksempler på hvordan publikum kan gi politiet en bedre beskrivelse av de faktiske omstendighetene.

3.1.1 DIGITALE BILDER: MER INFORMASJON

Politiet kan ofte lese mer ut av et bilde enn det et vitne kan fortelle over den tradisjonelle nødtelefonen. En vitneforklaring kan være upresis og kanskje mangle viktige detaljer. Erfaring viser også at stressfaktorer rundt alvorlige hendelser gjør at mange vitner kun kort tid etter glemmer viktig informasjon, for eksempel fargen på en jakke eller en bil.

Er du villig til å sende bilder eller video fra mobilen til politiet for at de skal forstå situasjonen bedre, hvis du er vitne til noe kriminelt eller er på stedet før dem ?



Et digitalt bilde eller en video kan ”stemples” med tidspunkt og sted. Tids- og stedsinformasjon kan brukes til å sortere bilder som er tatt på samme sted og til samme tid. Ettersom dette er digital informasjon, kan datamaskiner forenkle sorteringsprosessen betraktelig. Relevante digitale bilder og filmsnutter vil raskt og effektivt kunne deles med alle involverte parter, under for eksempel en redningsaksjon.

Publikum har nå anledning til å dokumentere hendelser og forhold med digitale bilder og video der hvor de befinner seg. Dette vil i mange tilfeller være en viktig informasjonsressurs for politiet.

3.1.2 BILDEMOSAIKK: BEDRE OVERSIKT

Når politiet får flere bilder fra samme hendelse kan disse settes sammen i ”bildemosaikker” og på den måten bidra til å gi bedre oversikt over situasjonen. Maskinell bildebehandling kan hjelpe med å sortere og analysere bildene.

Dette så vi et eksempel på i kjølvannet av bombeangrepene under Boston Marathon i april 2013. Kort tid etter eksplosjonene satte FBI og Boston Police Department i gang en etterforskningsprosess dels basert på ”crowdsourcing”, en slags informasjonsdugnad, hvor publikum bidro med store mengder digital informasjon. Politiet lette etter ledetråder om hvem som kunne ha plassert bombene nær målstreken og ba publikum og omkringliggende virksomheter om å sende inn bilder, videoer og andre beskrivelser fra målområdet umiddelbart før og etter eksplosjonene. På oppfordring fra politiet kunne publikum også sende inn tekstmeldinger og starte en dialog med politiet. Tipstjenesten er anonym, noe politiet i Boston anser som særdeles viktig for å få kritisk informasjon.

Politiet mottok over 2.000 tips umiddelbart etter angrepet. Tusenvis av bilder og videoer fra både offentlige og private overvåkningskameraer ble sydd sammen med bilder fra publikums mobiltelefoner. På denne måten kunne politiet lage en bildemosaikk som tegnet et overordnet og mer oversiktlig bilde av hendelsesstedet og områdene rundt fra forskjellige vinkler. Politiet mente selv at de fikk uvurderlig hjelp.[24]

Ulike digitale informasjonsfragmenter fra publikum kan altså sys sammen for å tegne et mer helhetlig bilde av en situasjon. Fordi de aller fleste er utstyrt

[24] Samtale med Boston Police Department

med en smarttelefon, kan publikum medvirke og bidra til å stryke politiets situasjonsforståelse gjennom en felles "informasjonsdugnad".

3.1.3 GPS: PRESIS LOKALISERING

Presis lokalisering av innringeren er viktig for at politiet skal kunne vurdere henvendelsen og planlegge en tilpasset respons, særlig hvis innringeren er utsatt for en ulykke, er vitne til en hendelse eller befinner seg i et risikoområde. Kjennskap til innringerens posisjon kan også være nyttig hvis politiet ønsker ytterligere informasjon, slik som bilder eller video, for å styrke sin egen situasjonsforståelse.

En innringer til et nødnummer i Norge blir i dag automatisk lokalisert. Ringer man fra en fasttelefon sendes gateadressen man ringer fra. Ringer man fra mobiltelefon sendes omtrentlig geografisk posisjon, som beregnes ut i fra basestasjonene i nærheten.

En smarttelefon med GPS vil kunne gi mer presis lokasjon enn posisjon beregnet fra basestasjoner. Den vil under gode forhold kunne vite hvor den er med en nøyaktighet på ca. 7 meter eller mindre[25]. (Under mindre ideelle forhold, for eksempel inne i tettbygde byrom, vil den kunne angi hvor den er med en nøyaktighet på ca. 40 - 100 meter).

Politiet på Island har laget en sporingsapplikasjon for smarttelefoner. Applikasjonen gjør det mulig for publikum å frivillig dele GPS-lokasjonen med islandske 112, hvor kun de 5 siste posisjonene lagres. Skulle en nødsituasjon oppstå, kan man med et enkelt tastetrykk melde fra ved hjelp av applikasjonen. Koordinatene brukes som startpunkt for å kunne geleide personer som har gått seg vill, eller å iverksette en leteaksjon dersom det skulle være nødvendig. I mange tilfeller har det vist seg at politiet har sluppet å sende ut letemannskaper, og dermed spart betydelige politiressurser, samtidig som personer raskere har kommet til rette. Med litt veiledning, har de savnede ofte vært i stand til å finne tilbake. Islandske myndigheter planlegger å utvide løsningen med mulighet for å sende multimedie-meldinger. [26]

Digital informasjon fra publikums smarttelefoner kan enkelt merkes med svært presis stedsinformasjon. Presise lokasjonsdata vil ikke bare kunne bidra til redusert responstid; også responskvaliteten vil kunne forbedres når politiet

[25] http://no.wikipedia.org/wiki/Gps
[26] Presentasjon: "112-app", Tómas Gíslason; deputy CEO 112 Iceland + samtale med islandsk politi

tidlig har kjennskap til presis lokasjon og kan hente ut nødvendig tilleggsinformasjon og gjøre nødvendige forberedelser i forkant. Dessuten viser erfaringen fra Island at slike data åpner for nye og interessante måter å levere tjenester til publikum på.

3.1.4 KARTLEGGING: FORSTÅ SITUASJONSFORLØPET

Samlinger av meldinger med informasjon om stedet de blir sendt fra kan gi ytterligere gevinst for politiet. Slike meldinger kan telles, grupperes og plasseres på kart der de sammen danner øyeblikksbilder fra et situasjonsforløp. Det kan for eksempel vise hvor mange som befinner seg i umiddelbar nærhet av en hendelse.

En smarttelefon vil automatisk kunne merke digitale meldinger med presis tids- og stedsangivelse. Nye meldinger og oppdateringer vil derfor kunne vise hvordan en situasjon utvikler seg over tid. Ved å legge nødmeldinger over på kart, kan politi og nødetater lettere gjøre riktige ressursprioriteringer og tilpasse responsen til hendelsen.

Haiti opplevde et kraftig jordskjelv i januar 2010. Mange var fryktet omkommet. Flere postet meldinger i sosiale medier der de beskrev ødeleggelsene der de oppholdt seg eller de ba om hjelp. Det ble også satt opp en egen SMS-kode for at publikum skulle kunne sende inn informasjon om de største behovene. Frivillige og hjelpeorganisasjoner gikk gjennom meldingene der de identifiserte og lokaliserte de mest akutte ”liv-og-død”-tekstmeldingene og plasserte disse på digitalt kart. Kartet ble brukt til å prioritere innsatsen og sende hjelp dit hvor behovene var størst. Hjelpeorganisasjonene på Haiti rapporterte at dette kartet var til uvurderlig hjelp i søk- og redningsoperasjonen etter jordskjelvet, og at det bidro til å redde hundrevis av liv.[27]

I Haiti ble mye av behandlingen av meldingene gjort manuelt, så det tok forholdsvis lang tid å plassere meldingene på kartet. Digitale verktøy vil kunne gruppere og plassere alle nødmeldinger med lokasjon på et kart (automatisk og i sanntid). Slike kart kan også berikes med informasjon fra sosiale medier. Politiet vil dermed umiddelbart kunne få denne oversikten og ikke bruke verdifull tid og ressurser på å utarbeide kartet.

[27] http://newswatch.nationalgeographic.com/2012/07/02/crisis-mapping-haiti/

Digital informasjon fra publikum legger i så måte til rette for rask kartlegging av et situasjonsforløp. Dette kan bl.a. være til stor hjelp i responsplanlegging, samhandling og koordinering nødetatene imellom.

3.1.5 BEVEGELSE AV STORE MENNESKEMENGDER

Kjennskap til bevegelsesmønstret til store menneskemasser kan også ha nytteverdi for politiet. Det kan bl.a. gjøre beredskapsplanlegging og –arbeid i forbindelse med store arrangement som konserter, idrettsstevner, 17. maifeiring og demonstrasjoner tryggere og mer effektiv.

Ny teknologi bedrer vesentlig mulighetene for å samle slik informasjon. Når en smarttelefon rapporterer sin lokasjon i jevnlige intervaller, kan denne informasjonen brukes til å tegne et bilde av bevegelsesmønsteret til personen som bruker telefonen. Når mange mennesker deler sin posisjon via smarttelefonen, kan dette gi innsikt i hvordan store systemer og mekanismer fungerer.

Et eksempel er mobilapplikasjonen Waze. Den bruker stedsinformasjon fra smarttelefonene til millioner av bilister for å gi brukerne oppdatert trafikkinformasjon i sanntid og forslag til alternative kjøreruter. I humanitær sammenheng har bevegelsesmønstre fra mobiltelefoner blitt brukt til å kartlegge sykdomsspredning i befolkningen[28].

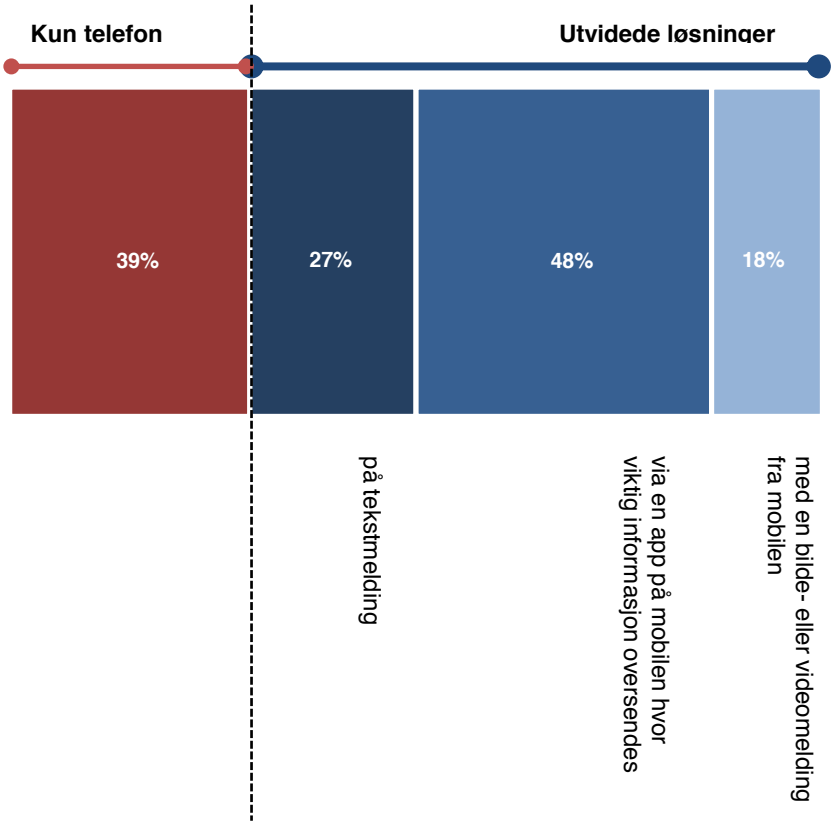
London Metropolitan Police tilbyr publikum en mobilapplikasjon for å dele informasjon mellom publikum og politi. De har utvidet applikasjonen med mulighet for å sende mobiltelefonens lokasjon og bevegelsesretning. Brukeren godkjenner at slike data sendes anonymt med jevne mellomrom i en begrenset tidsperiode, gjerne før, under og etter et planlagt arrangement. Dataene plasseres umiddelbart på et kart som viser hvor mennesker har samlet seg og hvordan ansamlingene flytter på seg i sanntid.[29]

Anonymiserte lokasjonsdata fra publikum kan altså brukes til å kartlegge bevegelsesmønstre til større menneskemasser i sanntid, og justere planlagt beredskap deretter. Eksempelet fra London viser at dette åpner for nye former for samvirke mellom politi og publikum.

---

[28] "Mobile Phone Network Data for Development", United Nations Global Pulse, oktober 2003
[29] http://www.cityoflondon.police.uk/contact-city-police/smartphone-app/Pages/default

Tenk deg at du er i en situasjon der du trenger rask hjelp fra nødetatene. Ønsker du å kunne melde fra på andre måter enn over tradisjonell telefon?



3.2 ET NYTT SAMSPILL MELLOM POLITI OG PUBLIKUM

Eksemplene over viser at smarttelefonen gir publikum helt nye muligheter til å rapportere hendelser og bistå politiet med nyttig informasjon der det skjer, når det skjer. På mange måter kan smarttelefonen betraktes som en plattform for et nytt samspill mellom politi publikum.

For publikum kan digital informasjon fra smarttelefonen brukes i minst tre ulike sammenhenger:

- **Føre var**: På samme måte som publikum kan installere en privat husalarm, viser eksemplene fra Island og London at publikum f.eks. ved å dele posisjon kan bruke smarttelefonen for å redusere risiko og muligens sikre seg mot en fremtidig ulykke på helt nye måter.

- **Rop om hjelp**: Når ulykken først er ute, gir smarttelefonen publikum anledning til å kommunisere med politi og nødetater på et utall ulike måter, f.eks. via tale, tekst, bilder og video. I en akutt nødsituasjon kan viktig informasjon som posisjon og helsedata ved behov oversendes nødetatene automatisk. Dette kan spare verdifull tid og styrke sikkerheten til innsenderen.

- **Øyenvitne**: Mens publikum i dag kan bistå politiet med tips over telefon eller som en tekstmelding på internett, kan de gjennom smarttelefonen også sende inn verdifull informasjon i form av f.eks. bilder, video og lydopptak. Fordi de fleste har telefonen med seg, vil slike tips kunne komme tettere opp til en hendelse og oppdateres når viktige endringer oppstår. Publikum kan f.eks. bidra til å beskrive utviklingsforløpet til en brennende bygning, mens nødetatene er underveis.

For politiet kan informasjon fra publikums smarttelefoner bl.a. gi:

- **Bedre situasjonsforståelse** gjennom en større informasjonsrikdom. Særlig når mange bidrar med informasjon, kan dette gi et betydelig tilskudd til politiets situasjonsforståelse.

- **Raskere og mer presis ressursstyring** gjennom bedre kjennskap til både hendelsessted og situasjonsforløp. Det gir også politiet

anledning til å overvåke hendelsesforløpet i sanntid og tilpasse og styre ressursene etter behov.

- **Tettere publikumskontakt** ved at publikum får tilgang til politiet på innerlommen. Det muliggjør også en elektronisk dialog med publikum på hendelsesstedet i sanntid.

Publikums smarttelefoner er i så måte ikke bare en informasjonskilde for politiet og et kommunikasjonsverktøy for publikum. Den er også med på å åpne for et nytt og tettere samspill mellom politi og publikum:

- For politiet vil publikum kunne brukes mer aktivt som en ressurs for å gi mer politikraft i forkant eller når ulykken er ute.

- For publikum vil politiet kunne oppleves som mer tilgjengelig og nært. Enkle og raske måter å komme i kontakt med politiet på vil i sin tur kunne gi økt publikumsengasjement og styrket tillitsforhold.

Når politiets kontaktflate mot publikum skal moderniseres, er det derfor viktig at man ikke begrenser seg til utviklingen av nettbaserte informasjons- og selvbetjeningstjenester, eller til oppdateringer av eksisterende meldepraksis (f.eks. muligheten til å sende nødmeldinger per SMS). Det er avgjørende å tenke bredt rundt hvilken rolle publikum skal spille i fremtidens politi.

3.3 112 SOM APP: EN NY KONTAKTFLATE MOT PUBLIKUM

Publikum må enkelt kunne kommunisere med politiet på de måtene og med de redskapene de ellers bruker i hverdagen. Samtidig er et publikum utstyrt med smarttelefoner en viktig ressurs som politiet må kunne trekke på ved behov.

Det er viktig å tilrettelegge for at det skal være enkelt og trygt for publikum å sende meldinger med bilder, video og annen informasjon til politiet. Politiet må ved behov også kunne be publikum om å sende inn slik informasjon, og ellers kunne ta i mot slike meldinger og behandle dem effektivt.

Land / region	Funksjonalitet
Danmark	Presise lokasjonsdata sendes automatisk når et nødanrop gjennomføres.
Island	Applikasjonen sender presise GPS-koordinater til nødsentralen per SMS når et nødanrop gjennomføres. Brukeren kan velge å til enhver tid dele de fem siste lokasjonspunktene med nødsentralen.
Nederland	Sende bilder og video til politiet via et online-skjema knyttet til politiets nettsider (www.politie.nl) som gjøres tilgjengelig gjennom applikasjon.
Catalonia	Brukeren kan motta informasjon om pågående nødsituasjoner, samt lokasjonstilpassede instrukser om hvordan man skal forholde seg til situasjonen. Applikasjonen gir samlet tilgang til trafikkinformasjon, værdata, offentlig transport, osv.
Kanariøyene	Presise lokasjonsdata oversendes, samt mulighet for nødanrop via tale, tekst (instant messaging) og bilder. Medisinske profildata som blodtype og kroniske sykdommer oversendes automatisk.
Lombardia	Presise lokasjonsdata oversendes, samt personprofil og liste over kontaktpersoner.

Tabell 1 Land og regioner som har utviklet applikasjoner for kontakt med nødtelefonen med utvidet funksjonalitet

3.3.1 TILRETTELEGGING FOR SMARTTELEFON

For brukere av smarttelefoner, vil en mobilapplikasjon (”mobil-app”) kunne gjøre det enkelt å sende digitale meldinger til politiet, både i en akutt nødsituasjon og som øyenvitnebeskrivelser eller tips. Som Tabell 1 viser, har flere politi- og nødetater begynt å lansere applikasjoner som på ulike måter utnytter de mulighetene som smarttelefonen tilbyr. En slik mobil-app vil typisk fungere som en plattform som gir tilgang til en rekke funksjoner på smarttelefonen, deriblant tale, SMS, MMS, kamera- og opptaksutstyr, GPS og chat/instant messaging.

En slik mobil-app vil dessuten kunne inneholde informasjon som

- avsenders navn, adresse og fødselsnummer
- alder og viktige helseopplysninger
- pårørendes navn og kontaktnummer, osv.

Videre kan applikasjonen hente informasjon om tidspunkt, lokasjon og eventuelt bevegelsesretning direkte fra smarttelefonens systemer. Om ønskelig kan denne informasjonen automatisk oversendes politi og nødetater sammen med

nødmeldingen eller taleanropet. Samtidig bør det være mulig for publikum å sende inn helt anonyme nødmeldinger, slik det er diskutert under.

Selve nødmeldingen eller tipset kan formuleres på ulike måter tilpasset situasjonen avsenderen befinner seg i:

- meldingen kan leses inn som en talemelding, med eller uten video
- meldingen kan skrives inn som tekst, med eller uten bilde
- meldingen kan bestå av en forhåndsdefinert tekst, hvor avsender for eksempel velger riktig kategori, og en passende beskrivelse og legger til bilder eller annen informasjon.

Smarttelefonen gjør det mulig å sende informasjon til nødetatene over mobilnettet (tale, SMS, MMS), mobilt bredbånd eller fast internett (IP-telefoni,chat/instant messaging, bilder, video, osv.). Ulike funksjoner på mobilen vil ta i bruk ulike kommunikasjonsprotokoller og avhengig av dekning og tilgjengelighet, vil mobil-appen delvis kunne veksle mellom disse ulike infrastrukturene. Er eksempelvis den mobile bredbåndsdekningen dårlig, kan et bilde også sendes i komprimert form over mobilnettet som en MMS.

Når meldingen er sendt vil brukeren gjennom mobilapplikasjonen kunne få en bekreftelse på at meldingen er mottatt. Avsenderen kan også få eventuelle statusoppdateringer fra politiet, slik som ”Enheter ventes å være på stedet om 12 minutter” eller ”hold en avstand på minst 100 m fra bygningen”.

3.3.2 TIDLIGERE OG PÅGÅENDE TILTAK I POLITIET

Politiet har tidligere (2010) forsøkt å innføre mottak av SMS-nødmeldinger fra publikum. Dette initiativet strandet da det ikke var tilstrekkelig forankret i etaten og i operasjonssentralene. Det var heller ikke klarlagt retningslinjer for bruk og håndtering, som implementering av nye arbeidsprosesser og oppgaver.[30] For å unngå at det samme skjer igjen, vil det være viktig at nødvendig forankring, retningslinjer og opplæring er på plass.

Vestfinnmark politidistrikt har fått utviklet en prototype på en mobilapp som gjør at du kan bestille pass, anmelde en sak eller chatte med politiet på telefonen eller på nettbrettet. Den gir også publikum anledning til å sende inn bilder

[30] http://www.aftenposten.no/nyheter/iriks/Stanset-SMS-nodmeldinger-i-2010-7268767.html#.UgTPRLzhX6w

og tips til politiet, eller uttrykke misnøye med politiets arbeid. Tjenesten kalles ”nødchat”. Politidirektoratet har imidlertid stoppet videreutvikling av appen. POD jobber med å etablere en sentral løsning som tilrettelegger for mobile løsninger og ønsker at lokale initiativ skal vente på denne sentrale løsningen.[31]

Direktoratet for samfunnssikkerhet- og beredskap (DSB) har på oppdrag fra Justis- og beredskapsdepartementet ledet en arbeidsgruppe som har utredet ulike alternativer for en fremtidig tekstbasert tjeneste til nødsentralene, slik at døve, hørselshemmede og personer med talevansker skal kunne kommunisere direkte med nødetatene (2013). Arbeidsgruppen erkjenner at smarttelefonen gir interessante muligheter for digital kommunikasjon mellom publikum og nødetater, men anbefaler likevel at man i første rekke prioriterer en SMS-basert løsning. Denne skal være en del av nødnettleveransen og den tilhørende oppgraderingen av nødetatenes sentraler og være klar innen utgangen av 2014[32]. Støtte for andre former for digital kommunikasjon som bilder, video, e-post, chat/IM og app´er anbefales vurdert først etter at det nye nødnettet er ferdig utbygget, SMS-tjenesten er sikker og effektiv i bruk og mobildekningen i landet er forbedret.

Tilrettelegging for SMS-basert løsning er et steg riktig retning, men ettersom en så stor andel av den norske befolkningen allerede er daglige brukere av smarttelefonen og de kommunikasjonsmulighetene denne gir, bør likevel ambisjonsnivået i en modernisering av nød- og tipstelefonen være høyere. Nødmeldesentralenes publikumstjenester må gjenspeile dagens teknologiske muligheter og gjøre det mulig for den nødstilte å benytte den kommunikasjonsformen som oppleves som mest passende. Samtidig bør en slik modernisering følges av en refleksjon rundt hvordan publikums smarttelefoner kan innlemmes i den operative virksomheten til politiet som en ressurs som bidrar til mer politikraft.

Utviklingen av en mobil-app bør skje parallelt med tilrettelegging for SMS-basert varsling og bør ikke måtte avvente en ferdigstillelse av det nye Nødnettet.

---

[31] http://www.nrk.no/nordnytt/tommelen-ned-for-politi-app-1.11352077 og http://www.nrk.no/nordnytt/tester-ut-ny-politi-app-1.11182558

[32] http://www.tv2.no/2014/06/11/nyheter/nodnett/5687506

3.4 HÅNDTERING AV INFORMASJONSFLOMMEN

3.4.1 VIL POLITIET KLARE Å TA I MOT OG BRUKE INFORMASJONEN?

Det blir en utfordring for politiet å kunne ta i mot store mengder digitale nødmeldinger og effektivt identifisere og viderebehandle de viktige og kritiske nødmeldingene. Informasjonstilfanget til operasjonssentralene kan allerede i dag til tider bli veldig stort, spesielt når det pågår store hendelser. I tillegg er det en stor utfordring at nødnummeret blir misbrukt. Av de 14.000 telefonene som ringer 112 i Oslo hver måned blir 80 % stoppet hos sentralbordet fordi de ikke er reelle nødsamtaler. [33]

Lav terskel for å sende digitale meldinger kan føre til at det sendes mange slike meldinger til politiet. Det er rimelig å anta at mange av disse også vil være ikke-reelle nødmeldinger.

Fordelen med digitale nødmeldinger er nettopp at de er digitale og dermed kan gå rett inn i politiets øvrige informasjonssystemer. Maskiner og digitale verktøy kan være til hjelp for å automatisk behandle meldingene videre uten tap av mening. Det krever at politiet etablerer nødvendige prosesser, har nødvendige analyseverktøy og gjennomfører rett opplæring for å kunne ta i mot og behandle digitale nødmeldinger.

"Den gule lappen"

Den 22. juli 2011 kl 15.34.50 ringte et vitne inn en vitneobservasjon til Operasjonssentralen i Oslo. Vitnet hadde observert en bevæpnet mann i politiuniform og bilens kjennemerker. Beskjeden ble skrevet ned på en lapp. Denne lappen ble liggende til kl. 15.56 før den ble behandlet videre og vitnet ringt opp igjen. Opplysningene fra dette vitnet ble satt i sammenheng med annen informasjon fra vaktsentralen i regjeringskvartalet. Vedkommende som ringte opp igjen vitnet var sikker på at personen i bilen hadde noe med eksplosjonen å gjøre. Hun markerte derfor meldingen som «viktig» i operasjonsloggen og opprettet tiltaksbehandling, slik at informasjonen skulle være tilgjengelig for alle.[34]

Hadde vitneobservasjonen vært digitalisert, ville det vært enklere for systemene å passe på at den ikke ble bortglemt eller gikk tapt i slik en presset situasjon.

[33] http://dittoslo.no/indre-by/nyheter-indre-by/hadde-problemer-med-lyden-pa-tv-en-ringte-politiets-nodnummer-1.7901975
[34] NOU 2012:14, Rapport fra 22. juli-kommisjonen, s100.

Digitale nødmeldinger kan gjøre prosessen med å ta i mot, behandle og dele informasjon om situasjonsbildet raskere, og enklere, og redusere graden av feil. Mulighetene for å forenkle behandlingen av digitale nødmeldinger ligger i verktøy som kan gjøre følgende:

- Indeksere og rangere nødmeldingene etter relevans, slik at viktig informasjon vil komme frem først, samtidig som ikke-reelle nødmeldinger dempes eller skjules helt. Dette kan sammenlignes med hvordan Google-søk fungerer.

- Sammenstille informasjon i nødmeldinger med informasjon i andre registre slik at man raskt kan identifisere ytterligere, relevant informasjon.

- Innlemme viktig informasjon i situasjonsbildet slik at det kan deles med alle relevante patruljer og enheter under en aksjon etter at den er gjenkjent som relevant og viktig.

Verktøy som behandler digitale nødmeldinger kan raskt gi alle involverte tilgang til kritisk informasjon, øke situasjonsforståelsen, og samtidig redusere sannsynligheten for at meldingen blir oversett.

LEEDIR: Ny tjeneste gir politiet hurtig tilgang til bilder og video fra publikums smarttelefoner

Los Angeles Sheriff´s Department har sammen med selskapene CitizenGlobal og Amazon Web Services utviklet en bilde- og videodatabase som politi og nødetater kan aktivere i en større krise. LEEDIR (Large Emergency Event Digital Information Respository) er en skybasert tjeneste som politiet enkelt kan aktivere ved behov.

Straks tjenesten er aktivert, varsles publikum via en app på smarttelefonen og oppfordres til å sende inn bilder og video til denne databasen. Informasjonen kan sendes inn anonymt. Etter hvert som datamengdene vokser, utvides størrelsen på databasen automatisk. Tjenesten håndterer mange ulike filformater, gjør det mulig for publikum å sende inn store filer ved behov og tilbyr dessuten politiet et brukergrensesnitt som gjør det mulig å:

- Kommentere og organsere bilder og video som kommer inn. Verktøyet gjør det også enkelt å hente ut tilleggsinformasjon knyttet til dataene, som f.eks. geografisk posisjon og kontaktinformasjon hvis slik informasjon er gjort tilgjengelig.

- Kommunisere og samarbeide med andre analytikere som tar del i operasjonen, samt dele bestemte data med samarbeidende nødetater og andre aktører som tar del i responsen.

Tjenesten gir i så måte politiet hurtig en kontaktflate ut mot publikum som er på hendelsessted og kan dokumentere situasjonsforløpet med sine smarttelefoner.

3.4.2 ER DET PLASS I NETTET?

Når en nødsituasjon oppstår vil det typisk være mange som ønsker å kommunisere. Belastningen på nettet kan fort bli stor. Det er nettopp i en slik situasjon det vil være avgjørende at publikum kan kontakte politiet og øvrige nødetater - med både talebaserte nødanrop og digitale nødmeldinger.

Det ble gjort svært mange nødanrop umiddelbart etter at skytingen på Utøya startet. Til tross for det høye antallet nødanrop, utgjorde nødnummeret en begrenset del av den samlede teletrafikken i området – på det meste i underkant av fem prosent. [35]

Post- og teletilsynet har fremmet et *Forslag til forskrift om prioritet i mobilnettet* der man ser for seg at om lag 10 000 forhåndsdefinerte personer med samfunnsmessige behov kan bli sikret prioritet til talebasert kommunikasjon. Forslaget omhandler ikke hvordan publikum kan få prioritet, og heller ikke

[35] NOU 2012:14, Rapport fra 22. juli-kommisjonen, s168.

datakommunikasjon, dvs. kommunikasjon av digitale nødmeldinger. [36] Det er utfordrende å sikre publikum prioritet i nettet.

Det er imidlertid mulig å gjøre noen grep i en eventuell 112-applikasjon, slik at ulike datatyper prioriteres på ulik måte. Applikasjonen kan for eksempel sørge for at kun viktig og "lett" informasjon som mobilnummer, lokasjon og en kort tekst om hendelsen sendes hvis applikasjonen oppdager at det er trangt i nettet. Mer båndbreddekrevende data, som bilder og video, kan applikasjonen sende når det er tilstrekkelig plass i nettet.

På sikt kan man ha ambisjon om å likestille digitale nødmeldinger med talebaserte nødanrop. Man er imidlertid ikke avhengig av at dette er på plass for å kunne starte å nyttiggjøre seg digitale nødmeldinger.

Samtidig med at man innfører digitale nødmeldinger, og mens man høster erfaringer, kan politiet ta initiativ til å finne løsninger som gjør at digitale nødmeldinger kan likestilles med talebaserte nødanrop.

3.4.3 MANIPULERT INFORMASJON

Digitale nødmeldinger egner seg godt for maskinell behandling, men er samtidig sårbare for manipulasjon og forfalskninger. Digitale bilder kan for eksempel lett manipuleres, retusjeres og forandres på. Et utall ulike applikasjoner gjør det mulig å manipulere bilder på smarttelefonen. Dermed er det også en fare for at innsendt informasjon fra publikum kan være uriktig.

Dette er ikke et nytt problem, også i dag kan folk ringe inn uriktig informasjon. Digital manipulasjon av informasjon innsendt til politiet kan reguleres ved lov, samtidig som programvare kan brukes for å kontrollere hvorvidt et innsendt bilde er manipulert eller ikke.

[36] Forslag til forskrift om prioritet i mobilnett, Post- og teletilsynet 2013, http://www.npt.no/aktuelt/nyheter/_attachment/6481?_ts=13d3fec825e

3.5 KRAV TIL INFORMASJONSHÅNDTERING

Et større informasjonstilfang fra publikum stiller krav til at politiet håndterer informasjonen godt. Dette gjelder særlig håndtering av personsensitiv informasjon og mulighetene til å anonymisere meldinger og innhold.

3.5.1 HÅNDTERING AV PERSONSENSITIV INFORMASJON

Digitale nødmeldinger er lukket informasjon som kun er ment for politiet. Slike meldinger kan for eksempel inneholde bilder av skadde personer og folk som er tilstede ved en hendelse. Nødmeldinger kan også inneholde tilleggsinformasjon som lokasjon, helsedata og kontaktnumre til nærmeste pårørende.

For at publikum skal sende slike nødmeldinger kreves tillit til at politiet behandler personopplysninger trygt og sikkert. Både avsenders identitet og innholdet i nødmeldingene må sikres mot innsyn fra uvedkommende.

Dette innebærer bl.a. at digitale nødmeldinger må kunne sendes sikkert over nettet fra publikum til politiet og de må kunne lagres sikkert gjennom hele informasjonsbehandlingen.

Bruk, og eventuell videre bruk, av nødmeldingene må skje innenfor lovens rammer og publikum må få tydelig beskjed om hvordan informasjonen brukes.

Videre bør nødmeldinger strippes for personsensitive opplysninger når bruksformålet ikke krever slik informasjon, for eksempel når meldinger aggregeres for å følge bevegelsene til store menneskemengder under et arrangement.

Det bør også vurderes om publikum bør få større råderett over hvilken informasjon som oversendes politiet i en digital nødmelding. Hvis avsender ønsker å dele et tips med politiet, men av ulike årsaker ikke ønsker å avsløre sin lokasjon, bør avsender få anledning til enkelt å fjerne informasjon som oppleves som overflødig. Selvbestemmelse og råderett over egne data kan være viktig for at publikum skal være bekvemme med å dele informasjon med politiet.

3.5.2 ANONYMISERING

Avsenderen av en nødmelding eller et digitalt publikumstips kan av ulike grunner ønske å forbli anonym. Det kan for eksempel være fordi innholdet i

meldingen oppleves som en risiko mot egen sikkerhet. Publikum bør derfor få anledning til å sende anonyme tips hvor navn, adresse og annen informasjon som røper avsenders identitet er fjernet. Eventuelle spor på telefonen som røper at en nødmelding er sendt, slik som for eksempel en elektronisk mottaksbekreftelse fra politiet eller oppføringer i trafikkloggen på telefonen bør også fjernes. En slik anonymisering bør kunne skje ved et enkelt tastetrykk.

Bilder fra publikum vil i noen tilfeller involvere utenforstående som tilfeldigvis befinner seg på stedet der bildet blir tatt, men som ikke vet eller er innforstått med at bildet sendes politiet. Når hensikten med bildet er å styrke politiets situasjonsforståelse, for eksempel ved å dokumentere en trafikkulykke, er ofte identiteten til menneskene på stedet heller ikke interessant. Algoritmer som visker ut ansikter på bilder i nødmeldinger før de sendes politiet, kan gjøre at bildedeling med politiet oppleves som mindre inngripende. Karttjenesten Google Streetview har for eksempel visket vekk ansikter på samtlige av sine bilder.

Digitale nødmeldinger kan altså formes etter behov, og personvernvennlige løsninger kan bygges inn tidlig.

3.6 PERSONVERN OG ÅPENHETSHENSYN

3.6.1 HÅNDTERING AV OVERSKUDDSINFORMASJON

Digitale nødmeldinger vil kunne gi mer informasjon enn dagens nødanrop på telefon. Fordelen er at politiet kan trekke ut viktig informasjon som innsender selv ikke har lagt merke til. Politiet vil imidlertid også kunne trekke ut informasjon som kan vise seg å være relevant for en helt annen sak. Dette kalles overskuddsinformasjon.

Når en ringer politiet i dag så forteller man sin versjon av en hendelse. Det er innringeren som kontrollerer hvilken informasjon politiet får. Bilder, video eller videoopptak kan imidlertid gi mye mer informasjon enn en telefonsamtale. I et bilde kan en person i bakgrunnen identifiseres (så fremt denne ikke er anonymisert av avsender) og dermed knyttes til både et sted og tidspunkt som kan være relevant for en annen sak. I et lydopptak kan noe en person sier uforvarende knytte vedkommende til en annen kriminell handling. Video inneholder enda mer informasjon.

Nye sammenhenger med andre saker kan også finnes maskinelt hvis politiet kobler de digitale nødmeldingene fra publikum med egne registre og datasett og analyserer dem på tvers. Innringeren har ikke kontroll på hva politiet kan tolke og få ut av informasjonen, og heller ikke om politiet bruker informasjonen til andre formål enn det hun hadde tenkt.

Overskuddsinformasjon er ikke informasjon som er innhentet til et gitt formål. Derfor er det viktig med klare regler for hvordan politiet eventuelt skal kunne benytte overskuddsinformasjon fra digitale nødmeldinger. Når er en sak alvorlig nok til at det legitimerer bruk av overskuddsinformasjon? I hvilke tilfeller skal overskuddsinformasjon kunne sammenstilles med annen informasjon politiet sitter på? Digitale nødmeldinger som dokumenterer en brann kan være interessante fordi ildspåsetteren kan befinne seg blant publikum. Men skal bilregisteringsnummeret til en forbipasserende bil avbildet i en trafikkulykke kunne sjekkes mot en database over seksuelle overgripere?

Slike problemstillinger tilsier at politiet bør bruke overskuddsinformasjon med varsomhet og kun i spesielle tilfeller.

Det bør også foreligge eksplisitte sletteregler som sørger for at innsendte digitale nødmeldinger fra publikum automatisk slettes og ikke kan sammenstilles med annen informasjon i ubegrenset tid. Det eksisterende regelverket for frivillig avlevert DNA-materiale kan legges til grunn for en slik regulering av materiale frivillig innsendt av publikum gjennom digitale nødmeldinger (i motsetning til materiale som politiet selv har innhentet som bevis).

3.6.2 ET NYTT OVERVÅKNINGSREGIME?

Kameraovervåkning er ifølge Personopplysningsloven § 36 ”vedvarende og regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkningskamera (...) som er fastmontert”. Slik overvåking regnes som et alvorlig inngrep i personvernet og er derfor sterkt lovregulert i Norge. Tillatelse til slik overvåkning forutsetter bl.a. at den dokumenteres som nødvendig, kun omfatter et begrenset område og at opptakene slettes senest 7-30 dager etter at de er gjort.[37] Publikum skal dessuten varsles om slike kameraer på offentlige steder.

[37] Datatilsynet (2012, rev. 2013): *”Kameraovervåking – hva er lov?”*

I Norge fantes det kun 12 politikameraer på landsbasis i 2013. Til forskjell har London mer enn 12 000 politikameraer plassert på ulike steder i byen.[38] Bilder fra slike overvåkningskameraer var viktige i den umiddelbare etterforskningen av bombeangrepene i London i 2005. I Boston kom de fleste bildene imidlertid ikke fra politikameraer, men fra smarttelefoner og private overvåkningskameraer.

Håndholdte kameraer, slik som mobiltelefoner, er ikke omfattet av denne lovgivningen. Samtidig viser erfaringene fra Boston at "crowdsourced surveillance" kan være et kraftigere overvåkningsverktøy enn tradisjonell kameraovervåking. Med en smarttelefon i hver jakkelomme, er det svært sannsynlig at større hendelser på befolkningstette steder vil dokumenteres grundig. Kroppsnær teknologi som "Google Glass" vil bare forsterke denne trenden ytterligere, og slik kan «crowdsourced surveillance» lett fungere som en "erstatning" for mer utstrakt politiovervåking. Vedvarende personovervåking kan ikke lenger forbindes med et kamera fastmontert på et bestemt sted, hvis det finnes kamera overalt hvor det finnes folk.

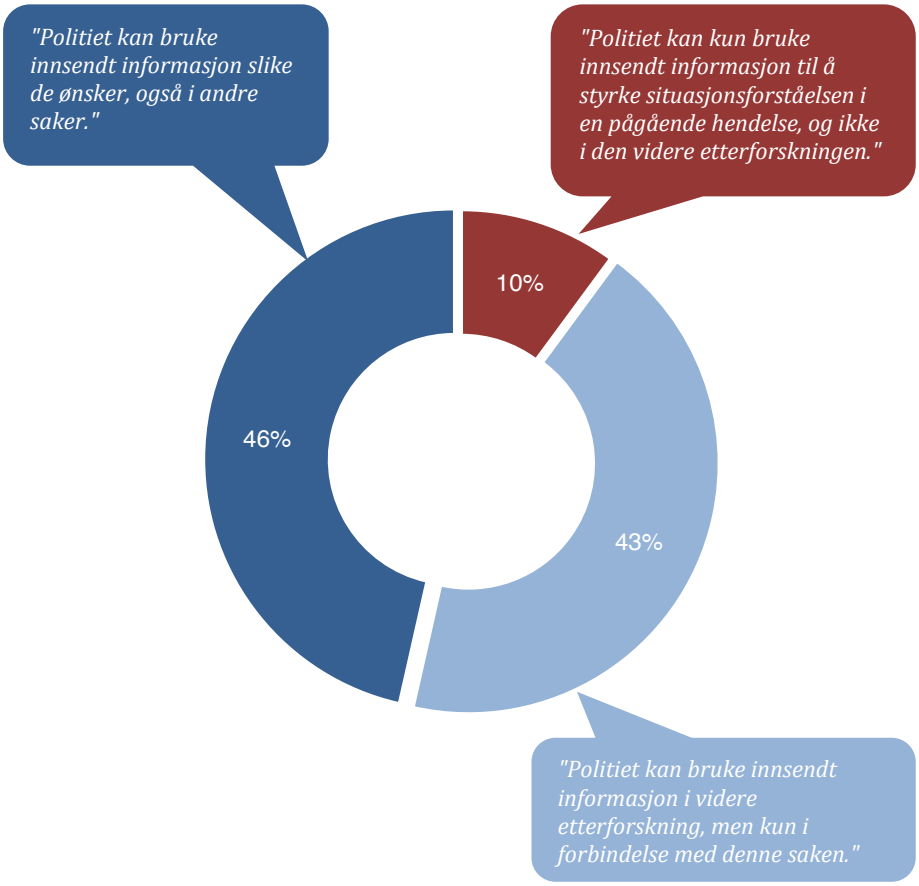
Hvordan kan vi garantere vi at overvåkningen er godt begrunnet, nødvendig og tilstrekkelig begrenset når publikum tar bildene og ingen styrer kameraet?

Erfaringene fra Boston viser dessuten at en utstrakt bruk av publikumsbilder og videomateriale i umiddelbar etterforskning etter en større hendelse, kan by på problemer:

- Uskyldige personer kan lettere innblandes i en etterforskningen fordi de tilfeldigvis er fotografert på "feil sted, til feil tid".
- Dette kan i sin tur bidra til å avlede politiets ressurser i en tid hvor det er viktig å handle hurtig og prioritere riktig. Samtidig kan det være svært ubehagelig for publikum å bli innblandet på denne måten.
- I en større krisesituasjon kan det fort oppstå et press om å handle på bakgrunn av innsendt informasjon fra publikum, uten at denne er tilstrekkelig verifisert.

[38] https://www.datatilsynet.no/Nyheter/2013/Bare-tolv-politikameraer-i-Norge/

Hvordan skal politiet få bruke bilder og video som er innsendt fra publikum?



4. POLITIET I SOSIALE MEDIER

Sosiale medier er en stor spreder av digital informasjon. Nordmenn er blant de ivrigste brukerne av sosiale medier i europeisk sammenheng[39]. I 2012 var hele 80 prosent medlem av et sosialt nettverk.[40]

Store mengder data lastes hver dag opp og deles i nettet. Mye av dette er åpen informasjon. Disse dataene utgjør en verdifull ferskvare. Riktig analyse av sanntidsdata fra sosiale medier kan gi rask oversikt over en situasjon. Markedsføringsselskaper benytter seg allerede av slike data for å bl.a. å overvåke populariteten til merkevarer og kjapt kunne tilpasse og styre markedsføringskampanjer.

Sammen med en tiltagende utvikling av nye verktøy som kan analysere informasjonen som deles på slike plattformer, åpner den brede populariteten til sosiale medier nye muligheter for politiet. Erfaringer fra andre land viser at informasjon som deles på sosiale medier bl.a. kan brukes til:

- Å avsløre kriminell aktivitet eller planer om kriminelle handlinger
- Å gi viktige etterretningstips om grupper eller individer

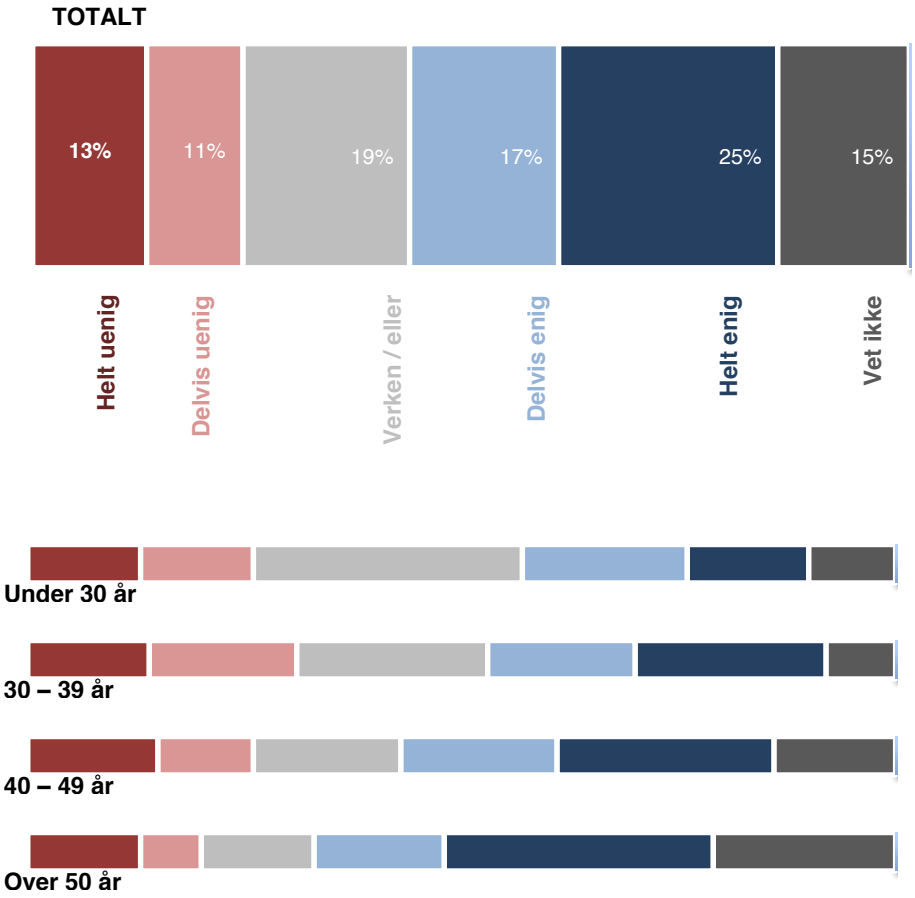
[39] http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics
[40] Facebook er det desidert største sosiale nettverket i Norge – 79 prosent av kvinnene og 72 prosent av mennene er medlem. Twitter (20 prosent), LinkedIn (17 prosent) og Instagram (15 prosent) er også populære. Hele 93 prosent av nordmenn i alderen 15-29 har en Facebook-konto, mens over halvparten av de over 60 år er på Facebook. TNS Gallup for Teknologirådet/Datatilsynet januar 2013

- Å bidra til tidlig varsling i krisesituasjoner eller større hendelser
- Å gi en styrket situasjonsforståelse og bedre oversikt
- Å gi et tettere samarbeid med publikum, med bedre forståelse av deres opplevelse av politiet og hva som opptar dem.

Dette kapittelet vil ta for seg hvordan sosiale medier kan gi politiet tidlig varsling, styrket situasjonsforståelse og et tettere samarbeid med publikum.

Mulighetene for både forebyggende og operativ virksomhet er store. Samtidig byr nye informasjonskilder ikke bare på tekniske utfordringer, men reiser også viktige verdispørsmål. Sosiale medier er en relativ ny aktør i et digitalt informasjonslandskap i kraftig utvikling, hvor gamle grenser mellom hva som betraktes som privat og offentlig er i stadig forandring. Erfaringene fra bl.a. den arabiske våren, og mer nylig den politiske uroen i Ukraina, viser dessuten at sosiale medier får en stadig viktigere plass i det offentlige ordskiftet. Ved større hendelser har sosiale medier blitt en viktig arena for ytringer. Da er det viktig at politiets bruk av sosiale medier ikke virker hemmende på andre viktige samfunnsroller sosiale medier vil kunne komme til å spille fremover.

Jeg synes politiet bør følge med på nøkkelord som "demonstrasjon", "Holmenkolldagen", "gjeng", osv. i åpne sosiale medier.



4.1 PASSIV TILSTEDEVÆRELSE: OVERVÅKING AV SOSIALE MEDIER

Oslo-politiet har fått mye ros for sin bruk av Twitter for å styrke sin synlighet og kontakt med publikum. Sosiale medier kan imidlertid også inneholde nyttig informasjon som politiet kan bruke til å styrke situasjonsforståelsen og løse sine oppgaver. Vi skal i det følgende se hvordan bruk av sosiale medier kan:

- Bidra til tidlig varsling
- Gi raskt overblikk over akutte situasjoner
- Identifisere nye vitner

Deretter vurderes utfordringer og begrensninger knyttet til slik informasjon.

Meldinger i sosiale medier kan som nødmeldinger og tips inneholde tekst, bilder, video og i noen tilfeller stedsangivelse. De skiller seg imidlertid vesentlig fra digitale tips- og nødmeldinger på to områder:

- informasjon på sosiale medier er sjeldent spisset informasjon som er rettet mot politiet
- det kan være krevende å finne relevant, korrekt informasjon som kan verifeseres

Dette gjør at sosiale medier må behandles på en annen måte enn digitale nødmeldinger. En effektiv håndtering og tolkning av et korpus av informasjon vil være viktigere enn å kvalitetssikre enkeltmeldinger. Meldinger i sosiale medier blir i denne rapporten vurdert som verdiøkende tilleggsinformasjon til nødmeldinger.

4.1.1 TIDLIG VARSLING

En sentral egenskap ved sosiale medier er at meldinger sprer seg raskt og bredt i befolkningen, både lokalt og globalt. Under orkanen Irene i USA ble det postet mer enn 3000 Twitter-meldinger per minutt. Ett minutt etter jordskjelvet i Virginia i 2011 var det 40.000 kommentarer om det på Twitter. Innbyggerne i New York fikk høre om hendelsen på Twitter 30 sekunder før selve skjelvet kunne merkes i byen[41].

[41] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

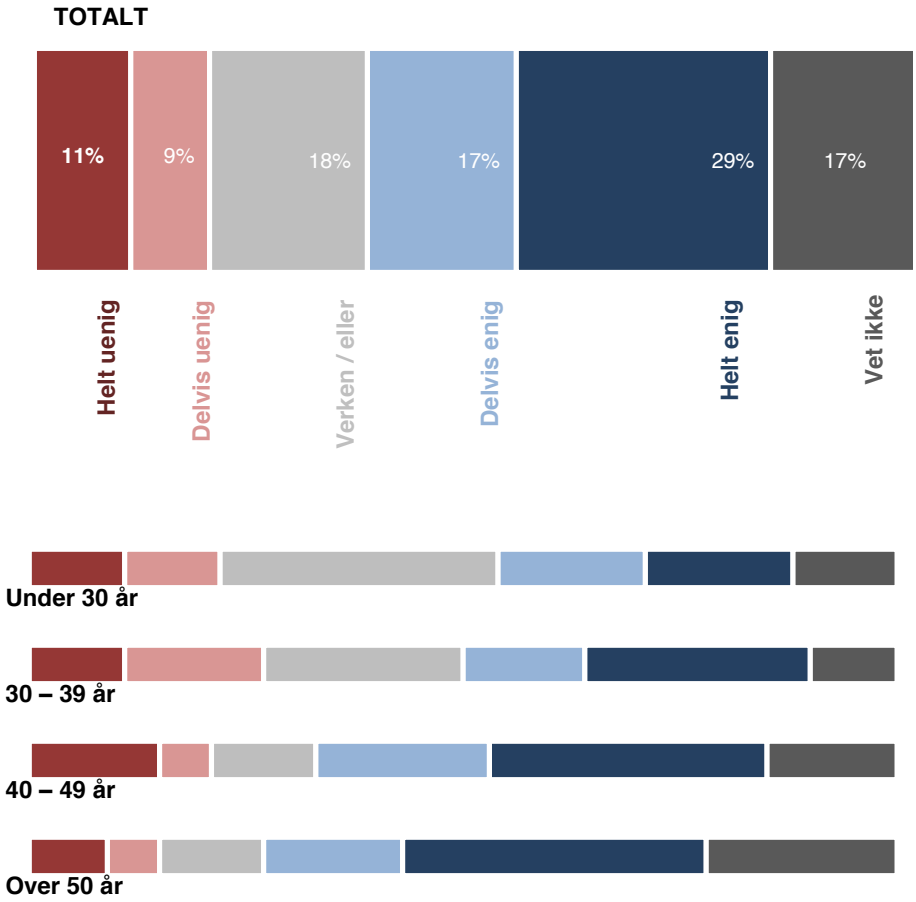
Amerikanske Geological Survey har utviklet en jordskjelv-detektor basert på sanntidsinformasjon fra meldinger på Twitter. Detektoren overvåker Twitter-meldinger som omhandler jordskjelvrelaterte ord, og legger til sted, tid og kvantitative data. På den måten hevder de at de kan varsle jordskjelv innen 60 sekunder fra utbruddet. Til sammenligning kan tradisjonelle, sensorbaserte alarmer ta mellom 2-20 minutter[42]. Denne samlingen av meldinger danner samtidig en sentral katalog over korte førsteinntrykkshistorier og bilder fra publikum på stedet der jordskjelvet har slått til.[43] I tillegg til å kunne varsle jordskjelvet tidligere vil man også kunne få dannet seg et bilde av omfanget.

Jordskjelvdetektoren er et eksempel på hvordan det at mange snakker om en hendelse i sosiale medier kan styrke situasjonsforståelsen og gjøres om til handlingsorientert informasjon. Politiet kan også utvikle slike varsler, for både planlagte hendelser som man allerede har på radaren, og for uforutsette hendelser.

Kontinuerlig overvåking av nøkkelord på sosiale medier kan brukes som et varsel om at noe vesentlig skjer eller er i ferd med å skje. Dataprogrammer som kan identifisere og analysere slike signaler i sosiale medier kan være et viktig supplement for politiet for å oppdage hendelser som har skjedd, eller tilløp til hendelser.

[42] http://www.livescience.com/45385-earthquake-alerts-from-twitter.html
[43] http://recovery.doi.gov/press/us-geological-survey-twitter-earthquake-detector-ted/

Jeg synes politiet bør følge med på ord som "skyting", "eksplosjon" og "slåssing" i åpne sosiale medier som Twitter for å fange opp om noe har skjedd.



4.1.2 SITUASJONSFORSTÅELSE: RASKT OVERBLIKK

I krisesituasjoner, så vel som daglige hendelser, er det viktig for politiet raskt å danne seg et overordnet bilde av hva som skjer. Det vil ikke nødvendigvis være tilstrekkelig å kartlegge antall meldinger med gitte nøkkelord – politiet vil være interessert i det relevante informasjonsinnholdet i meldingene.

Ved mindre hendelser med liten aktivitet på sosiale medier vil det være en relativt enkel oppgave å hente ut relevant informasjon. Imidlertid vil informasjonsmengden raskt kunne øke under større hendelser eller når det er stor aktivitet på sosiale medier. Gode analyseverktøy er en forutsetning for at politiet skal kunne hente ut relevant informasjon i sosiale medier på en effektiv måte. Ulike analyseteknikker gjør det mulig å trekke ut relevant informasjon fra store mengder data, bl.a.:

- Kartlegge frekvensen av ulike ord og uttrykk
- Hente semantisk mening fra store mengder tekst
- Sortere og filtrere meldinger etter ulike kriterier
- Kartlegge nettverk mellom ulike aktører
- Redusere støy

LONDON FIRE BRIGADE OVERVÅKER SOSIALE MEDIER

London Fire Brigade følger aktivt med på Twitter. De søker gjennom meldinger og ser etter nøkkelord som passer med hendelser de har blitt varslet om. Skulle det begynne å brenne et sted i London, søker en operatør på navnet på gaten, området, eller de omkringliggende bygningene på Twitter for å se om noen twitrer om hendelsen i dette området. De mener selv at dette er en god måte å få med seg hva folk ser og opplever før de kommer til stedet selv. [44]

4.1.3 IDENTIFISERE NYE VITNER

Analyseverktøy kan identifisere de mest sentrale formidlerne av en hendelse i sosiale medier. Det kan være de som har postet flest meldinger, eller de som har postet meldinger som er blitt delt videre flest ganger. Dette er indikatorer på at vedkommende kan sitte på relevant informasjon for politiet og muligens være interessant å kontakte for oppfølging og kvalitetssikring av informasjon.

[44] Samtale med representant fra London Fire Brigade.

4.1.4 EKSEMPEL: 22. JULI 2011 PÅ TWITTER

Twitter ble hyppig brukt under terrorangrepene 22. juli 2011. Ved hjelp av analyseverktøyet Topsy[45] har vi filtrert ut Twitter-meldinger fra denne dagen som enten inneholder ordet ”eksplosjon” eller ordene ”skyting” eller ”skudd”. Figur 2 viser den kumulative forekomsten av meldinger som inneholdt disse ordene og som ble delt på Twitter i løpet av ettermiddagen 22. juli 2011.

Figur 2 viser en kraftig økning i antall meldinger med ordet ”eksplosjon” kort tid etter eksplosjonen i Regjeringskvartalet. En tilsvarende kraftig økning i meldinger med ordene ”skyting”/”skudd” er også tydelig kort tid etter at de første skuddene ble avfyrt på Utøya.

Muligheter i maskinanalyse

Figur 2 viser samtidig at Twitter-meldinger kan betraktes som digitale signaler og at en delautomatisert analyse av slike signaler vi kunne fungere som et varsel: hadde politiet ikke blitt varslet via andre kanaler og kun overvåket ordene ”skyting”/”skudd” på Twitter, ville de kort tid etter at gjerningsmannen avfyrte første skudd på Utøya fått en sterk indikasjon på at en skyteepisode var i gang.

Den bratte stigningen i kurvene i Figur 2 viser dessuten en kraftig økning i antall meldinger på svært kort tid. En slik unormal oppførsel kan muligens indikere at hendelsen har et stort omfang og vil kanskje også kunne fungere som en alarm.

Maskinell analyse av sosiale medier kan gjøre det lettere å håndtere store mengder informasjon og hente ut viktig å relevant informasjon. I denne enkle øvelsen kommer f.eks. de to ulike hendelsene som inntraff 22. juli 2011 tydelig tilsyne.

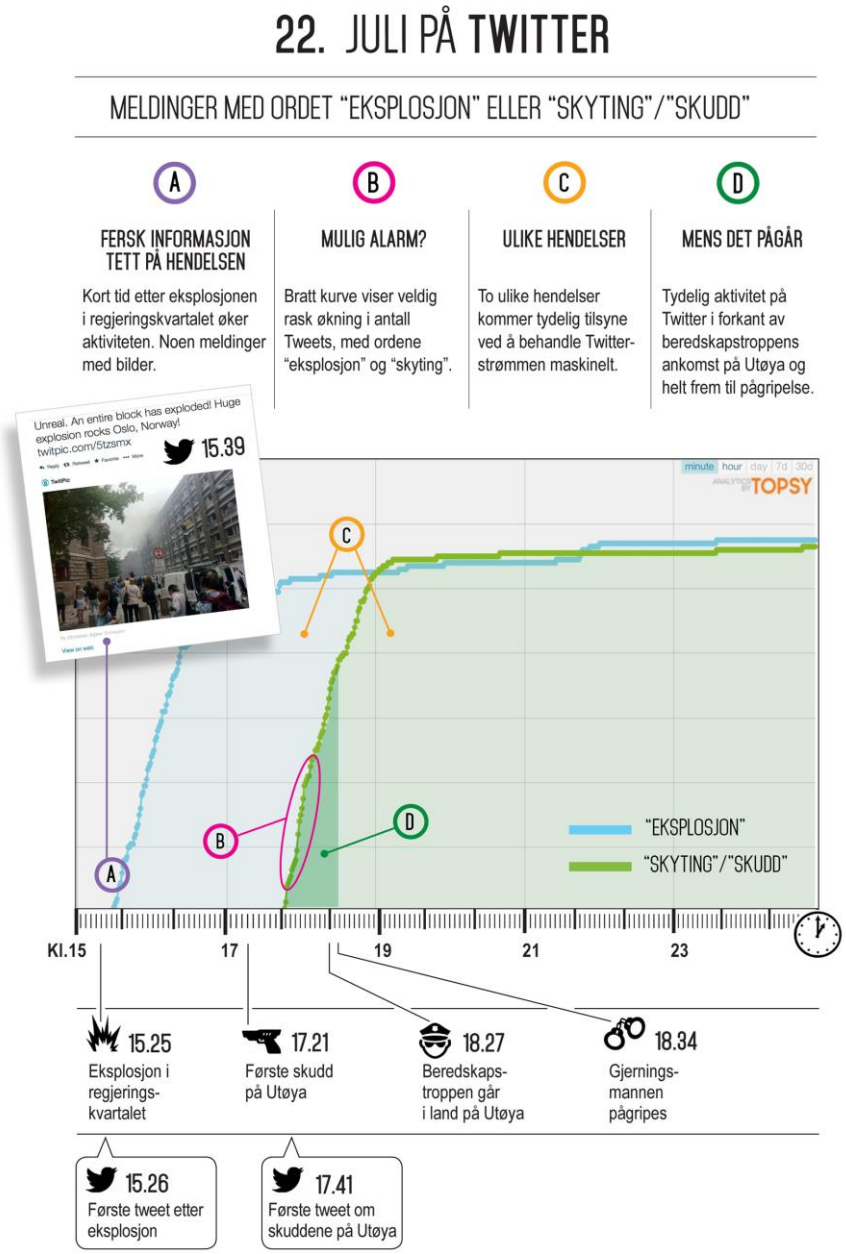
Fersk informasjon, tett på hendelsen

Kort tid etter eksplosjonen i Regjeringskvartalet øker aktiviteten på Twitter. Mye av denne informasjonen vil muligens være gjentagelser, men av og til vil det også komme meldinger med informasjon som kan bidra til å styrke politiets situasjonsforståelse. Eksempelvis ble det 14 minutter etter eksplosjonen postet et publikumsbilde fra Regjeringskvartalet på Twitter.

---

[45] www.topsy.com

Figur 2 viser dessuten at publikum også er aktive på Twitter både umiddelbart etter eksplosjonen i Regjeringskvartalet og både i forkant av beredskapstroppens ankomst på Utøya og helt frem til gjerningsmannen pågripes. Sosiale medier gir i så måte muligheter for politiet til å styrke sin situasjonsforståelse i en kaotisk situasjon, mens en hendelse utfolder seg.



Figur 2 Twitter-meldinger fra 22. juli 2011 analysert ved hjelp av analyseverktøyet TOPSY (Grafikk av Birigitte Blandhoel).

4.2 AKTIV TILSTEDEVÆRELSE: KOMMUNIKASJON MED PUBLIKUM

4.2.1 KORRIGERE INFORMASJON

Politi- og nødetaten i Norge har allerede en tilstedeværelse i sosiale medier. Her orienterer de om hendelser og spesielt ransutsatte steder, gir tips og advarsler, korrigerer rykter og feilinformasjon, eller de orienterer om det indre liv i politiet. Operasjonssentralen i Oslo har med sin Twitterbruker "@oslopolitiops" over 131 000 følgere på Twitter[46] og er blant de fem mest fulgte Twitterbrukerne i Norge[47]. Facebookbrukeren "Utrykningspolitiet" har nærmere 63 000 likes[48].

Operasjonssentralen på Twitter

Operasjonssentralen, kjent som @oslopolitiops på Twitter, fikk prisen «Årets beste tweet» for denne uttalelsen: «**Storo: Vi fikk melding om pågående husbråk med kvinneskrik. Da vi kom fram fant vi et sykepleier-vorspiel. Vi forlater stedet snart.**» Juryens begrunnelse var bla. «(…) har plukket en vinner som om og om igjen har tvitret på en måte som har gitt følgerne helt ny innsikt i en aktør som både er elsket og hatet.»[49]

En slik aktiv tilstedeværelse i sosiale medier gir politiet en god plattform for rask spredning av riktig og oppdatert informasjon, samt til å korrigere feilinformasjon og rykter. Meldinger fra politiet kan også enkelt deles videre. På den måten får man en bred og rask spredningseffekt som kan supplere mer formelle informasjonskanaler.

Rask spredning av korrekt informasjon vil også indirekte kunne påvirke diskusjonene i sosiale medier slik at disse i størst mulig grad baserer seg på riktig informasjon. Det vil øke publikums forståelse for situasjonen og bidra til en større trygghetsfølelse. Videre vil det også kunne føre til at politiet får mer korrekt informasjon fra publikum.

---

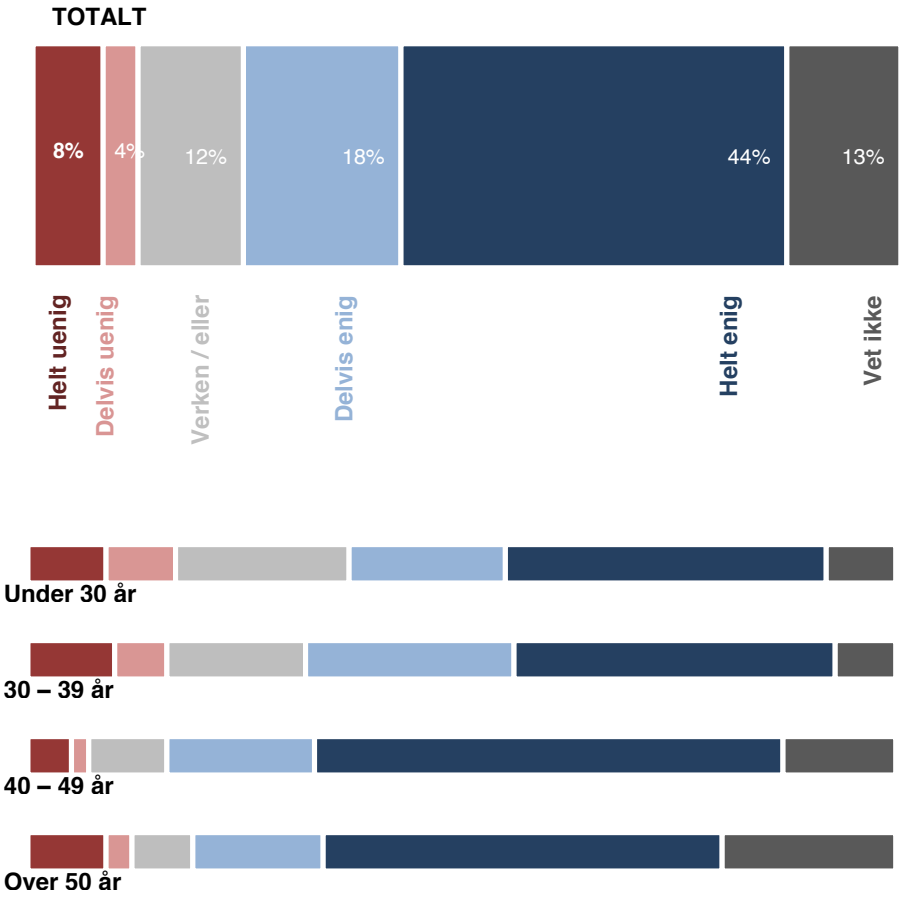
[46] https://twitter.com/oslopolitiops, august 2014
[47] Rangering ifølge tvitre.no/norsktoppen
[48] https://www.facebook.com/utrykningspolitiet
[49] http://www.kampanje.com/markedsforing/article6482988.ece

Kvalitetssikring av informasjon

For å klart skille meldinger fra politiet fra andre meldinger og for å tydeliggjøre sitt budskap, kan politi- og nødetater ta i bruk forhåndsdefinerte nøkkelord (”emneknagger”) i offisielle meldinger. Dersom politiet fanger opp rykter og uriktig informasjon kan de poste en melding for å korrigere et rykte og komme med riktig informasjon ved å merke meldingen med ”#AVKREFTER RYKTE: xxx”.
Andre ganger kan politiet ønske å komme raskt ut med informasjon, før innholdet er verifisert. Da kan meldingene merkes med ”#UVERIFISERT: xxx”.

Slike forhåndsdefinerte nøkkelord vil sørge for at politiets meldinger synes tydelig i meldingsstrømmen og vil også kunne fanges opp av søkemotorer og analyseverktøy.

Det er greit at politiet tar kontakt med meg fordi jeg har lagt ut informasjon i sosiale medier om en alvorlig hendelse.



4.2.2 ENGASJERE PUBLIKUM

Politiet i Norge har lang tradisjon for å samarbeide tett med publikum. Godt samarbeid og god kommunikasjon med publikum kan være nyttig i forebyggende sammenheng for å fange opp tidlige utviklingstrekk i eget distrikt, for å få inn tips i en konkret hendelse, og for å bedre forstå årsaker og mulige løsninger på problemer.

Publikum både ønsker og har vilje til å bidra med egne erfaringer og samarbeide åpent med politiet[50]. Politiet kan videreutvikle sin tilstedeværelse i sosiale medier for å engasjere publikum, samarbeide med dem, og dermed få mer målrettet informasjon som de kan bruke videre i sitt arbeid. Gjennom aktiv tilstedeværelse kan politietatene jevnlig publisere åpent materiale, korrigere informasjon og rykter, konsultere lokalsamfunnet, og få feedback og respons. Det åpner også opp for å fjerne feilaktig informasjon og falske rykter så vel som informasjon som krenker andres personvern.

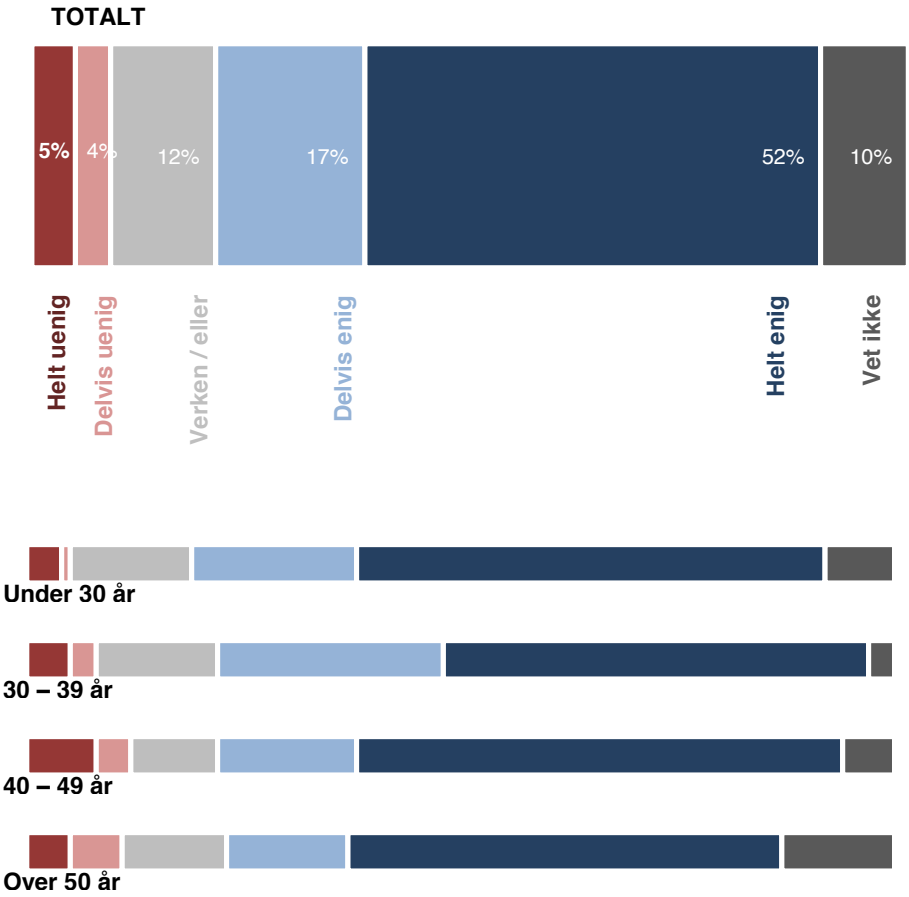
Aftenpostens Oslo Puls har laget et kart der folk kan angi på hvilke steder i Oslo de føler seg utrygge[51]. Publikum kan selv zoome inn på et sted på kartet og skrive inn sine merknader. Andre kan stemme over innlegget, og på den måten angi om de selv har en lignende opplevelse av stedet. Tjenesten er moderert. Disse innspillene gir en god indikasjon på hvilke steder som folk opplever som utrygge i Oslo og er et godt eksempel på hvordan politiet kan engasjere og bruke publikum aktivt i sitt arbeid.

---

[50] Iversen og Dahl (2010): *Politi 2.0: Kan sosiale medier bidra til økt dialog og samhandling mellom politi og publikum?*

[51] http://www.aftenposten.no/nyheter/oslo/Her-foler-oslofolk-seg-utrygge-7112377.html#.UWkjYxmlgn9

Politiet bør bruke sosiale medier som informasjonskanal til publikum, for eksempel til massevarsling ved større hendelser.



KØBENHAVNS TRYGGHETSINDEKS

København kommune har gjennomført en spørreundersøkelse hvor publikum har blitt spurt om sine egne opplevelser med kriminalitet og vurderinger av kriminaliteten i nabolaget. Publikums tilbakemeldinger har deretter blitt sammenstilt med politiets egne data. Til sammen utgjør dette en såkalt "Trygghetsindeks". Trygghetsindeksen indikerer hvor stort behovet er for trygghetsskapende innsats i ulike områder i København.[52] En representant fra København kommune uttaler at "tryggheten i København er stigende og beboerne er mindre utsatt for kriminalitet" etter at de startet med kartleggingen[53].

Politiet i flere land har på liknende vis høstet gode erfaringer med å både følge med på og engasjere publikum på sosiale medier. Vi har funnet inspirasjon fra New Zealand og Storbritannia.[54]

[52] http://subsite.kk.dk/sitecore/content/Subsites/tryghedsindeks/SubsiteFrontpage.aspx
[53] http://www.aftenposten.no/nyheter/oslo/Her-foler-oslofolk-seg-utrygge-7112377.html
[54] http://www.civildefence.govt.nz/memwebsite.nsf/Files/CDEM%20resilience%20fund/$file/Greater-Wellington-Social-media-in-an-emergency-A-best-practice-guide-2012.pdf

OPPTØYER I LONDON

Høsten 2011 brøt det ut mange opptøyer i London som raskt spredde seg over hele England. London Metropolitan Police (MPS) hadde samme sommer ansvar for sikkerheten ved sommerolympiaden, diamantjubileet til dronningen og det årlige Notting Hill-karnevalet.

MPS fant ut at de måtte gjøre mer for å engasjere seg i lokalsamfunnet gjennom sosiale medier, med tanke på å avverge uro, bedre ressursplanlegging og stimulere til proaktivt engasjement.

MPS satt i gang et pilotprosjekt som hjalp dem å lage en langsiktig strategi for bruk av sosiale medier. Pilotprosjektet visste bl.a. at sosiale medier gjorde det mulig å identifisere mulige hendelser mye raskere og mer nøyaktig enn på tradisjonelle måter. Dette gjorde politiet bedre i stand til å iverksette målrettede tiltak. De klarte også å identifisere flere potensielle vitner til en knivstikkingsepisode. Pilotprosjektet hjalp dessuten politiet med å bygge en ordliste med søkeord som styrket tilfanget av relevant informasjon. [55]

4.2.3 FORUTSETNINGER FOR GOD DIALOG GJENNOM SOSIALE MEDIER

Jevnlig publisering og korrigering av informasjon til publikum, kombinert med kontinuerlig innhenting av informasjon fra publikum, vil kunne danne en god sirkel for effektiv informasjonsbehandling i politiet. For at en slik dialog med publikum skal fungere mest mulig effektivt, forutsetter det at politi- og nødetater:

- Fortløpende publiserer oppdatert, korrekt og relevant informasjon om pågående og planlagte hendelser (både på eget nettsted og på andres nettsteder). Ved å være raskt ute med riktig informasjon i mange kanaler kan politiet redusere (feilaktige) spekulasjoner.

- Markerer tydelig hva som er informasjon fra politiet slik at det blir lett for andre (både mennesker og maskiner) å gjenkjenne at meldingen er fra en offentlig etat, og samtidig gjøre det lettere å dele videre.

- Overvåker sentrale nøkkelord for raskt å fange opp feilaktig informasjon, og korrigerer falske rykter blant publikum (både på egne og andres nettsteder).

[55] Metropolitan Police leverage social media to engage local community with HP social media analytics tools (Case study/4AA4-5393EEW.pdf), http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA4-5393EEW

- Modererer og korrigerer feilaktig informasjon og personsensitiv informasjon på egne nettsteder.

- Publiserer informasjon og tilrettelegger/setter i gang diskusjoner rundt tematikk og problemområder man ønsker tilbakemeldinger på.

Figur 3 Informasjonshjul for en operasjonalisert bruk av sosiale medier i politiet.

4.3 UTFORDRINGER OG BEGRENSNINGER

4.3.1 KAN POLITIET STOLE PÅ SOSIALE MEDIER?

Bruk av informasjon i sosiale medier kan også by på utfordringer for politiet. Informasjonen kan være feil, villedende eller upresis, enten bevisst eller ubevisst. Noen ganger kan folk trekke feil slutninger og feilaktig informasjon kan spres raskt.

Politiet har høye krav til verifisering og kvalitetssikring av informasjonen som de får fra publikum. Innhentet informasjon kan kryssjekkes med annen type informasjon. Ofte blir vitner ringt opp for å verifisere hendelser.

Meldinger i sosiale medier er i utgangspunktet ikke ment for politiet. I mange tilfeller vil politiet måtte tolke slike data for å trekke ut relevant informasjon. Dette medfører selvfølgelig også en større mulighet for misforståelser og feiltolkninger.

Dette gir politiet utfordringer på flere områder:

- hvordan kan og bør politiet kvalitetssikre informasjon fra sosiale medier for eget bruk, uten å miste sanntidsverdien til slik informasjon?
- hvordan kan og bør politiet engasjere seg for at publikum i størst mulig grad får riktig informasjon raskt nok?

4.3.2 VERIFISERE OG KVALITETSSIKRE

Det vil være både vanskelig og tidkrevende å manuelt verifisere informasjon i sosiale medier med de kvalitetskrav som normalt er påkrevd i politiet. Dette gjelder spesielt under store kriser hvor mye informasjon må håndteres på kort tid. Sosiale medier har sin styrke i en større samling av materiale. Hver enkelt melding vil ikke bestandig ha samme nytteverdi eller kunne kvalitetssikres på samme måte som digitale tips- og nødmeldinger. Imidlertid kan analyseverktøy være til hjelp.

Når mange meldinger beskriver den samme situasjonen kan det være en indikasjon på at hendelsen er reell. Analyseverktøy kan også hjelpe til med å verifisere både om en hendelse har funnet sted og til å kvalitetssikre informasjonen.

I situasjoner der det kommer inn store mengder digitale nødmeldinger og nødanrop til politiet, kan analyser av sosiale medier brukes for å supplere, verifisere og kvalitetssikre situasjonsbildet.

Kvalitetssikring av informasjon kan også gå gjennom publikum. Sosiale medier vil kunne fungere som arena for å oppdage og rette opp feilaktig informasjon fra politi- og nødetater. Operasjonssentralen i Gudbrandsdalen sier at de

bruker Twitter for å " kvalitetssikre informasjonen frå politiet".[56] Politiet kan også bruke publikum til å verifisere påstander: "Har det gått et ras over riksvei 88?" eller "Hørte noen det smelle i Nordberggata?", kan enkelt besvares med "ja" eller "nei" av publikum på sosiale medier.

4.4 PERSONVERN OG ÅPENHET

Det reiser seg flere prinsipielle spørsmål knyttet politiets bruk av sosiale medier. Sosiale medier gir politiet både ny informasjon som kan styrke situasjonsforståelsen, samt en ny plattform for kommunikasjon og samarbeid med publikum. Disse mulighetene må imidlertid vurderes opp mot viktig spørsmål knyttet til personvern og åpenhet.

4.4.1 EKSPONERING OG FORHÅNDSDØMMING

Rett etter eksplosjonene under Boston Marathon i 2013 engasjerte både Boston Police Department, FBI og flere sosiale nettsteder publikum for å innhente bilder og annet materiale som brukes i etterforskningen. Selv om politiet forsøkte å kanaliserte svarene i egne dedikerte kanaler (telefonnummer og e-postadresse), ble også publikum engasjert i åpne, sosiale medier. Der utviklet det seg etter hvert en egen etterforskning, drevet frem av diskusjoner publikum imellom. På det åpne diskusjonsforumet Reddit ble en student feilaktig identifisert som mistenkt. Umiddelbart etter ble bilder og annen informasjon om vedkommende samlet og spredt bredt. Bildene nådde til og med forsiden av New York Post. [57]

Erfaringene fra Boston viser at smarttelefoner og sosiale medier gjør det mulig for publikum å støtte politiarbeidet med verdifulle data. De viser imidlertid også at publikum fort kan bli overivrige bidragsytere. Når engasjementet blir sterkt kan publikum, med god støtte fra nye kommunikasjonsverktøy og hurtig informasjonsspredning på sosiale medier, enkelt sette i gang sin egen parallell-etterforskning. En slik utvikling kan ha svært uheldige konsekvenser, som i Boston hvor publikum trakk feilaktige konklusjoner som raskt ble spredt. Dette kan også virke hemmende for politiarbeidet. Derfor er det nød-

[56] http://www.fjuken.no/index.cfm?event=doLink&famID=318350&frontFamID=84050
[57] http://www.bbc.co.uk/news/technology-22214511

vendig med tydelige mekanismer som gjør at publikum først og fremst bidrar med informasjon, og ikke tar del i etterforskningen.

4.4.2 PERSONSENSITIV INFORMASJON

Vitneobservasjoner kan inneholde personsensitiv informasjon, og kan krenke andres personvern. Denne type informasjon egner seg ikke for åpne diskusjoner. Visse typer informasjon vil av taktiske grunner heller ikke egne seg for å deles åpent.

Politiet har likevel ikke ansvar for og kontroll over hva som formidles åpent i sosiale medier. I utgangspunktet kan alle ytre seg fritt i sosiale medier så fremt de holder seg innenfor den alminnelige bestemmelsen om ytringsfrihet i Grunnloven § 100. Erfaringene fra Boston bekrefter likevel behovet for en bevisst strategi for bruk av sosiale medier i politiet.

Politiet kan imidlertid redusere faren for at personsensitiv informasjon blir spredd ved å

- moderere diskusjoner i sine egne sosiale mediekanaler
- dirigere personsensitiv informasjon til lukkede kanaler inn til politiet som telefon, SMS, MMS og digitale tips- og nødmeldinger.

4.4.3 FÅR VI EN NEDKJØLINGSEFFEKT?

Vi ønsker et åpent samfunn med fri ytring, uten at det vi sier i sosiale medier blir lagret og analyseres av statlige aktører og brukes mot oss senere. Samtidig ønsker vi at politiet skal ha de beste forutsetninger for å løse sine oppgaver på best mulig måte. Men hvis vi vet at politiet følger med på sosiale medier, vil vi da ytre oss annerledes eller bruke tjenestene på andre måter?

Når folk unnlater å bruke en tjeneste eller på ulike måter modererer og begrenser egen bruk av frykt for hvordan opplysningene kan brukes, omtales dette som en ”nedkjølingseffekt”. En slik nedkjøling kan følge av både bevisste og ubevisste valg vi gjør.

I en undersøkelse Teknologirådet har gjort i samarbeid med Datatilsynet, svarer 1 av 4 nordmenn at de har unnlatt å skrive under på et opprop fordi de

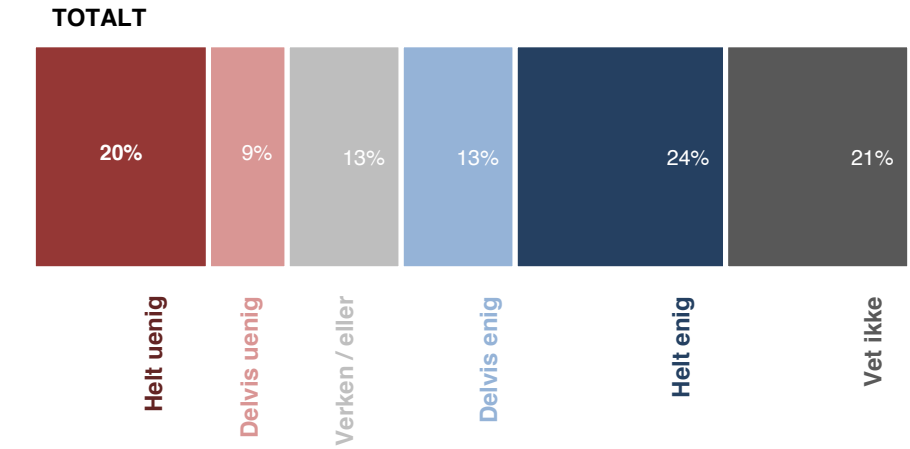
er usikre på hvordan opplysningene kan bli brukt senere. 1 av 10 har meldt seg ut av et sosialt nettsted av samme grunn[58]. I Teknologirådets spørreundersøkelse gjennomført i forbindelse med denne rapporten, svarer nesten 2 av 5 at de ville unngått å bruke ord og uttrykk som overvåkes av politiet.

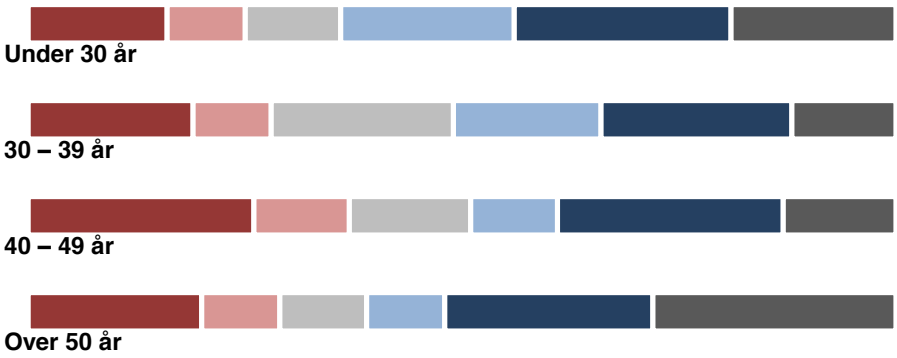
Selv om en viss grad av selvsensur er en naturlig del av den digitale hverdagen til de fleste, er det viktig at myndighetenes bruk av digital informasjon ikke bidrar til en utvikling som forringer den frie ytring i et åpent demokrati. Mange steder har sosiale medier vist seg å være en viktig arena for diskusjoner og politisk deltakelse[59]. Både under den "arabiske våren" i Midtøsten og Nord-Afrika i 2011, og under den politiske uroen i Ukraina i 2014, har sosiale medier vært viktige instrumenter i det offentlige ordskiftet.

Mangel på åpenhet og klarhet i rutiner og retningslinjer for bruk av informasjon i sosiale medier kan ha en nedkjølende effekt på ytringsfriheten. Det kan også skje hvis politiet overvåker informasjon fra sosiale medier, selv om den er åpen.

[58] Personvern 2014 – tilstand og trender, Teknologirådet og Datatilsynet, januar 2013
[59] Social Media and Human Rights, Commisioner for Human Rights, Council of Europe, februar 2012,

Hvis jeg visste at politiet fulgte med på bestemte ord og uttrykk i sosiale medier, ville jeg unngått å bruke disse ordene.





4.4.4 HVOR ”ÅPEN” ER EGENTLIG INFORMASJON I SOSIALE MEDIER?

Vår holdninger til hva som er å regne som privat og offentlig forandres kontinuerlig. Særlig kan det på sosiale medier være vanskelig å skille privat fra offentlig. Hvordan bestemmer vi hva som er ”offentlige rom”, hva som er ”private rom” og hva som muligens er en ny hybrid mellom offentlig og privat? Det finnes mange ulike sosiale medier, og de opererer på ulike måter. Noen er helt åpne, noen krever registrering og pålogging for å kunne se innhold, mens andre opererer med ulike fora hvor noen er mer åpne og andre mer lukkede. Facebook er stort nettsamfunn som krever pålogging. Deler av informasjonsutvekslingen er åpen for alle, mens andre deler skjer i mer lukkede fora.

Hvorvidt informasjon i sosiale medier deles bredt eller ikke, bestemmes dels av tjenesten, og dels gjennom bevisste valg brukeren gjør gjennom innstillinger tilbudt av tjenesten. Etter hvert som slike innstillinger blir mer komplekse og standardinnstillinger rigges mot aktiv og bred deling, er det imidlertid urimelig å anta at alle brukere til enhver tid er bevisst på hvor mye og hvor bredt informasjonen faktisk deles.

- Teknisk åpenhet er med andre ord ikke alltid ensbetydende med tiltenkt åpenhet.

Likevel bør politiet kunne bruke informasjon som også er åpent tilgjengelig for alle andre aktører i samfunnet. Twitter-meldinger kan leses av hvem som helst med internettilgang og må derfor kunne betraktes som åpen. Twitter-meldinger har i så måte klare paralleller til informasjon i massemedier. Det er imidlertid mer uklart hvorvidt informasjon som deles åpent med f.eks. alle påloggede Facebook-brukere er å betrakte som åpen eller lukket informasjon. Denne informasjonen kan være lukket for en vanlig søkemotor på Internett, men samtidig være tilgjengelig for mange tusen eller muligens millioner påloggede brukere.

- Teknisk lukket er i så måte ikke ensbetydende med at informasjonen ikke deles svært bredt og med svært mange.

Det kan være naturlig å definere informasjon som åpen hvis den er tilgjengelig gjennom en vanlig søkemotor, men selv en slik definisjon vil nødvendigvis være flyktig og noe vilkårlig (skal Googles indekserings- og søkealgoritmer bestemme hva som er åpent og lukket?) fordi slike verktøy er i stadig utvikling. En teknisk definisjon av skillet mellom privat og offentlig i sosiale medier vil derfor vanskelig fange alle nyanser av hva folk opplever som offentlig og

privat informasjonsutveksling. Likevel må en bred tilgjengelighet blant publikum og andre samfunnsaktører kunne kvalifisere informasjonen som åpen.

Informasjon som derimot deles i lukkede fora og som er tiltenkt en begrenset gruppe mennesker, vil ikke like opplagt kunne regnes som åpen informasjon. For å få tilgang til slik informasjon, kreves typisk ikke bare pålogging hos en tjeneste, men også medlemskap i en gruppe eller "vennskap" med en bestemt bruker. Selv om politiet søker slikt medlemskap med full åpenhet og transparens, vil datainnsamlingen finne sted i et lukket, "privat rom" og derfor ha paralleller til spaningsvirksomhet.

En utfordring ligger i å trekke klare skillelinjer mellom hva folk anser som offentlig og hva de anser som privat i sosiale medier. Dette er ikke skikkelig utredet i Norge, noe Nettby-saken tydelig viste.

NETTBY – ER GAMLE YTRINGER PÅ NETT OFFENTLIG INFORMASJON?

"Nettby" ble etablert i 2006, og var fra 2007-2009 Norges største nettsamfunn. Tjenesten var tilgjengelig for alle, men krevde registrering og pålogging for bruk. I likhet med Facebook, opererte Nettby med både åpne og lukkede fora. Noe informasjon ble gjort tilgjengelig for alle. Annen informasjon kunne brukeren selv begrense andres tilgang til. Tjenesten ble nedlagt i 2010.

Etter nedleggelse reiste bl.a. Datatilsynet krav om at dataene knyttet til nettsamfunnet skulle slettes. Ifølge Datatilsynet var ytringer på nettstedt å regne som private fordi tjenesten krevde pålogging. Eieren VG mente derimot at deler av ytringene var å regne som offentlig informasjon, bl.a. fordi de var tilgjengelig for indeksering i allmenne søkemotorer og dermed tilgjengelig for alle på internett. (Personvernnemda tok ikke klagen fra VG til følge og VG måtte slette alt materiale fra Nettby).[60]

Etter hvert som andre sektorer tar i bruk informasjon fra sosiale medier i større grad, vil publikum lett forvente at politiet er enda mer sofistikert i sin bruk av slike verktøy. Samtidig må politiets bruk av sosiale medier ha både bred aksept og samtykke hos publikum. Dette krever en forståelse for hva som regnes som akseptabel praksis og hva som oppleves som inngripende handlinger. Aktivitetene må forankres langs disse skillelinjene.

[60] http://www.personvernnemnda.no/vedtak/2012_03.htm

4.4.5 KRAV TIL ÅPENHET OG TRANSPARENS

Åpenhet rundt formålet med overvåkningen, hva informasjonen som kommer inn brukes til, hva slags type søkeord som blir overvåket, samt hvor lenge informasjonen vil bli lagret, vil være viktig for å få nødvendig tillit fra publikum. Politiet kan løse dette ved for eksempel å publisere:

- **Formål**
  Formålet med å overvåkingen av sosiale medier og hva informasjonen vil bli brukt til. En mulig formålsbegresning kan for eksempel være at informasjonen kun brukes til overordnet situasjonsforståelse og ikke brukes til å identifisere individer eller i en etterforskning.
- **Kilder og metode**
  Hvilke sosiale medier som overvåkes, samt når dette skjer og hvilke metoder som brukes for innsamling og analyse.
- **Søkeord**
  Åpenhet rundt hvilke generiske nøkkelord som overvåkes kontinuerlig (”skyting”, ”bombe”, osv).
  For spesifikke arrangementer (som et statsbesøk, et idrettsarrangement eller en varslet demonstrasjon); vise sammenheng mellom det aktuelle arrangement og hvilke type nøkkelord det søkes på.[61]
- **Lagringstid**
  Lagringstiden til søkeresultatene bør stå i forhold til formålet med overvåkingen. Informasjon som kommer inn i forbindelse med en redningsaksjon kan for eksempel slettes kort tid etter at redningsaksjonen er avsluttet.

Politi- og nødetater som bruker informasjon fra sosiale medier bør også være gjenstand for tilsyn som kontrollerer at de kun overvåker nøkkelord som er offentliggjort.

4.4.6 RETNINGSLINJER FOR POLITIET PÅ SOSIALE MEDIER

Kommunikasjon mellom politi og publikum er ryggraden i et moderne politi. Sosiale medier er en viktig måte å dele informasjon på i dagens samfunn. Selv om det er utfordringer knyttet til at politiet er på sosiale medier, er den poten-

[61] Når det gjelder overvåkning av nøkkelord knyttet til spesifikke hendelser, kan søkeordene variere avhengig av hva slags hendelse det er snakk om . Det kan være gode grunner for at de faktiske søkeordene man søker på ikke deles med publikum.

sielle gevinsten så stor at politiet allerede nå bør vurdere hva som skal til for å bruke informasjon fra sosiale medier i større skala.

RETNINGSLINJER FRA BRANNVESENET I LONDON

Hos London Fire Brigade finner man et eksempel på hvordan slike retningslinjer kan utformes. De har utviklet det de kaller "husregler" som beskriver hvordan de ønsker at diskusjonene skal være på deres Facebook side. De ønsker en vennlig tone, og vil ikke tolerere mobbing eller trakassering, verken av andre brukere eller ansatte i brannvesenet. De ønsker i utgangspunktet ikke å utelate noen eller å fjerne innhold, men vil gjøre dette i tilfeller de anser som grove nok.[62]

Dagens retningslinjer for hvordan politiet skal engasjere seg i sosiale medier handler stort sett om hvordan politiet skal formidle informasjon til publikum på en forsvarlig måte. Publikum kan poste en melding på sosiale medier som er ment for politiet, men politiet har ikke plikt til verken å lese eller svare på den. Politiet svarer og modererer likevel til en viss grad meldingene som kommer fra publikum til sine egne Facebook-sider eller til egne Twitter-kontoer.[63]

En av nøklene til datainnsamlingen etter bombene i Boston Marathon var at politiet allerede hadde retningslinjer på plass. Politiet visste derfor hvordan de skulle bruke sosiale medier for å håndtere situasjonen[64].

Politi- og nødetater i Norge har en god plattform å bygge videre på for å snu informasjonsstrømmen og innhente informasjon fra sosiale medier. Klare og transparente retningslinjer vil være viktig og nødvendig for å fremskaffe en god dialog med publikum. Retningslinjene vil også kunne rettferdiggjøre fjerning av informasjon og eventuell utestengelse av brukere som gjentatte ganger poster upassende meldinger. Det vil bidra til å skape tillit og legitimitet for politiets engasjement i sosiale medier. Samtidig kan politiet igangsette pilotprosjekter slik at man kan få erfaring med bruk av sosiale medier i politisammenheng. Disse to prosessene bør kjøres parallelt og gjensidig gi hverandre input og inspirasjon. Retningslinjene bør svare på følgende spørsmål og åpent deles med publikum:

---

[62] https://www.facebook.com/LondonFireBrigade/app_128953167177144
[63] http://politiforum.07.no/id/3879
[64] http://www.london.gov.uk/sites/default/files/Police%20technology%20report%20-%20Final%20version.pdf

- Hvilke sosiale medier overvåkes og til hvilket formål?

- Hvilke metoder brukes i overvåkningen, og er sammenhengen mellom formål og metode proporsjonal og nødvendig?

- Hvor lenge lagres innsamlet informasjon og hvordan kan denne informasjonen brukes og sammenstilles med annen informasjon.

- Hva er formålet med en aktiv og åpen tilstedeværelse i sosiale medier? Hvilken type kommunikasjon med publikum ønskes og hva er uakseptabel praksis?

- Hvilke mekanismer har politiet for å beskytte personvernet og når publikum aktivt engasjeres i en sak eller problemstilling gjennom sosiale medier?

Når Politiregisterloven trer i kraft 1. juli 2014, bør disse retningslinjene også tas i betraktning i praktiseringen av forskriften.

5. REFERANSELISTE

DOKUMENTER FRA NASJONALE MYNDIGHETER

Datatilsynet (2012, revidert 2013): *Kameraovervåking – hva er lov?*

Datatilsynet og Teknologirådet (2014): *Personvern 2014 – tilstand og trender*

Direktoratet for samfunnsikkerhet og beredskap (2013): *Digital kommunikasjon med nødstilte*

Innst. 425 S (2012-2013): *Innstilling fra justiskomiteen om terrorberedskap. Oppfølging av NOU 2012:14 Rapport fra 22. juli-kommisjonen. Instilling til Stortinget fra justiskomiteen, Oslo.*

Iversen, T og Dahl, I. 2010. *Politi 2.0: Kan sosiale medier bidra til økt dialog og samhandling mellom politi og publikum?*

Meld. St. 21 (2012-2013): *Terrorberedskap: oppfølging av NOU 2012: 14 Rapport fra 22. juli-kommisjonen.* Melding til Stortinget, Oslo.

NOU 2012:14 (2012): *Rapport fra 22. juli -kommisjonen.* Norsk offentlig utredning, Oslo.

NOU 2013:9 (2013): *Ett politi - rustet til å møte fremtidens utfordringer. Politianalysen.* Norsk offentlig utredning, Oslo.

PUBLIKASJONER

Omand, D., Bartlett, J., Miller, C. (2012): *#Intelligence*

Queensland Police Service (2011): *Disaster management and social media – a case study*. Queensland, Australia.

Rive, G., Hare, J., Thomas, J. & Nankivell, K. (2012): *Social Media in an Emergency: A Best Practice Guide*. Wellington Region CDEM Group, Wellington, New Zealand.

London Assembly (2013): *Smart Policing. How the Metropolitan Police Service can make better use of technology*. Budget and Performance Committee. London, Storbritannia.

Government 2.0 taskforce (2009-2010): *Social Media helping Emergency Management – Final Report*. NGIS Australia, Australia.

United Nations Global Pulse (2013): *Mobile Phone Network Data for Development*

OMTALTE NETTSIDER

Jordskjelvkart over Haiti: http://irevolution.net/2012/02/26/mobile-technologies-crisis-mapping-disaster-response/

Jordskjelvdetektor: http://recovery.doi.gov/press/us-geological-survey-twitter-earthquake-detector-ted/

Politiet og Twitter:
http://www.kampanje.com/markedsforing/article6482988.ece

Trygghetskart: http://www.aftenposten.no/nyheter/oslo/Her-foler-oslofolk-seg-utrygge-7112377.html#.UWkjYxmlgn9

Dansk trygghetsindeks:
http://subsite.kk.dk/sitecore/content/Subsites/tryghedsindeks/SubsiteFrontpage.aspx

Det engelske politiets pilotprosjekt:
http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA4-5393EEW

Personvernnemdas behandling av nettbysaken:
http://www.personvernnemnda.no/vedtak/2012_03.htm

Retningslinjer fra brannvesenet i London:
https://www.facebook.com/LondonFireBrigade/app_128953167177144

Oslopolitiets Twitter-konto: https://twitter.com/oslopolitiops, august 2014