POLITIJURISTENE

NORGES JURISTFORBUND

www.juristforbundet.no

Det Kongelige Justis- og Beredskapdepartement
Gullhaug Torg 4 A
0484 OSLO

lovavdelingen@jd.dep.no

Deres referanse:2012055778 ES/SSA/bj Vår referanse: SB Dato: 19. september 2012

HØRINGSSVAR TIL FORSLAG TIL ENDRING AV DEFINISJONEN AV "OFFENTLIGHET" HVA GJELDER INTERNETT

1. Internett og kriminalitet

Ethvert virusangrep på en PC er, satt på spissen, en kriminell handling. Det skulle vært politiets (del-)ansvar å forhindre og å oppklare disse. En slik tankemessig tilnærming sier noe om potensialet og utfordringene for politi- og påtalemyndighetens tilnærming til cyberkriminalitet.

Organisasjonsutvikling og IKT går hånd i hånd. Politiets IKT har blitt beskrevet som "den veteranbilen vi kjører". Spørsmålet som må stilles blir da hvordan vi skal fange de som kjører racerbil når politiet selv kjører veteranbil? Det er vel få andre svar enn at veteranbilen raskest mulig må byttes ut, særlig hva gjelder IKT-støtte, men også hva gjelder tilnærming og arbeidsmetodikk.

Politi- og påtalemyndighet er ved utviklingen av internett tilført en nytt "territorium" å håndheve lov og orden på. Dette er i forsvinnende liten grad blitt fulgt opp med nye bevilgninger. Noen få millioner har fulgt oppfølgingen av Faremo-rapporten, og i år har Kripos fått noen få millioner øremerket til Datakriminalitet. Politijuristene har vært kritiske til de stadige ropene om mer penger til politiet. Når spørsmålet kommer om hvordan politiet kan bli bedre, og hvordan man skal håndtere den og den utfordringen, er for mange svaret at politietaten må tilført mer ressurser. Vi mener dette er mer hemmende enn stimulerende for utviklingen av norsk politi. Først må politiet evne å tenke nytt, bli kunnskapsstyrt og ikke styrt av meninger, besitte riktig kompetanse ut fra en analyse av hvilket behov vi har og hvilke problemer vi skal løse, få et fremtidsbilde å styre etter, evne å samarbeide og evne å både styre og trekke i samme retning, bli ikke bare omstillingsvennlig men også omstillingsdyktig, evne å bruke ressursene vi har riktig, prioritere riktig og så videre.

Men når det gjelder cyberkriminalitet er bildet noe annet. For på det området har norsk politi- og påtalemyndighet i liten grad blitt tilført noen ressurser noen gang, og aldri for et nasjonalt løft. I den grad det har kommet midler, har det kommet til små enheter ved særorganene, i den tro at det kan løse problemet med kriminalitet på internett. Noe som etter vår oppfatning har vist seg å være både naivt og en helt forfeilet tilnærming. Alle, hele politi- og påtalenorge må gjennomføre et felles løft. Så kan man fortsatt ha særorgan som tar enkelte særskilte saker og områder her, men størsteparten av kriminaliteten bør bekjempes av dagens distrikter.

Dersom norsk politi skal ha en troverdig innsats mot cyberkriminalitet, må det fra øverste politiske nivå være forståelse for den "nye" utfordringen samfunnet står ovenfor, og vilje til å gjøre etaten i stand til å øke publikums følte og reelle trygghet også mot kriminalitet som begås på/ved hjelp av internett.

Det internett har medført, kan deles opp i hvert fall tre bokser, selv om enkelte former passer inn flere steder;

1. Det er kommet helt ny kriminalitet som ikke ville ha eksistert uten internett. Det er dette som går under begrepet "high tech crime". Typiske eksempel er ddos-angrep mot netttjenester, og ikke minst generelt hindring/forstyrring av kommunikasjonen på internett.
2. Det er tradisjonell kriminalitet som benytter internett og som med internett har fått et nytt verktøy for å utføres. Typisk eksempel på dette er bedrageri, som nå kan utføres med e-post. Et annet typisk eksempel er det som behandles i denne høringen, ulike ytringer som ikke skal tillates i det offentlige rom.
3. Det er tradisjonell kriminalitet som har ekspandert/eksplodert som følge av internett, og hvor internett har medført en helt ny arena for å begå denne type kriminalitet. Typisk eksempel på dette er spredning av overgrepsmateriale (barneporno). Eksempelet som behandles i denne høringen, er også et typisk eksempel på denne boksen, ulike ytringer som man ikke ønsker eller vil tillate i det offentlige rom.

Bekjempelse av cyberkriminalitet krever et stort løft på flere områder, som samtlige er ressurskrevende. For det første kreves at man bygger opp riktig kompetanse i etaten. På dette område kan det være fornuftig å få andre profesjoner inn som supplement. Videre må det sørges for vedlikehold og utvikling av eksisterende kompetanse, og at etaten har de til enhver tid nødvendige verktøy. Dette krever en langsiktig innsats og planlegging.

2. Ny straffelov

Det må påpekes at denne problemstillingen, og mange av problemstillingene og utfordringene politiet har stått overfor hva gjelder "lovtomme" rom de siste årene, eller hvor tiden har løpt i fra straffeloven av 1902, skyldes manglende iverksettelse av straffeloven av 2005. Vi tillater oss derfor å påpeke at det grepet regjeringen burde gjøre, var å sette denne nye straffeloven i kraft. Det er vanskelig å prinsippielt kunne forsvare at en lov som har blitt vedtatt av vår lovgivende foramling ikke settes i kraft pga "interne hindringer" i politiet, i dette eksempelet manglende IKT-verktøy. Det problemet bør være opp til politietaten og Justisdepartementet å løse, og ikke

skyves over på samfunnet og det samlede rettsapparat. Rettsstatens prinsipper, blant annet om maktfordeling, burde veid tyngre enn pragmatiske hensyn tatt til politiets arbeidshverdag.

3. Lovforslaget

De forslag som fremmes av Justisdepartementet er etter vår oppfatning et godt og fornuftig forslag. Lovforslaget bør settes i kraft raskest mulig.

Det er lett å ha sympati med mindretallet i Høyesteretts kjennelse av 2. august 2012. Lovgivers intensjon bør ha være en sterk indikator på hvordan staffebestemmelsene er ment å tolkes i en verden i stadig endring. Og i den stadig mer globaliserte og teknifiserte verden, kan det være vanskelig for lovgiver å ramme alle tenkelige eksisterende og kommende straffverdige forhold. Samtidig som det naturligvis er viktig å ha med seg at straffebestemmelser ikke bør tolkes for utvidende, og at det er lovgivers ansvar å vurdere og eventuelt straffeberamme det som måtte være nye straffeverdige forhold. Dette kan være en tidivs vanskelig balansegang, noe som jo også viser seg her ved at Høyesterett var delt.

Men situasjonen nødvendiggjør den foreslåtte lovendring. Og lovteksten kan vi gi vår støtte. Det er et spørsmål om departementet burde gi noen indikatorer på hva som menes med "*et større antall personer*". Slik vi ser det, bør det være tilstrekkelig for straffverdighet at ytringen kan være tilgjengelig for et større antall personer, uten at det skal kreves at ytringen faktisk er sett eller hørt av dette antallet. Men at det nødvendige antall med letthet kan skaffe seg tilgang til ytringen. I forlengelsen av dette kan det bli noe snevert, eller uklart, hva departementet har i tankene når det på side 3 snakkes om "over åpne internettsider". Er bestemmelsen da kun forbeholdt nettsider hvor ingen innlogging kreves? Hva da med nettsider hvor alle vil ha tilgang, men som krever brukernavn og passord av hver deltager? Vi mener departement bør påpeke at en side ikke nødvendigvis må være "ubetinget åpen" for å være offentlig. At man må abonnere eller kjøpe seg adgang til et "trykt skrift" for å lese det, betyr ikke at det "trykte skrift" ikke er offentlig. Når er en weblog (blog) en åpen nettside, og hva med twitterkontoer og facebooksider, ulike diskusjonsfora mv.?

Når det gjelder spørsmålet om jurisdiksjon vil vi gi uttrykk for mer generelle sysnpunkter enn å behandle hver enkelt bestemmelse, men det bør skinne igjennom at flest mulig bestemmelser bør, etter vårt syn, på grunn av internetts natur og funksjon, tas med i strl § 12 nr 4 og evt § 12 nr 3. et av internetts fordeler, og ulemper, er nettopp denne grenseløsheten.

Det synes som om departementet legger til grunn at den straffbare handling skjer når en ytring legges ut på internett, og ikke der den oppfattes eller er ment oppfattet. Det er et spørsmål vi mener departementet med fordel kunne problematisert og drøftet ytterligere, særlig hvor ytringen åpenbart er ment for norske mottakere, eksempelvis at den er på norsk og gjelder norske forhold. Og tilsvarende for andre forhold. Vi er ikke sikre på at spørsmålet er så enkelt som at man skal se på hvor vedkommende befant seg da budskapet ble lagt ut. Dersom et leserinnlegg med straffbare ytringer forfattes og skrives i utlandet og sendes til en norsk avis og trykkes i Norge, hvor er det da riktig å si at den straffbare handling har blitt foretatt?

Bestemmelsene for straffelovens stedlige virkeområde er ikke like godt egnet å benytte på kriminalitet begått ved bruk av internett. Som eksempelet over kanskje kan peke på. Dersom en ytring på en av de store nettavisene sine debattsider er lagt ut på internett i utlandet, er ytringen da ikke straffbar i Norge? Det er lett å mene at formålet med budskapet eller handlingen bør være med på å påvirke straffverdigheten sett med norske øyne, og dermed vurderingen av hvorvidt handlingen skal være straffbar i Norge. Dersom formålet er et å nå et norsk publikum, og budkapet fremsettes på en måte som gjør at det vil være lett mottakelig for et norsk publikum, er det etter vår oppfatning lett å mene at budskapet, om det skal være straffbart, også bør kunne straffeforfølges i Norge.

Moss, 19. september 2012

Sverre Bromander
Leder
Politijuristene