Politidirektoratet

Deres referanse:	Vår referanse:	Sted, dato:
21/53274-3	21/53274	Bryn, 5. august 2021

Bestilling - oppfølging av Prop. 167 L (2020-2021) Endringer i ekomloven

Det vises til skriv fra Justis- og beredskapsdepartementet av 22. april 2021 vedrørende oppfølging av Prop. 167L og behov for mer informasjon fra etatene i den anledning. Videre vises det til tilhørende skriv fra Politidirektoratet av 12. mai 2021.

I det følgende gis innspill fra Kripos knyttet til behov for uthenting i forebyggende øyemed og behov for opplysninger lagret til driftsformål.

Uthenting til forebyggingsformål

Når det pålegges lagring og uthenting av opplysninger til etterforskning, bør det etter Kripos' vurdering også åpnes for at de samme opplysningene kan utleveres når det vil være nødvendig for å forebygge de samme kriminelle handlinger. Forebygging er politiets primærstrategi. Greier etaten å innrette virksomheten sin slik at straffbare handlinger ikke gjennomføres kan man unngå menneskelig lidelse og tap, forhindre skade av annen karakter og spare samfunnet for store kostnader knyttet til reaktiv oppfølging av handlingen og de som er involvert/rammet. Det må i denne sammenheng også sees hen til at de aktuelle opplysninger representerer abonnentinformasjon som er lite personsensitivt og som allerede kan utleveres til bruk for politimessige formål etter ekomloven § 2-9.

NOEN EKSEMPLER

Politiet mottar tips som gi mistanke om at noen forbereder straffbar handling. Dette kan være fra privatpersoner som er deltagere i sosiale medier eller på nettsteder for kommunikasjon. Tipsene kan også komme fra moderatorer på slike nettsteder.

Det finnes for eksempel ideelle organisasjoner som National Center for Missing and Exploited Children (NCMEC) som videreformidler tips til politiet om aktivitet på internett som kan utsette barn for fare. Tilsvarende informasjon kan politiet komme over gjennom åpen og skjult patruljering på internett gjort i forebyggende øyemed. Politiet kan i samme øyemed mer aktivt gjøre bruk av informanter som innehar særskilte kunnskaper om aktivitet på internett.

KRIPOS
Post: Postboks 2094 Vika, 0125 Oslo / Besøk: Nils Hansens vei 25, 0667 Oslo / (+47) 23 20 80 00
kripos@politiet.no / www.politiet.no/kripos / Org.nr: 974 760 827

Tipsene kan typisk gå ut på varsel om deltagere som viser seksuell interesse for barn, personer som med seksuelle undertoner tilbyr kontakt med barn eller som får tilsendt materiale som tilsier seksuell interesse for barn.

Mye av informasjonen som fanges opp gjennom tips og aktivt forebyggende arbeid på internett har naturlig nok et skjult opphav. Det vil si at den det varsles om skjuler sin identitet for eksempel bak et kallenavn. For å kunne vite hvor og mot hvem tiltak skal rettes i slike tilfeller vil en knytning mellom IP-adresse og abonnementsinformasjon være avgjørende.

Politiet har (i tillegg til Nettpatruljen) til enhver tid flere løpende prosjekter innen for forebygging på internett. Et eksempel på et slikt prosjekt er "Hack_OUT". Prosjektet er startet med utgangspunkt i at det i datakrimsaker stadig oppdages at svært unge personer står i fare for å begå datainnbrudd gjennom sin aktivitet på internett. Gjennom forebyggende tiltak for ungdommer som hacker, er det sannsynlig at ungdommer vil kunne avstå fra fremtidige forsøk på slik virksomhet, herunder forsøk på rekrutering fra land som har ønske om å påføre skader på norske interesser. Abonnementsinformasjon knyttet til IP-adresser vil være viktig for å identifisere denne type hackere.

BEHOV FOR LAGRINGSTID OVER TRE UKER

Politiets tilgang til IP-opplysninger til forebyggingsformål avhenger i dag i realiteten av teletilbyders vurdering av eget lagringsbehov til driftsformål. For Kripos fremstår dette som en uakseptabel situasjon, sett hen det ansvar samfunnet har for å forebygge straffbare handlinger. Forebygging er politiets primærstrategi, og de aktuelle opplysninger er svært lite personsensitive.

Dagens regulering innebærer at politiet er avskåret fra forebyggende oppfølging dersom oppfølgende tiltak forutsetter tilgang til IP-opplysninger og oppfølgingsbehovet viser seg mer enn tre uker etter at IP-opplysningene ble lagret. Som beskrevet i høringsprosessen rundt IP-lagring for etterforskningsformål vil behovet for IP-opplysninger ofte vise seg etter denne tre-ukers-perioden. Det samme vil være situasjonen i forbyggingssaker. Fravær av slike opplysninger vil vanskeliggjøre for eksempel politiets muligheter til å sette inn treffende forebyggende tiltak mot personer som opererer på internett eller som bruker internett til kommunikasjon.

VED HVILKEN TYPE KRIMINALITET VIL BEHOVET OPPSTÅ

Dersom en handling kan forebygges før den inntreffer ved hjelp av informasjon om hvem en IP-adresse tilhører, bør politiet som et utgangspunkt kunne innhente denne informasjonen i samme omfang som hvor opplysningene kan innhentes til etterforskningsformål. Dette er heller ikke uvanlig. I en rekke bestemmelser som åpner for utlevering av opplysninger til politiet til forebygging og etterforskning er strafferammen sammenfallende for disse formålene, jf. blant annet passloven § 8 a, vegtrafikkloven § 43 b og utlendingsloven ny § 84 a.

BRUK AV OPPLYSNINGENE TIL FOREBYGGINGSFORMÅL

Abonnementsopplysninger knyttet til IP-adresser er i stor grad opplysninger politiet trenger for å identifisere hvem som kan stå bak spor som er avsatt gjennom aktivitet på internett. Innenfor det forebyggende området betyr dette at politiet da kan fange opp på hvilket område og mot hvem forebyggende tiltak kan settes inn.

Innenfor for eksempel sedelighetsfeltet betyr dette at politiet gjennom å identifisere en person kan finne ut om vedkommende selv har mindreårige barn, om vedkommende

jobber med barn eller har tillitsverv som omfatter samvær med barn. Med denne informasjonen kan politiet finne ut om og i så fall hvilke forebyggende tiltak som er passende for situasjonen.

RAMMER / VILKÅR

Departementet reiser problemstillingen om hvordan det kan sikres tydelige og gode rammer for et system der politiet får tilgang til abonnementsinformasjon tilknyttet IP-adresser med et forebyggendeformål.

Begrepet forebygging favner svært vidt og vi er enige med departementet i at rammer er nødvendig der hvor begrepet skal gi grunnlag for uthenting av denne type opplysninger. Et forslag i så henseende er at man i den nye § 2-8b inntar en tilføyelse som gjør bestemmelsen anvendelig også for forebyggingsformål. Det kan for eksempel gjøres ved en tilføyelse avslutningsvis i bestemmelsens første ledd ved bruk av en ordlyd tilsvarende den som brukes i politilovens § 17d. Da vil første ledd få en slik avslutning; "……., eller åndsverkloven § 104 jf. § 79, *eller dersom det er grunn til å undersøke om noen forbereder en slik handling*." Nødvendighetsvilkåret bør etter vår vurdering gjelde også i forebyggingstilfellene. At det skal gjelde også her kan, om man mener det er uklart, klargjøres i lovteksten eller i forarbeidene. Vi antar at en slik løsning også vil forutsette at man justerer formuleringen *"…..til bruk for etterforsking av alvorlig kriminalitet…"* i den nye § 2-8a første ledd.

KONTROLLMEKANISMER

Etter Kripos mening er det ikke behov for ytterligere mekanismer ut over det som følger av de kompetanse- og formkrav som fremgår av den nye § 2-8b. Det bør nærmere bestemt settes krav om at anmodning fremmes av en med politimyndighet, og at den fremsettes skriftlig slik at det er notoritet rundt uthenting av denne type informasjon også i forebyggendesakene. Det bør utformes et skjema som skal benyttes og dette må ta opp i seg de kvalifiserende vilkår som måtte stilles i loven for uthenting av denne type informasjon.

Skjemaene og opplysningene som innhentes vil være underlagt behandlingsreglene i politiregisterloven med forskrifter og således også være undergitt Datatilsynets tilsynsmyndighet. Etter Kripos' syn er det ikke påkrevet å ha et særskilt behandlings- eller tilsynsregime for denne type opplysninger.

Uthenting etter ekomloven § 2-9

Tilgang til opplysninger som er lagret med driftsformål er ikke underlagt de samme uthentingskrav som de opplysningene som er lagret med et etterforskingsformål. I medhold av § 2-9 kan politiet således få tilgang til IP-opplysninger til forebygging, samt for øvrig IP-opplysninger i etterforskingssaker som ikke oppfyller vilkårene i § 2-8b.

Foruten til forebyggende formål og i etterforskningssaker hvor strafferammekravene i § 2-8b ikke er oppfylt, er politiets tilgang til IP-opplysninger lagret etter § 2-9 særlig viktig for politiets oppgaver innen redningsarbeid, søk etter savnede eller i andre situasjoner hvor politiets hjelp eller inngripen er nødvendig for å avklare situasjoner.

Kripos får som eksempel nesten daglig tips fra moderatorer på flere nettsteder om barn og ungdom som anonymt truer med, eller som opplyser at de er i ferd med å ta sitt eget liv. Av tipsene fremgår hvilken IP-adresse vedkommende benytter og Kripos har da muligheten til å hente ut abonnementsinformasjon om IP-adressen etter § 2-9 tredje ledd. I akutte tilfeller hvor det fremstår som en reell nærliggende fare for at

vedkommende skal gjennomføre et selvmord, vil nødrett kunne gi hjemmel til å innhente abonnementsinformasjon som kan identifisere vedkommende. I mindre akutte situasjoner vil ekomloven § 2-9 gi politiet tilgang på slik informasjon, men det forutsetter at informasjonen faktisk er lagret til driftsformål på det tidspunktet politiet trenger den.

Tilsvarende kommer politiet gjennom nettpatruljering i kontakt med sårbare barn og ungdom med ulike problemer, herunder at de snakker om å ta sitt eget liv. Dette er ofte grobunn for en bekymring. Dette kan være en bekymring som bør rettes til foreldre, barnevernet eller helse. I den grad man har tilgang til abonnementsinformasjon tilknyttet IP-adresse i slike tilfeller, så vil dette kunne hjelpe politiet med å rette bekymringen til rette vedkommende.

Der politiet mottar melding om savnede personer vil logging av IP-adresser sammenholdt med annen informasjon kunne si noe om hvor vedkommende oppholder seg. Videre vil savnedes aktivitet på sosiale medier være en av indikatorene for om vedkommende er frivillig borte eller ikke. Siden slik aktivitet kan være foretatt av andre, vil det være av betydning å kunne sjekke innlogginger mot abonnent for aktuelle IP-adresser. Det samme gjelder for IP-adresser fra bruk av bank-id, mailkorrespondanse mv.

Også innen politiets ordenstjeneste kan abonnementsopplysninger knyttet til IP-adresser være av betydning. Politiet kan for eksempel fange opp planlagte masseslagsmål som kommuniseres på nett, eller arrangører av ulovlige demonstrasjoner som bruker internett til å "kalle inn" deltagere.

Til sist vil uthenting av IP-opplysninger lagret for driftsformål være sentralt ved etterforsking av brann/ulykke, jf straffeprosessloven § 224, fjerde ledd.

Kripos kan – samlet sett - ikke se gode grunner til at det ikke fortsatt skal være mulig å hente ut IP-opplysninger i ovennevnte tilfelle. Dette selv om man finner grunn til å innføre særlige regler om uthenting til forebyggingsformål. Etter vår vurdering foreligger med andre ord ikke gode grunner til å skille tilgangen til abonnementsinformasjon om IP-adresser fra de *"abonnementsopplysninger*" som for øvrig omfattes av § 2-9 tredje ledd. Kripos er snarere bekymret for hva som vil bli situasjonen dersom tilbyders drift ikke lenger nødvendiggjør lagring av IP-opplysninger. Da vil en avgjørende kilde til informasjon av sentral betydning for politiets øvrige oppgaveutførelse forsvinne.

Med hilsen

Ketil Haukaas
assisterende sjef

Dokumenter er elektronisk godkjent uten signatur.

Saksbehandler
padv Håvar Undeland

Kopi
Det nasjonale statsadvokatembetet