Sitering av artikkelen i APA (6th):

Sunde, I. M. (2019). Patruljering på internett. I K. E. Sæther, K. Kvande, R. Torgersen & U. Stridbeck (Red.). *Straff & frihet: Til vern om den liberale rettsstat. Festskrift til Tor-Aksel Busch* (s. 597-608). Oslo: Gyldendal Juridisk.

Patruljering på internett

Inger Marie Sunde[1]

1. TO DOMENER – ETT REGELSETT

Cyberspace ble i sin tid påstått å være et separat domene som lå utenfor lovgivers jurisdiksjon.[2] Dette synet, som riktignok aldri fikk stor gjennomslagskraft, ble etter hvert så ettertrykkelig avskrevet at det uten videre tas for gitt at loven gjelder likt i det fysiske og det virtuelle domenet. I en kriminalitetsbekjempende kontekst betyr det at handlinger som er straffbare i det fysiske domenet, også er straffbare når de begås på internett. Videre betyr det at handlinger som politiet har adgang til å utføre i det fysiske domenet, også kan foretas på internett. Dette kan virke opplagt, ikke minst i lys av prinsippet om at like tilfeller skal behandles likt. Likevel fremheves det for eksempel at utkastet til ny straffeprosesslov «innenfor forsvarlige rammer» er utformet teknologinøytralt.[3] Det samme gjelder retningslinjene for infiltrasjon og provokasjon som etterforskingsmetode, som påpeker at den rettslige reguleringen bør være «*mest mulig* ensartet og teknologinøytral» (min utheving).[4] Forbeholdene tyder på at fysiske og virtuelle forhold ikke nødvendigvis er like, og at det kan ha rettslig betydning.

De strafferettslige, straffeprosessuelle og politirettslige bestemmelsene er historisk sett utformet med det fysiske domenet for øye. Gjennom langvarig praktisering har en omforent forståelse av hva reglene konkret innebærer, blitt etablert. Når det derimot gjelder internett – det virtuelle domenet –, er lovens operasjonalisering neppe like velutviklet. Loven gjelder, ja vel, men nøyaktig hva går den ut på i praksis? Og hvis forholdene virkelig *er* annerledes enn i det fysiske domenet, hva går rettsreglene i så fall ut på?

Jeg skal i det følgende belyse *politiets patruljering på internett* med utgangspunkt i konseptet patruljering slik vi kjenner det fra det fysiske rom. Spørsmålet er om dette konseptet er egnet for overføring til internett. Mot denne øvelsen kunne man kanskje innvende at siden patruljering utføres i medhold av den alminnelige handlefrihet, er det ikke nødvendig å forholde seg til patruljering *som konsept*, men heller gå rett på sak og finne ut hvilke handlinger politiet kan utføre på internett uten særlig hjemmel (med tilsvarende formål

1 Inger Marie Sunde er professor (ph.d.) ved Politihøgskolen og har arbeidet med datakriminalitet siden slutten av 1990-tallet. Hun leder den flerfaglige forskergruppen *Politiet i et digitalisert samfunn* og var medlem av Stortingets kontrollutvalg for de hemmelige tjenestene (EOS-utvalget) i perioden 2014–2019.

2 «A Declaration of the Independence of Cyberspace», J.P. Barlow, 8.2.1996, hvor det blant annet erklæres: «Governments of the Industrialized World … You have no sovereignty where we gather.» (Tilgjengelig bl.a. på www.eff.org/cyberspace-independence, besøkt 14.12.2018).

3 NOU 2016: 24 *Ny straffeprosesslov* (Straffeprosessutvalget), s. 153.

4 Infiltrasjon og provokasjon som etterforskingsmetode – vederlag til politiets kilder. Riksadvokaten, rundskriv 2/2018, punkt I.

som for fysisk patruljering). På den annen side sies det ofte at politiet *kan* patruljere på internett, eventuelt at det *bør* gjøre det, og da er nettopp det fysiske konseptet referansepunktet. Metodekontrollutvalget (2009) sier for eksempel at endringer i personellbehovet «illustreres godt av behovet for 'patruljering' på Internettet som følge av dets økte betydning som operasjonssted også for kriminelle»,[5] mens Politidirektoratet (2015) taler om «politiets aktiv[e] deltakelse – 'patruljering på nett'»,[6] og Lystad-utvalget (2017) forutser en samfunnsutvikling som leder til at politiet «må bruke store ressurser på nettpatruljering».[7]

Det kan være at fysiske og virtuelle handlinger ytre sett fremstår som like, uten at de nødvendigvis er *likeverdige* etter en kvalitativ vurdering. Internetteknologien har et stort overvåkingspotensial som setter menneskerettighetene på spill, særlig personvernet og ytringsfriheten. Videre går det antakelig en grense for hvor stor «politistyrke» som kan være på internett uten at de samme rettighetene kommer under press. Dette utløser spørsmål om hvorvidt patruljering på internett har sider i form av overvåking og maktuttrykk som *ikke* har sitt motstykke i det fysiske domenet. Endelig er det naturlig å spørre om patruljering slik vi kjenner det fra det fysiske domenet, er hensiktsmessig å overføre til internett.

I det følgende redegjør jeg først for fysisk patruljering som konsept (punkt 2). Deretter drøfter jeg hvordan patruljering på internett kan utføres, og om det tilsvarer fysisk patruljering (punkt 3). Herunder tar jeg opp den rettslige betydningen av automatisering og kunstig intelligens i patruljering. Videre behandler jeg «tilstedeværelse», noe som inngår i fysisk patruljering. Tilstedeværelse er imidlertid er en så komplisert størrelse på internett at det er skilt ut til egen behandling (punkt 4). Avslutningsvis følger en oppsummering (punkt 5).

2. FYSISK PATRULJERING SOM KONSEPT

Jeg vil tro at uttrykket «politiets patruljering» utløser en mer eller mindre bestemt forståelse av hva det er tale om. Dette tankebildet omtaler jeg som *patruljeringskonseptet*. Jeg skal konkretisere hva konseptet rimeligvis innebærer, gjennom å klargjøre patruljeringens formål og oppgaver, hvor patruljering kan foregå, og karakteren av politiets tilstedeværelse. Videre ser jeg på avgrensningen av patruljering mot andre oppgaver utført av politiet.

Politidirektoratet har beskrevet *patruljetjenestens* formål og oppgaver slik:

Formål:

> «Politipatruljene skal være til stede for befolkningen der befolkningen er, og utgjør politidistriktets døgnkontinuerlige grunnberedskap. Patruljene skal yte rask respons med god service og kvalitet i nært samspill med befolkningen og samfunnets aktører. Patruljetjenesten skal

5 NOU 2009: 15 *Skjult informasjon – åpen kontroll* (Metodekontrollutvalget), s. 74.

6 *Datakrimstrategien*, Politidirektoratet, 2015, s. 77.

7 *Politi- og lensmannsetatens kapasitets- og kompetansebehov de kommende tiårene* (Lystad-utvalget), Politidirektoratet, 2017, s. 33.

> arbeide kriminalitetsforebyggende, med særlig vekt på straksforebyggende tiltak, og utføre oppdrag innen hele politiets oppgavespenn, med politiarbeid på stedet som hovedmetode. Politipatruljen skal registrere aktuell informasjon i relevante databaser som grunnlag for etterretning.»[8]

Oppgaver:

> «[Politipatruljen skal] utføre oppdrag prioritert og tildelt av operasjonssentralen; utføre hendelsesstyrte oppgaver patruljen selv avdekker; utføre straksetterforsking med politiarbeid på stedet som metode; utføre målrettede og planlagte oppgaver i tråd med politidistriktets virksomhetsplaner og innhentingsplaner for informasjon.»[9]

Det fremgår at *patruljetjenesten* har omfattende oppgaver, utløst enten av oppdrag fra operasjonssentralen eller av det patruljen selv avdekker gjennom sin tilstedeværelse og observasjon. Patruljering kan således gå over i håndtering av oppgaver som styres av egne regler, for eksempel (straks)etterforsking, som er undergitt straffeprosessuelle bestemmelser, jf. straffeprosessloven § 224 flg., eller inngripen for å håndheve ro og orden, jf. politiloven § 7 nr. 1–3. Som sitatene viser, kan patruljering også innebære informasjonsinnhenting. Behandlingen av informasjonen må følge politiregisterlovens regler for dette, samt straffeprosesslovens regler i tillegg dersom det skjer som ledd i etterforsking. Men siden politiet generelt har stor frihet til å velge hvordan den konkrete oppgaveløsningen skal skje, uansett om det er tale om etterforsking, forebygging eller operativ tjeneste, kan patruljering inngå som aktivitet i disse, inkludert i etterforsking. Det er ikke noen motsetning her, såfremt reglene for fremgangsmåtene overholdes når de slår inn, som for eksempel ved pågripelse og ransaking. Også generell informasjonsinnhenting foregår som en integrert del av patruljeringen på grunn av den nære sammenhengen med observeringen.

Som nevnt skjer patruljering i kraft av den alminnelige handlefrihet, noe som for så vidt også følger av det første sitatet, som sier at politipatruljen «skal være til stede for befolkningen der befolkningen er». Politiet trenger ikke en egen hjemmel for å være til stede der befolkningen er, typisk i byrommet, og tilstedeværelsen kan være uniformert eller i sivil. Patruljeringen må imidlertid ha et formål som angitt i det første sitatet. Hvis ikke gjelder aktiviteten noe annet.

Med utgangspunkt i at rettsgrunnlaget er den alminnelige handlefrihet, kan man slutte seg til *hvor* patruljering kan foregå. Det må være der allmennheten kan oppholde seg, det vil si i det offentlige rom og på private steder hvor allmennheten har tilgang. Motstykket er steder hvor politiets tilgang krever lovhjemmel, f.eks. ransakingsbestemmelsene under etterforsking. Slike steder kan ikke patruljeres, fordi det ville innebære en krenkelse av privatlivets fred, jf. Grunnloven § 102, og man har ikke lovbestemmelser, jf. Grunnloven § 113,

8 Rammer og retningslinjer for etablering av nye politidistrikter. Versjon 1.2. Politidirektoratet, 16. juni 2017, s. 114.
9 Ibid.

som hjemler patruljering av det private rom. En lovmessig adgang som nevnt ville anses som uforholdsmessig og i seg selv krenke menneskerettighetene om den ble innført.[10] Patruljering kan således foregå for eksempel i byens gater og parker, på torg, jernbanestasjonen og idrettsplassen. Videre kan det patruljeres på privateid grunn som er allment tilgjengelig, for eksempel et kjøpesenter, en restaurant eller et konsertlokale.

Implisitt følger det at patruljering innebærer en *tilstedeværelse* på de angitte stedene, noe som for så vidt står i den nevnte passusen om at politipatruljen «skal være til stede for befolkningen der befolkningen er». Forutsetningen om tilstedeværelse er i tråd med patruljeringens formål: Beredskapsformålet innebærer at patruljen skal ha evne til å gi «rask respons» dersom noe skjer. Da må den også være til stede, i det minste i nærheten av hendelsen. De disiplinerende, trygghets- og tillitsskapende formål som kan utledes av forebyggingsoppgavene og samspillet med publikum, forutsetter også tilstedeværelse. Tilstedeværelse synes derfor å være et klart kjennetegn på patruljering.

Oppsummert kjennetegnes patruljering i det fysiske rom som konsept av å gå ut på observasjon og informasjonsinnhenting gjennom tilstedeværelse på et allment tilgjengelig sted. Patruljering kan gå over i konkret oppgavehåndtering undergitt egne regler. Patruljering er en del av grunnberedskapen og utføres i medhold av den alminnelige handlefrihet.

3. PATRULJERING PÅ INTERNETT

I det følgende drøfter jeg patruljering på internett i lys av kjennetegnene for patruljering i det fysiske rom. Formålet er som nevnt å undersøke hvorvidt patruljering slik vi kjenner det i det fysiske rom, er overførbart til internett. Formålet er videre å fastlegge de rettslige grensene for patruljering på internett, det vil si hva politiet kan gjøre i kraft av den alminnelige handlefrihet kontra handlinger som må ha hjemmel i lov. Med «den alminnelige handlefrihet» forstår jeg det politiet kan gjøre overfor og i samspill med borgerne uten hjemmel i lov. Adgangen til å registrere falsk profil på sosiale medier – og problemene politiet har med dette – holder jeg utenfor, selv om det inneholder visse avtalerettslige spørsmål overfor tjenestetilbyderne, noe som kan sies å ha betydning for handlefriheten. Teknologiens store kapasitet og overvåkingspotensial aktualiserer spørsmålet om hvorvidt patruljeringen kan ta en form som representerer inngrep i grunnleggende rettigheter som personvern og ytringsfrihet. Spørsmålet bør stilles selv om handlingene *fremstår* som like med dem som utføres i fysisk patruljering.

3.1 Formålet

Et grunnleggende spørsmål er hva som ønskes oppnådd med patruljering på internett. Formålsavklaring er for det første nødvendig for å fastslå hvilke regelsett som gjelder. Dersom man er i det forebyggende sporet, eventuelt er ute etter å håndheve «ro og orden» på

10 Proporsjonalitetsvilkåret følger eksplisitt av EMK artikkel 8.2 (personvern) og 10.2 (ytringsfrihet). Det er ikke inntatt i Grunnloven, men gjelder like fullt, fordi de nevnte bestemmelsene gjelder som del av norsk rett, jf. menneskerettsloven § 2 (lov 21. mai 1999 nr. 30).

internett, må den alminnelige handlefrihet kombineres med rammene satt av politilovens bestemmelser. Hvis man er ute på etterforsking, må den alminnelige handlefriheten utøves innen de straffeprosessuelle rammene for dette.

Videre er formålet viktig for å gjøre seg opp en mening om betydningen av *tilstedeværelse*. For eksempel går etterforsking ut på informasjonsinnhenting, noe som på internett *ikke* nødvendigvis forutsetter tilstedeværelse. Informasjonsinnhenting på nettet som ledd i etterforsking er derfor ikke nødvendigvis å regne som patruljering. Forebygging og operativt arbeid krever mer av *en reaksjon på stedet*, for eksempel en advarsel eller inngripen, som nevnt i politiloven §§ 6 og 7. For disse formål synes tilstedeværelse å ha større betydning.

3.2 Tilstedeværelse og betydningen av automatisering

Det er således nødvendig å belyse hva tilstedeværelse betyr på internett. Utgangspunktet er at politibetjenten sitter i det fysiske rom, logger seg på og foretar seg noe på internett. Hva kreves av handlingen for å utgjøre tilstedeværelse på internett, og kan politiet gjøre det i medhold av handlefriheten?

Til denne diskusjonen hører også spørsmålet om betydningen av automatisering. Det gir ikke god mening om alt politiarbeid på internett skulle utføres manuelt fordi det er slik det gjøres i det fysiske rom. I det fysiske rom må politiet forflytte seg til fots eller med bil, og patruljen kan bare være på ett sted av gangen. På internett kan politiet derimot sette opp automatiske innsamlingsfunksjoner på mange forskjellige steder (tjenester) og slik skaffe seg informasjon som kan analyseres i ettertid. Den virtuelle fremgangsmåten bryter med den fysiske både i tid og rom, fordi politiet kan «være» mange steder samtidig (rom), samtidig som det ikke behøver å være til stede mens informasjonsinnhentingen foregår (tid). Som nevnt reiser tilstedeværelse på internett så mange spørsmål at temaet behandles separat (punkt 4).

3.3 Kan politiet la seg representere av kunstig intelligens?

Videre bør man ta opp spørsmålet om hvorvidt politiet kan la seg representere på nettet ved hjelp av kunstig intelligens, og i tilfelle på hvilke vilkår det kan skje. I det nederlandske «Sweetie»-prosjektet har man for eksempel sett for seg å bruke kunstig intelligens til å skape politiroboter som kan operere selvstendig på sosiale medier og pratekanaler under fiktiv profil som en 10 årig pike («Sweetie»).[11] Politiroboten, rettere sagt *dataprogrammet*, produserer Sweetie-profilens innlegg på pratekanaler, hvor hun bruker et naturlig språk. Med avansert 3D-teknologi kan hun også utgi seg for å være et naturlig barn i en weboverføring.[12] Formålet er å forebygge og etterforske seksuelle overgrep mot barn på internett

11 www.tdh.ch/en/projects/sweetie-how-stop-webcam-child-sex-tourism (besøkt 3. oktober 2018).

12 De tekniske egenskapene er beskrevet i punkt 2 i rapporten *Legal aspects of Sweetie 2.0.* av Schermer, B.W., Georgieva, I., van der Hof, s. & Koops, B.-J., Leiden University, Tilburg University, Leiden, 2016. Rapporten beskriver prosjektets tekniske visjon, som nok foreløpig ikke er fullt realisert.

(nettovergrep). I en annen artikkel har jeg behandlet strafferettslige og straffeprosessuelle spørsmål knyttet til «Sweetie» etter norsk rett og viser til denne artikkelen for nærmere opplysninger om teknologien.[13] I skrivende stund (mars 2019) er det et åpent spørsmål om den tekniske visjonen i «Sweetie»-prosjektet fullt ut vil bli gjennomført, men den gir uansett en pekepinn om teknologianvendelser som kan være aktuelle for norsk politi, og tas derfor som utgangspunkt for drøftelsen her.

Tanken bak «Sweetie» er at hun kommer til å bli oppsøkt av overgripere så snart hun settes ut på nettet. Når de fremsetter uanstendige eller krenkende forslag mv., logger hun kommunikasjonen automatisk sammen med de elektroniske sporene, før hun trekker seg fra kontakten. Når hun registrerer kontakt med en potensiell overgriper, kan hun reagere med en advarsel om at handlingen er straffbar og innebærer en risiko for straffeforfølgning, samt gi en oppfordring om å søke profesjonell hjelp for problemet. Den lagrede informasjonen kan brukes som grunnlag for å iverksette etterforsking og oppspore overgriperen.

Bruk av fiktiv profil har vist seg å være en effektiv fremgangsmåte for å spore opp overgripere. I «Sweetie»-prosjektets innledende fase (2013) gjorde man dette manuelt over ti uker og lyktes med å identifisere 1000 nettovergripere.[14] Dette skjedde på et tidspunkt da det ennå bare fantes 6 – seks – domfellelser for nettovergrep på verdensbasis.[15] Tilnærmingen er hensiktsmessig også fordi nettovergripere gjerne har svært mange ofre. «Sweetie» gir nemlig politiet god mulighet til å komme i inngrep med hele omfanget av overgriperens forbrytelser og redde ofrene.

En «Sweetie» som er basert på kunstig intelligens, opptrer selvstendig. Politiet kan nøye seg med å bestemme i hvilke fora hun skal settes ut, og når hun skal trekkes tilbake. Teknologien er skalerbar, noe som innebærer at flere politiroboter kan være til stede flere steder samtidig uavhengig av hverandre. Det innebærer at det bare er *tekniske kapasitetshensyn* som eventuelt begrenser bruken. Det gjelder både for «Sweetie» og for andre vektøy av tilsvarende karakter.

Effektiviseringen som følger med «Sweetie», ligger derfor på flere plan: Metoden som sådan er effektiviserende *for den generelle måloppnåelsen*, som gjelder kriminalitetsbekjempelse gjennom forebyggende tiltak og etterforsking. Det er for eksempel i denne betydningen Metodekontrollutvalget bruker ordet «effektivisering» i kapittel 8 *Behovet for effektiv kriminalitetsbekjempelse*, hvor politiets samlede virkemidler i kriminalitetsbekjempelsen gjennomgås.[16] Ved å gå ut *proaktivt* med profilen til en mindreårig pike tiltrekker politiet seg nettovergripere, noe som er mye mer effektivt enn å arbeide reaktivt i påvente av politianmeldelse (nettovergrep har som kjent i liten grad vært anmeldt). Det er imidlertid ikke *nødvendig* å bruke kunstig intelligens for å oppnå dette, fordi det også kan gjøres manuelt

13 I.M. Sunde, «Sweetie, et politibarn eller en politistyrke på internett?». I Sunde, I.M. & Sunde, N. (red.) *Det digitale er et hurtigtog – vitenskapelige perspektiver på politiarbeid, teknologi og digitalisering*, Fagbokforlaget, Bergen, 2019.

14 Terre des Hommes, *Webcam child sex tourism – becoming Sweetie: a novel approach to stopping the global rise of webcam child sex tourism*. Rapport. November 2013, s. 5.

15 Ibid.

16 NOU 2009: 15 *Skjult informasjon – åpen kontroll* (Metodekontrollutvalget), s. 68 flg.

av en politibetjent som sitter online med «Sweeties» profil, slik man gjorde i «Sweetie»-prosjektets innledende del. Etter gjeldende rett krever ikke fremgangsmåten lovhjemmel av hensyn til legalitetsprinsippet, selv om man nok kan tenke seg å innføre slike bestemmelser for å ivareta «rettsstatsidealer som har sterk forankring … i norsk rettsliv», jf. Straffeprosessutvalgets forslag om å lovfeste tidligere ulovfestede metoder.[17] Heller ikke hensynet til *lex superior*-prinsippet tilsier at metoden må lovfestes. Straffeloven § 202 om identitetskrenkelse rammer nemlig ikke bruk av fiktiv identitet, bare bruk av en identitet som er lik eller er lett å forveksle med identiteten til en reell person.[18] Fremgangsmåten kan altså benyttes i kraft av den alminnelige handlefrihet. Det gjelder både manuell og automatisert fremgangsmåte.

Med kunstig intelligens effektiviseres også *ressursforbruket i det enkelte tilfelle*, fordi man sparer personellressurser som ellers hadde medgått til å styre «Sweetie» online. En politibetjent klarer kanskje bare å delta i fire samtaler samtidig når hun arbeider online. Det tilsier at man kan erstatte betjenten med fire politiroboter, fordi resultatet blir det samme. Samtidig har man spart innsatsen til den ene politibetjenten. Dette bør kunne skje i medhold av den alminnelige handlefrihet, som nettopp beskrevet.

Det store spørsmålet gjelder adgangen til å sette ut mange flere «Sweetier» samtidig, slik at politiets kapasitet på nett øker i forhold til det som hadde vært mulig å utrette manuelt. Også dette er effektiviserende for den generelle måloppnåelsen: Kriminalitetsbekjempelsen (rettet mot nettovergrep) bedres fordi politiet identifiserer flere overgripere enn før. Samtidig brukes mindre personellinnsats enn man ellers måtte ha gjort for å oppnå det samme. Denne bruken av «Sweetie» er imidlertid kvalitativt forskjellig fra det som ble beskrevet ovenfor. Brukt på denne måten er det mer nærliggende å karakterisere teknologien som en ny kapasitet som lar politiet utføre handlinger som det tidligere ikke kunne gjøre. Det er noe annet og mer enn en effektivisering av det politiet allerede kunne gjøre på mer tungvint vis.

For å bruke et enkelt bilde: I det fysiske rom er måltallet for politistyrken 2 per 1000 innbyggere (2 : 1000).[19] På nettet, med bruk av skalerbar kunstig intelligens, kan hvilket som helst forholdstall realiseres, eksempelvis 2 «Sweetier» per innbygger (2 : 1). Dersom vi hadde hatt to politibetjenter på gaten for hver øvrige innbygger, ville samfunnet vært ganske forskjellig fra dagens. En omfattende skjult polisiær tilstedeværelse står i et tvilsomt forhold til prinsippene om at politiet skal avspeile samfunnets idealer og virke i et samspill med publikum.[20] Det bryter også med det fysiske patruljeringskonseptet som nettopp er tuftet på disse idealene, jf. sitatene i punkt 2.

Politiets bruk av skalerbar kunstig intelligens overfor befolkningen har derfor sider som trenger regulering for ikke å komme i konflikt med grunnleggende rettigheter og et demokratisk styresett. For det første er det åpenbart at politiet ikke på egen hånd kan utvide styrken

17 NOU 2016: 24 *Ny straffeprosesslov* (Straffeprosessutvalget), s. 343.

18 I.M. Sunde, *Datakriminalitet*, Fagbokforlaget, Bergen, 2016, s. 143.

19 *Politiet mot 2020. Bemannings- og kompetansebehov i politiet.* Politidirektoratet, 2008, s. 7 og 60–62.

20 R.L. Auglend & H.J. Mæland, *Politirett*, 3. utg., Gyldendal Juridisk, Oslo, 2016, s. 177 flg., med referanse til Politirolleutvalget (NOU 1981: 35).

sin. Politiet er regjeringens redskap, og dimensjoneringen er politisk bestemt. Samtidig må det erkjennes at når det gjelder *antall,* lar virtuelle og fysiske forhold seg vanskelig sammenligne. Mens 2 per 1000 er et klart parameter i det fysiske rom, er det høyst uklart hvordan et lignende forholdstall skulle kunne fastlegges for det virtuelle rom. Hver «Sweetie» kan anses som en politiprofil på internett, men slik er det også for borgerne. «Alle» er på nettet, og de fleste har flere registrerte brukere. En forholdstallsbetraktning mellom politi og befolkning på nett er derfor antakelig lite egnet som parameter for hvor grensen for politiets kapasitet bør gå. Men selv om det er uklart hvilke størrelser som bør sammenlignes, bør en vurdering foretas.

Ett er i hvert fall sikkert, og det er at politiet er et uttrykk for makt. Hvis dette uttrykket blir for massivt, kan både personvernet og ytringsfriheten settes under press. Effektiviteten i kriminalitetsbekjempelsen kommer i så fall i konflikt med de grunnleggende rettighetene som er nedfelt i Grunnloven §§ 100 og 102, sml. EMK artikkel 10 og 8, og behøver lovhjemmel, jf. Grunnloven § 113. En nærmere regulering synes imidlertid å kreve et empirisk grunnlag som sier noe om befolkningens holdninger til skjult polisiær virksomhet på nett. Videre bør sentrale reguleringspunkter gjelde muligheten for å føre kontroll med teknologien. Herunder bør det lovfestes krav om at teknologien *allerede når den innføres, er tilrettelagt for kontroll*. Behovet for at kontrollmuligheten hensyntas allerede når teknologien utvikles og informasjonssystemer etableres, synes å gjøre seg stadig sterkere gjeldende. Behovet ble blant annet fremhevet av Stortingets kontrollutvalg for de hemmelige tjenestene (EOS-utvalget) i høringsuttalelsen til forslaget om ny lov for Etterretningstjenesten.[21] Det bør også gjelde kompetansekrav til dem som skal bruke verktøyet, samt en tydelig ansvarsregulering ved feil eller misbruk. Konklusjonen på dette punktet er således at skalerbar kunstig intelligens som politiverktøy på nettet bare kan tas i begrenset bruk i medhold av den alminnelige handlefrihet.

4. TILSTEDEVÆRELSE PÅ INTERNETT

Politipatruljen skal altså «være til stede for befolkningen der befolkningen er». Befolkningen er jo på internett, så da bør politiet også være der, men hva menes med dette? Spørsmålet om hva som kan regnes som patruljeringsmessig «tilstedeværelse» på internett, synes best å kunne angripes ved å fastlegge forholdet mellom tilstedeværelse, observasjon og informasjonsinnhenting. Som det har blitt redegjort for, inngår alle aktivitetene i patruljering. Videre er det spørsmål om tilstedeværelse må skje personlig, eller kan skje automatisert.

4.1 Rapporter som behandler patruljering på internett

Politidirektoratets rapport *Politiet i det digitale samfunnet* fra 2012 trekker ikke inn betydningen av tilstedeværelse. Her brukes uttrykket «digital patruljering» generelt om *informasjonsinnhenting fra åpne kilder på internett*.[22] I *Datakrimstrategien* (2015) behandles imidlertid

21 Høringssvar fra EOS-utvalget av 12. februar 2019, punkt 3.

22 *Politiet i det digitale samfunnet*, Politidirektoratet 2012, s. 14.

politiets «tilstedeværelse» på nett og betegnes som «aktiv deltakelse – 'patruljering på nett'».[23] Også «åpen uniformert *tilstedeværelse*» nevnes (min utheving), noe som forstås som politiets aktive deltakelse «med registrerte brukere … som klart tilkjennegir seg med politiets logo og identitet».[24] *Skjult tilstedeværelse* derimot, anses som «digital spaning, infiltrasjon og provokasjon … og bør kunne brukes til informasjonsinnhenting for forebygging og etterforsking».[25] Hvorfor patruljering på nettet nødvendigvis må skje «uniformert», er ikke begrunnet. Som nevnt gjelder ikke dette vilkåret for fysisk patruljering, og det er alt konkludert med at politiet kan bruke fiktiv identitet på nettet i kraft av den alminnelige handlefrihet.

4.2 Et krav om interaktivitet

Tilstedeværelse er et vanskelig begrep på internett, men målestokken for hva som menes, bør i hvert fall være lik for politi og befolkning. Dessuten tilsier den utbredte oppfatningen om at alle *er* på nett, at begrepsbruken kan ha noe for seg.

Enkelt sagt betyr tilstedeværelse at man *er* et sted. I tillegg må oppmerksomheten være innrettet mot det som skjer på stedet, ikke nødvendigvis målrettet og intenst, men man må i hvert fall kunne oppfatte om andre er i nærheten, og kunne respondere på henvendelse. Den som sover på vakt, er ikke til stede selv om kroppen er det. Man kan for eksempel tenke seg at politiet markerer seg på internett uten å ha et opplegg for interaktivitet eller informasjonslagring. Politiet registrerer for eksempel brukeren «Politiet» på et forum uten at noen politibetjent følger med på hva som skjer, verken i sanntid eller i etterkant. Formålet kan for eksempel være å oppnå en disiplinerende effekt. Men siden brukeren reelt sett er «død», minner fremgangsmåten mer om *skilting* enn om patruljering.

Muligheten for *interaktivitet* synes dermed å være et kriterium for tilstedeværelse. Forståelsen er naturlig i lys av patruljeringens formål, som er å «yte rask respons med god service og kvalitet i nært samspill med befolkningen og samfunnets aktører». Videre støttes det av at patruljering kan gå ut på å «registrere aktuell informasjon i relevante databaser som grunnlag for etterretning» (begge sitatene er fra punkt 2 i dette kapitlet). Informasjonsinnhentingen har da forutsetningsvis skjedd under patruljering, det vil si som følge av at politiet er til stede.

Det er rimelig å tale om tilstedeværelse dersom politiet selv oppretter et nettsted som kan kontaktes av befolkningen, og som innbyr til interaktivitet. Dette må regnes som *passiv tilstedeværelse*, siden politiet bare yter en service og ikke utfører handlinger rettet mot et bestemt sted eller person. Politiets nettpatrulje er et eksempel på dette. Både web- og Facebook-siden er opprettet og styrt av politiet med klar markering av denne statusen. Politiet kan kontaktes og gi råd og veiledning. Nettpatruljen er således nærmest å anse som et virtuelt politikammer betjent på dagtid (websiden opplyser at Nettpatruljen bare er betjent på dagtid).[26]

23 *Datakrimstrategien*, Politidirektoratet, 2015, s. 77.
24 *Datakrimstrategien*, Politidirektoratet, 2015, s. 77.
25 *Datakrimstrategien*, Politidirektoratet, 2015, s. 77.
26 I hvert fall var dette tilfelle på tidspunktet for besøk av nettpatruljens nettsted: www.politiet.no/rad/trygg-nettbruk/politiets-nettpatrulje/ (besøkt 15.12.2018).

En registrert profil som «Sweetie» som nevnt i punkt 3.2 må også sies å ha en tilstedeværelse på nettstedene hun besøker. Grunnen er at hun deltar med en synlig profil, er med i chat mv., som foregår på det åpne forumet. Interaktiviteten sammenholdt med formålet om å forebygge/etterforske en bestemt kriminalitetstype innebærer at dette må anses som *aktiv tilstedeværelse*. Når «Sweetie» går over i samtale med en annen på en lukket kanal, er man over i infiltrasjon og må følge reglene for dette, jf. riksadvokatens rundskriv nr. 2/2018 punkt IV. Dersom dette skjer automatisert, oppstår visse spørsmål i tilknytning til straffeprosessloven § 216 l, som det fører for langt å gå inn på her. Leseren henvises til den tidligere nevnte artikkelen om «Sweetie».[27]

Det er derimot verken nødvendig eller naturlig å tale om tilstedeværelse når det gjelder utnyttelse av internett som *generell informasjonskilde*. En politibetjent som for eksempel «surfer» på nyhetskanaler for å holde seg oppdatert, kan vanskelig sies å patruljere på nettet. Hvis hun derimot setter visse nettsteder under systematisk observasjon, regnes aktiviteten som spaning og må følge reglene for dette.[28] Den rettslige betydningen av å klassifisere en aktivitet som spaning i stedet for patruljering synes imidlertid å være noe uklar. Det som *har* betydning, er at *formålet* er klart, nemlig hvorvidt det gjelder etterforsking som er undergitt påtalemessig styring, eller andre politioppgaver som er undergitt politimesterens styring. Den forståelsen av digital patruljering som er tilkjennegitt i Politidirektoratets rapport fra 2012 (se punkt 4.1), er uansett lite treffende fordi den bare fokuserer på informasjonsinnhentingen. Det kan politiet gjøre som enhver annen, for forskjellige formål. Adgangen er også presisert i datakrimkonvensjonen (CETS 185), som Norge har sluttet seg til, artikkel 32 bokstav a, som bestemmer at politiet kan «skaffe seg tilgang til offentlig tilgjengelige, lagrede data (åpne kilder), uansett hvor dataene befinner seg geografisk».[29] Hvorvidt informasjonsinnhentingen skjer manuelt eller automatisert, for eksempel ved bruk av automatiske varslinger om nye innlegg i debattråder på bestemte fora, kan ikke ha betydning, annet enn at man etter gjeldende rett må være oppmerksom på grensen mot spaning.

Eksemplet viser for øvrig at informasjonsinnsamling også kan foregå *uten forutgående observasjon*. Slik er det ikke når innsamlingen skjer i forbindelse med fysisk patruljering, for da går observasjon hånd i hånd med politiets sansebruk. Dermed er det også nødvendigvis en forbindelse mellom politibetjentens observasjon og den påfølgende informasjonsbehandlingen. Denne forbindelsen er ikke nødvendig på nettet. Med automatisk informasjonsinnhenting kan «observasjonen» skje i etterkant, når informasjonen gjennomgås. Man handler ikke i «sanntid» som ved fysisk patruljering, og arbeidsoperasjonene kan følgelig skje i en annen rekkefølge enn i det fysiske rom.

27 Sunde (2019).

28 Straffeprosessutvalget karakteriserer spaning som «langvarig eller systematisk observasjon av en person eller sted» (NOU 2016: 24, s. 343).

29 Den norske oversettelsen av konvensjonen er inntatt til sist i NOU 2007: 2 *Lovtiltak mot datakriminalitet* (Datakrimutvalget). Den offisielle engelske teksten lyder «access publicly available (open source) stored computer data, regardless of where the data is located geographically».

Gjennomgangen viser at begrepet «tilstedeværelse» er nyttig for å karakterisere og avgrense bestemte handlinger på internett. Det kan derfor brukes om patruljering på internett. Kravet om interaktivitet innebærer en forståelse av patruljering på internett som er snevrere enn lagt til grunn i 2012-rapporten. Videre har gjennomgangen belyst at observasjon, tilstedeværelse og informasjonsinnhenting kan utføres uavhengig av hverandre på grunn av automatisering. Den kronologiske orden som gjelder ved fysisk patruljering, oppheves. For å oppnå klarhet bør derfor uttrykket «patruljering på internett» brukes med forsiktighet. Etter mitt skjønn er det bedre å snakke konkret om hver enkelt aktivitet. Det gir også best forutsetning for å forvisse seg om at den omfattende reguleringen for informasjonsbehandling i politiet overholdes, jf. politiregisterlovgivningens regler om dette.[30]

Et siste spørsmål gjelder betydningen av om politiets tilstedeværelse er åpen eller skjult. Som nevnt opplyser Politidirektoratets rapport fra 2015 (*Datakrimstrategien*) at skjult tilstedeværelse er å anse som «digital spaning, infiltrasjon og provokasjon …», og den tar til orde for at «patruljering på nett «bare bør brukes om 'åpen uniformert tilstedeværelse', det vil si politiets aktive deltakelse «med registrerte brukere … som klart tilkjennegir seg med politiets logo og identitet».[31] Nettpatruljens passive tilstedeværelse oppfyller dette. Men grunnen til at det bør legges så streng ramme for patruljeringen, er ikke opplyst og følger neppe av gjeldende rett.

Patruljering kan som nevnt utføres i sivil når det skjer i det fysiske rom. Politiet er til stede og observerer, men ikke så intenst at det går over i spaning, og ikke så interaktivt at det er tale om infiltrasjon. Skjult patruljering på nettet må innebære at politiet skjuler sin identitet ved bruk av en profil som verken opplyser om politibetjentens identitet eller tilhørigheten til politiet. Politiet må med andre ord bruke en profil med en uriktig identitet. Det er tidligere konkludert med at politiet har adgang til dette i medhold av handlefriheten, såfremt man ikke bruker en identitet som tilhører eller er lett å forveksle med identiteten til en reell person. Spørsmålet er dermed om skjult patruljering innebærer en slik risiko for maktmisbruk og krenkelse av grunnleggende rettigheter at den *burde* være formelt regulert, selv om den rettslige adgangen allerede foreligger.

Svaret synes å være usikkert, fordi det generelt gjelder andre premisser om identitet på sosiale medier enn i den fysiske verden, et poeng som for øvrig er fremhevet i Lasse Lund Madsens analyse av de danske reglene om agentvirksomhet, anvendt på internett.[32] Grunnen til at premissene er forskjellige, er at man ikke har tilgang på umiddelbar observasjon av den andre, noe som illustreres av ordtaket «on the Internet, nobody knows you're a dog».[33] Hvem man har med å gjøre på nettet, kan generelt være høyst usikkert, noe ikke minst de

30 Lov nr. 16/2010 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) med tilhørende forskrift.

31 *Datakrimstrategien*, Politidirektoratet, 2015, s. 77.

32 L.L. Madsen, Agentvirksomhed online – efterforskning i IT-relaterede sager om misbrug af børn. U.2017B.95. *UfR Online*. Karnov Group. Danmark.

33 Ordtaket stammer fra en vitsetegning laget av Peter Steiner, publisert i *The New Yorker* 5. juli 1993. Wikipedia opplyser at tegningen (per 2013) var *The New Yorker*s til da mest reproduserte og hadde innbrakt Steiner mellom 200 000 og 250 000 USD. en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog. (besøkt 6. juni 2019).

mange ulykksalige historiene om nettdating viser. Usikkerheten går begge veier. Politiet (under fiktiv identitet) kan prinsipielt ikke vite identiteten til den annen part, og den annen part kan ikke ta for gitt at den anonyme brukeren ikke er politi. Derav også munnhellet «The Internet – where the men are men, the women are men, and little girls are FBI-agents».[34]

Krav til notoritet for aktiviteten på internett er nok det viktigste elementet for å hindre uakseptabel politiatferd, noe som stiller betydelige krav til den tekniske infrastrukturen for politiarbeid på nett, foruten et tydelig regelverk. Men dette gjelder generelt, ikke bare for patruljering. For øvrig bør et eventuelt vilkår om at politiet skal tilkjennegi politiidentiteten under patruljering på internett, utformes slik at det ikke omfatter den generelle informasjonsinnhentingen, bare tilstedeværelsen (interaktiviteten) overfor publikum. Ellers kan systemet bli for rigid. Et vilkår som nevnt kan ellers tenkes å virke avklarende, i den forstand at man dermed kan skille patruljering fra spaning og infiltrasjon. Videre kan det tjene de forebyggende, trygghetsskapende og disiplinerende formål som patruljering har.

5. OPPSUMMERING

Gjennomgangen har vist at patruljering på nett skjer i et komplisert terreng både faktisk og rettslig. Konseptet for fysisk patruljering er bare delvis overførbart til internett, siden både observasjon og informasjonsinnhenting kan utføres uten tilstedeværelse på nett. Videre bringer automatisering og kunstig intelligens inn flere utfordringer med hensyn til hvordan metodene bør utformes og reguleres. Hvorvidt reglene bør være teknologinøytrale, må vurderes konkret. Hvis fenomenene i det fysiske og det virtuelle domenet ikke er like, kan det være behov for forskjellige regler for å sikre det felles mål, nemlig en effektiv kriminalitetsbekjempelse som ikke går på bekostning av rettssikkerheten eller menneskerettighetene. For så vidt gjelder patruljering på internett, er det mye som er forskjellig fra det fysiske rom, noe som blir særlig åpenbart ved bruk av kunstig intelligens. Men denne utfordringen melder seg også med full styrke for fysisk patruljering, for eksempel dersom politiet ønsker å bruke «google-briller» for å identifisere kriminelle gjengangere i byrommet. Med «google-briller» mener jeg sensorer og dataskjermer integrert i en brille, som med mobilt internett og kunstig intelligens er koblet til databaser som kan berike brukerens visuelle informasjon. Politiet kan således bruke en «google-brille» for å identifisere personer i folkemengden på grunnlag av ansiktsgjenkjenning, samtidig som personenes straffehistorikk lar seg avlese på skjermen i brillen. Lovgivers utfordringer kommer til å stå i kø i fremtiden, samtidig som den teknologiske utviklingen stiller betydelige krav til politiets etiske refleksjonsnivå. Det er viktig at lovgiver stiller kontrollkrav som er tilstrekkelig teknologispesifikke til at fremtidens politi utvikles i en politisk styrt retning, ikke bare i en retning som gis av teknologiens muligheter.

34 www.quickmeme.com/meme/3r4bus (besøkt 6. juni 2019).