



Justiskomiteen
Stortinget

Vår ref.: 150.13
Deres Ref.:
Dato: 22. april 2013

Høringsinnspill til Meld. St. 21 "Terrorberedskap"

Vi viser til Meld. St. 21 (2012-2013) *Terrorberedskap. Oppfølging av NOU 2012: 14*. Teknologirådet behandlet meldingen på rådsmøtet 19. april, og gir med dette brevet våre innspill til Stortinget.

Rapporten fra 22. juli-kommisjonen tegner et detaljert øyeblikksbilde av situasjonen for norsk politi og beredskapsarbeid. Kommisjonen kritiserer politiets gjennomførings- og samhandlingsevne, og legger vekt på mangelfull bruk av teknologi som en viktig forutsetning for sviktende prestasjoner: "Potensialet i moderne informasjons- og kommunikasjonsteknologi har ikke vært godt nok utnyttet" (NOU2012: 14, s16).

Teknologirådet støtter denne analysen. Den teknologiske utviklingen og digitaliseringen av samfunnet har endret premissene for beredskapsarbeidet og bør endre politiets metoder og organisering fremover. Politiet vil kunne utstyres med verktøy som kan forebygge kriminalitet, gi bred tilgang til flere informasjonskilder i sann tid, samt gjøre det enklere å dele informasjon innad i politiet, på tvers av etatene og med publikum.

I Teknologirådets pågående prosjekt "Sikkerhet og åpenhet etter 22. juli" gjør vi en analyse av det nye mulighetsrommet som digitalisering, smartmobiler og data-analyser nå gir for politiets arbeid. Vi analyserer den generelle teknologiske utviklingen, erfaringer fra andre land som Finland, Spania og USA, samt viktige trender innen politiarbeid internasjonalt. Prosjektet tar også for seg spørsmål knyttet til personvern, overvåkning og ytringsfrihet.

Stortingsmeldingen adresserer flere av anbefalingene i 22. juli kommisjonens rapport. Teknologirådet mener meldingen på flere punkter mangler ambisjoner og tydelighet om hvordan potensialet i IKT skal utnyttes for å skape et mer slagkraftig politi. Vi ønsker i denne høringen å kommentere på følgende avsnitt:

- Avsnitt 8.7 Operasjonssentralene i politidistriktene
- Avsnitt 8.6.1 Mobile løsninger
- Avsnitt 10.9.2 Særlig om IKT i justissektoren
- Avsnitt 8.9.2 Særlig om politiets helikoptertjeneste

Avsnitt 8.7 Operasjonssentralene i politidistriktene

Regjeringen diskuterer utførlig anbefalingen fra 22. juli kommisjonen om tilstrekkelig bemanning av operasjonssentralene (anbefaling 14). Regjeringen adresserer imidlertid ikke hvordan operasjonssentralene i fremtiden skal være utrustet, slik 22.juli-kommisjonen anbefaler.

Etter vår mening er det viktig at operasjonssentralene utrustes slik at operatørene og patruljene kan få tilgang til riktig og fullstendig informasjon så raskt som mulig. IKT vil spille en nøkkelrolle for å få dette til.

Enhetlig situasjonsbilde

I 2004 ble Madrid utsatt for et terrorangrep der ti bomber sprengetes med få minutters mellomrom på fire ulike forstadstog. De forskjellige nødetatene agerte hver for seg, og hver av dem hadde forskjellige systemer som ikke snakket sammen. Dette gjorde det vanskelig å få oversikt over situasjonen og å etablere et enhetlig og helhetlig situasjonsbilde.

I likhet med 22. juli, var et viktig læringsmoment i Madrid at flere store hendelser kan inntreffe samtidig. Uten et oversiktlig bilde av situasjonen er det vanskelig å få øye på viktige mønstre i utviklingsforløpet, samt å fordele ressursene riktig.

For at operasjonssentralen skal kunne håndtere slike krisesituasjoner på en effektiv måte, begrense tilgangen til de berørte områdene og sørge for en best mulig responskvalitet på hendelsesstedet, er det viktig at de er i stand til å motta og kvalitetssikre informasjon fra forskjellige kilder. Sentralen må også raskt kunne sammenstille informasjonen og lage et enhetlig situasjonsbilde som deles med alle relevante parter.

Myndighetene i Madrid har derfor samlokalisert nødetatene i en felles operasjonssentral og sydd sammen de forskjellige IKT-systemene. Slik får alle aktører i felt til enhver tid en felles situasjonsforståelse og kan kommunisere og utveksle informasjon på tvers gjennom operasjonssentralen. I følge myndighetene i Madrid har responstiden gått ned 25 prosent etter omleggingen.

Bemanning alene vil ikke gjøre operasjonssentralene tilstrekkelig rustet til å løse sine oppgaver. Operasjonssentralene må kunne fungere som et nav i informasjonsflyten mellom publikum, operative politistyrker og andre nødetater. Etterhvert som informasjonstilfanget vokser, må sentralene også utrustes med teknologi som muliggjør rask og robust inntak, kvalitetssikring og deling av informasjon.

Teknologirådet anbefaler at det legges til rette for at informasjon fra alle involverte i en nødsituasjon kan samles for å danne et mest mulig enhetlig og helhetlig situasjonsbilde. Teknologirådet anbefaler videre at samlokalisering av nødetatene vurderes.

Smart nødtelefon – et rikere situasjonsbilde

Norge og Island ligger i verdenstoppen i smart-telefonutbredelse. Dette betyr at en eller flere smart-telefoner høyst sannsynlig vil befinne seg i nærheten av enhver hendelse.

Smart-telefonene gjør det mulig å ta bilder, videoer og lydopptak av høy kvalitet med presis tids- og stedsangivelse fra en hendelse. Slik informasjon vil kunne beskrive en hendelse presist, og kan berike situasjonsbildet til politiet. Smart-telefoner er i ferd med å bli allemannseie i Norge, og deling av tekst, bilde og video er en normal del av hverdagen. Da er det også naturlig at publikum skal kunne sende inn slike multimedia-meldinger til operasjonssentralene for å gi nødetatene et mer presist situasjonsbilde.

Island har laget en smart nødtelefon-applikasjon. Med denne kan man velge å etterlate seg spor som politiet kan bruke hvis en nødsituasjon skulle oppstå. Telefonen sender da GPS-lokasjonen til islandske 112. De 5 siste posisjonene lagres. Skulle en nødsituasjon oppstå, kan man med et enkelt tastetrykk melde fra ved hjelp av applikasjonen. Da sendes GPS-lokasjonen til 112 samtidig som telefonen ringer opp nødnummeret. Koordinatene brukes som startpunkt for å kunne geleide personer som har gått seg vill, eller å sette i gang en leteaksjon dersom det skulle være nødvendig.¹

Island har tatt noen tidlige grep for å gjøre nødtelefonen smartere. I neste runde planlegges det å utvide løsningen med mulighet for å sende multimedia-meldinger.

Teknologirådet anbefaler at operasjonssentralene utvides til å kunne ta i mot og nyttiggjøre seg multimedia-meldinger fra publikum.

Sosiale medier som informasjonskilde

Nordmenn er blant de ivrigste brukerne av nett og sosiale medier i europeisk sammenheng.² Hele 80 prosent er medlem av et sosialt nettverk. Sosiale medier representerer en unik mulighet for politiet til å få informasjon fra omgivelsene.

Vi har sett at sosiale medier har vært en viktig informasjonskilde i flere store kriser i senere tid. Under orkanen Irene ble det postet mer enn 3.000 tweets 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.³

Erfaringene fra 22. juli viste at sosiale medier var en viktig kommunikasjonskanal for ungdommene og formidlet for mange den første informasjonen fra hendelsen.

Sosiale medier kan hjelpe politiet med et overordnet bilde av en situasjon. Når mange mennesker snakker om den samme hendelsen på samme sted og på samme tid på sosiale medier, kan dette være et sterkt signal om at noe vesentlig er i ferd med å skje eller allerede skjer. Dette kan gi politiet viktig tilleggsinformasjon både i forkant og under en kritisk hendelse. Det finnes verktøy for å automatisk aggregere meldinger og visualisere informasjonen slik at man enkelt kan danne seg et slikt overblikk. NRK lagde en Twitter-visualisering som viser Twitter-meldingene i døgnene etter terrorangrepene 22. Juli.⁴ Tilsvarende "Twitter-signal" ligger til grunn for "Twitter-alarmer" som nå utvikles i bl.a. USA og Japan for å varsle jordskjelv.

Enkeltmeldingene i sosiale medier kan på samme måte som meldinger fra en smartnødtelefon også være med å berike situasjonsbildet. Politiet kan fange opp – eller anmode publikum direkte om å bidra med manglende informasjon for å supplere et situasjonsbilde.

Informasjonsmengden i sosiale medier kan være stor, og det kan være tidkrevende å identifisere og verifisere kritisk informasjon. Verktøy som automatisk identifiserer, filtrerer og sorterer relevant informasjon brer om seg og kan avhjelpe dette.

Teknologirådet anbefaler at operasjonssentralene utstyres med automatiserte verktøy som gjør at operatørene på operasjonssentralen kan følge med på sosiale medier. Dette

¹ European Directory of Health Apps 2012-2013. A review by patient groups and empowered consumers. European Commission Director General for Communications Networks, Content and Technology. 2012.

² http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics

³ <http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html>

⁴ <http://nrk.no/terrotwitter/>

kan gi bedre oversikt og samtidig effektivt identifisere og plukke ut relevant informasjon som kan berike situasjonsbildet.

Offentlige kilder

Regjeringen har et uttalt mål om gjenbruk av offentlige data. Flere slike registre vil kunne berike situasjonsbildet til politiet og gjøre arbeidet på operasjonssentralen mer effektivt.

Noen av videostrømmene fra Vegtrafikksentralen overføres i dag til Operasjonssentralen i Oslo. Videostrømmene vises på egne TV-skjermer men har ingen integrasjon til politiets egne datasystemer. Politiet har dermed ikke anledning til å sammenstille videoene med egne data og nyttiggjøre seg informasjonen i eget arbeid.

Ved å bruke sanntidsdata fra Vegtrafikksentralen og Statens vegvesen vil politiet til enhver tid ha oppdatert trafikkinformasjon som de kan bruke for å beregne raskeste vei til et hendelsessted, eller hvor langt en gjerningsperson kan ha rukket å rømme en gitt tid etter hendelsen. Dette kan redusere responstiden og styre ressursene riktig.

Beregninger som bruker eksterne data krever at dataene kan leses på maskinlesbar form og integreres inn i systemene på operasjonssentralen.

Teknologirådet anbefaler at det legges til rette for at operasjonssentralene kan innhente datastrømmer fra ulike offentlige etater – på maskinlesbar form og i sann tid.

Sømløs tilgang til data

I kjølvannet av 11. september, tok også politiet i New York grep for å styrke operasjonssentralen og dermed også politiets slagkraft. New York Real Time Crime Center (RTCC) er bygget for å kunne motta, behandle og videreformidle informasjon i sann tid til politi i felt.

Mens politiet i gatene er utstyrt med mobile enheter som gjør det mulig å hente informasjon fra politiets systemer og registre, vil operative hensyn ofte gjøre det vanskelig for dem å gjøre mer avanserte sammenstillinger av informasjon fra forskjellige kilder og registre som kan understøtte arbeidet på hendelsesstedet. Informasjon om f.eks. en mistenkt, en bil eller et våpen blir da i stedet sendt til RTCC for videre bearbeiding.

RTCC kan i sin tur gjøre en maskinell analyse for å koble sammen den innsendte informasjonen med andre politiinterne data og kan straks sende nye ledetråder tilbake til politiet på hendelsesstedet. På denne måten kan operasjonssentralen bistå det operative politiet med analytisk brukerstøtte ute i felt, og politiet kan til enhver tid være sikre på at de har den mest fullstendige informasjonen og det best mulige beslutningsgrunnlaget så nært opp til hendelsen som mulig.

For å kunne levere slike tjenester, må analytikerne ved RTCC få sømløs tilgang til data fra forskjellige systemer og registre.

Data som kan understøtte politiarbeidet befinner seg i dag ofte i databaser av ulike slag som ikke nødvendigvis kommuniserer. For å sikre flyt av data mellom ulike datasystemer må man bryte ned kunstige murer mellom slike datasamlinger. Dette gjøres ofte ved å legge et harmoniseringslag "på toppen" av de eksisterende registrene

og systemene. Harmoniseringslaget gjør nødvendig tilpasning slik at dataene kan gjenbrukes i andre systemer og at man kan gjøre operasjoner så som søk og dataanalyser på tvers av systemer.

Kriminalitet respekterer ikke nødvendigvis distriktsgrenser eller organisatoriske grenser, så informasjon må kunne deles på tvers av etater og distrikter. En slik flyt er nødvendig for at politiet skal kunne være sikre på at de har den informasjonen de trenger og at de "vet hva de vet". Dette behovet vil forsterkes ettersom informasjonstilfanget øker.

En slik informasjonsflyt fordrer imidlertid klare og detaljerte bruksregler for hvordan og når informasjon skal kunne deles. Denne tematikken er omtalt i kommentarer til avsnitt 10.9.2.

Teknologirådet anbefaler at operasjonssentralene får sømløs, men bruksregulert tilgang til alle relevante politiinterne data.

Avsnitt 8.6.1 Mobile løsninger

Regjeringen sier at "nye mobile løsninger vil gi politiets førstelinje bedre forutsetninger for krisehåndtering". Videre påpeker den at mobile løsninger flytter kunnskap og politiarbeid vekk fra kontorene og ut i operativ virksomhet.

Politiet skal utstyres med nye nettbrett. Dette betyr at politiet gjennom Mobiliti på bærbare enheter vil kunne få tilgang til all informasjon de til vanlig har tilgang til på kontoret. For eksempel kan man sjekke bilregistreringsnummeret i systemet, slik at man vet hvem man har å gjøre med før man stopper bilen. Dette vil kunne avlaste operasjonssentralen, lette arbeidet for patruljen og spare tid.

Regjeringen sier videre «at politiet på sikt vil kunne få tilgang til skreddersydde tjenester for utførelse av politioppgaver med smarttelefon, nettbrett og pc i utrykningskjøretøyene». Det er imidlertid ikke konkretisert hvordan slike tjenester vil understøtte det operative politiet. Det fremgår heller ikke tydelig hvordan Mobiliti på bærbare enheter kan bidra til at politiets førstelinje får bedre forutsetninger for å håndtere og opptre koordinert i krisesituasjoner.

Politiet trenger som de fleste andre kunnskapsarbeidere tilgang til informasjon som er tilpasset den oppgaven de skal løse, der hvor de befinner seg. Neste skritt vil være applikasjoner som leverer informasjon som er mer skreddersydd til oppgaven som faktisk skal løses.

En politibetjent som er kalt ut til en hendelse vil kunne få tilsendt all relevant informasjon om hendelsen som operasjonssentralen sitter på. Det kan være informasjon om involverte personer (lovbryter og vitner), involverte objekter (biler, bygninger, veier etc.) og omgivelsene på hendelsesstedet (farlig gassutslipp, trafikkbildet, værforhold etc.). For å sikre at patruljene skal kunne håndtere en hendelse på en trygg måte både for de involverte og seg selv trenger de oppdatert informasjon knyttet til situasjonen; eksempelvis om noen av de involverte kjent for å være voldelige, om noen av bilene ettersøkte eller om det er eksplosjonsfare i omgivelsene.

Informasjonen vil typisk være en sammenstilling av informasjon fra ulike registre og systemer som vises frem på et kart. Denne samlingen av informasjon danner situasjonsbildet. I tillegg må politibetjenten enkelt kunne lage meldinger med lokasjon, lyd og (levende) bilder fra hendelsen og sende disse direkte til operasjonssentralen.

Krisesituasjoner, som 22. juli, skjer heldigvis veldig sjelden. Daglige operasjoner krever en annen type informasjon. En politibetjent som er ute på patrulje trenger derfor annen type applikasjon på nettbrettet. Dersom politidistriktet har identifisert innsatsområder og knyttet mål og tiltak til disse vil informasjon på nettbrettet signalisere hvor og hva betjenten bør gjøre den neste tiden. Dette kan for eksempel være kart med markeringer av små og presise geografiske områder som utviser høyere kriminalitet eller som av andre årsaker krever større eller mer tilpassede politiresurser enn de øvrige omgivelsene. Denne betjenten må også selv kunne sende multimedia meldinger rett inn i systemet.

Kommunikasjonen som foregår på nettbrettet vil være et supplement til politiradioen. Dagens nødnett kan ikke overføre denne type informasjon. Politibetjenten må være sikret dekning, prioritet og tilstrekkelig båndbredde til å kunne kommunisere lyd, tekst, bilder og video uansett hvor i landet han befinner seg. I tillegg må informasjonen som utveksles være sikret.

Teknologirådet anbefaler at operasjonssentralene må tilrettelegge informasjon for nettbrett slik at politibetjenten enkelt kan forstå situasjonen, ta informerte beslutninger og kontinuerlig kommunisere med alle involverte.

Teknologirådet anbefaler at politistasjoner som bruker data-analyser må tilrettelegge informasjon for nettbrett slik at politibetjenten enkelt kan forstå målene, hvilke tiltak som kreves, ta informerte beslutninger og kontinuerlig kommunisere med alle involverte.

Avsnitt 10.9.2 Særlig om IKT i justissektoren

Regjeringen har et uttalt mål om at "IKT i årene framover skal bidra til effektiv samhandling, god informasjonssikkerhet og god styrings- og beslutningsinformasjon i justissektoren, også på beredskaps- og sikkerhetsområdet". De nevner imidlertid ikke hvordan hensyn til åpenhet, transparens og personvern bør adresseres i en ny IKT-strategi for justissektoren.

Deling og gjenbruk av data

Effektiv samhandling vil kreve at data deles og gjenbrukes i større grad, både internt i politiet og mellom politiet og andre enheter. Både operasjonssentralene i Madrid og New York trekker på informasjon fra et bredt antall kilder som brukes til ulike formål og deles med involverte i en hendelse.

Denne tendensen kan man også spore i Norge. Regjeringens foreslår i meldingens kapittel 6.5.5 (side 53) at politiet skal kunne benytte passregisteret til flere formål enn det som foreligger i dagens. Dersom IKT-potensialet skal utnyttes av politiet, vil gjenbruk av informasjon være et sentral spørsmål.

Slik deling og gjenbruk er viktig for å sikre en effektiv samhandling. Da må politiet også få adgang til å bruke disse dataene. Det er samtidig viktig å sørge for at dette skjer på en trygg måte, innenfor rammen av hva loven tillater, og med hensyn til personvernet.

I dag er tilgangskontrollen og lovverk for når informasjon kan deles og hvordan det kan brukes knyttet til bestemte formål og registre. Personvernmeldingen definerer gjenbruk som " bruk ut over det som opphavleg var tanken bak innsamlinga, eller bruk hos andre enn den som først samla inn opplysningane " (Meld. St 11 2012-2013, s38).

Deling er åpenbart et nøkkelpunkt i fremtidens politi. Her er det en potensiell målkonflikt mellom mulighetsrommet for politiets arbeid og personvernet. Dersom data deles og gjenbrukes i sann tid, bør bruksreglene for dataene følge med.

Obama-administrasjonen har nylig utarbeidet en nasjonal strategi for sikker og forsvarlig informasjonsdeling⁵. Denne strategien forsøker å forenkle tilgang til informasjon fra et bredt antall kilder for godkjente personer, samtidig som man handler innenfor lovverket og ivaretar personvernet på en god måte. For å få til dette anbefaler strategien bl.a. en mekanisme de kaller data-merking (engelsk "data tagging").

Data-merking⁶ betyr at dataene merkes med bruksregler som følger dataene slik at systemene som avleverer og mottar dataene vet

1. om en gitt person/avdeling/system
2. kan bruke et bestemt stykke data
3. på en bestemt måte (samle, dele, sammenstille, slette)
4. under gitte omstendigheter

Teknologirådet anbefaler at det settes i gang et arbeid med å utvikle prinsipper og metoder slik at politiet kan dele og gjenbruke data på en måte som ivaretar personvernet. Prinsippene rundt data-merking bør ligge til grunn for dette arbeidet.

Avsnitt 8.9.2 Særlig om politiets helikoptertjeneste

Regjeringen presiserer i meldingen at politihelikopteret brukes som en plattform for observasjon og dokumentasjon i den daglige polititjenesten. Væpnede oppgaver må løses med forsvarrets helikoptre.

Det siste tiåret har utviklingen av ubemannede luftfartøy (UAV) vært omfattende. UAV-teknologi er i dag det raskest voksende feltet innen luftfart. UAV er fleksible flyvende plattformer som kan bære en rekke type sensorer, og teknologien er derfor i ferd med å revolusjonere tilgangen til luftrekognosering og datainnhenting. Ubemannede systemer representerer en betydelig reduksjon av kostnad, responstid og behov for personellressurser sammenliknet med konvensjonelle helikoptre. Samtidig gjør en størrelse ned i noen få gram at slike systemer kan operere på steder som er utilgjengelige for helikoptre.

At plattformene er ubemannende gjør at de kan operere i områder som ellers er begrenset av sikkerhetshensyn. Politihelikopteret er ikke armert for å kunne fly inn i et område hvor det skytes med skarpt. En ubemannet plattform kan derimot operere som observasjonsplattform ved slike hendelser uten personellrisiko.

Det foregår nå et omfattende utredningsarbeid knyttet til UAV-teknologi i beredskap i mange europeiske land. Samtidig utgjør teknologiens potensial for observasjon og overvåkningsformål et felt med behov for nøye vurdering av bredere samfunnsmessige konsekvenser.

Teknologirådet anbefaler at ubemannede plattformer vurderes som et potensielt supplement til politiets nåværende luftkapasitet. I denne forbindelse vil vi understreke viktigheten av en grundig vurdering av konsekvensene for personvernet.

⁵ National strategy for Information Sharing and Safeguarding, December 2012.

⁶ Bruening, Paula J., and K. Krasnow Waterman. "Data Tagging for New Information Governance Models." IEEE Security & Privacy Magazine 8.5 (2010) : 64-68. Copyright © 2010, IEEE.