POLITIET

Kommunal- og distriktsdepartementet

Politidirektoratet

Deres referanse:	Vår referanse:	Dato:
	22/129918 - 17	09.09.2022

Politidirektoratets høringssvar - Tilleggshøring til ny ekomlov - datasenterregulering

Innledning

Politidirektoratet viser til Kommunal- og distriktsdepartementets høringsbrev av 7. juli 2022. Høringsfristen er 9. september 2022.

Politidirektoratet har forelagt høringen for Finnmark politidistrikt, Politiets IT-enhet (PIT), Politiets fellestjenester (PFT), Kripos og Økokrim.

Politidirektoratet har mottatt innspill fra Kripos og PFT. Mottatte innspill følger vedlagt dette høringssvaret.

Generelle kommentarer

Departementet fremhever i tilleggshøringen datasentrenes samfunnskritiske betydning og den tilhørende samfunnsrisiko ved fravær av nødvendig regulering.

Kripos viser i sin uttalelse til sine tidligere merknader til datasenterstrategien i høring av ny ekomlov (vedlagt), som POD sluttet seg til.[1] Kripos støtter på denne bakgrunn en ytterligere regulering av datasenter, men mener at forslagene i høringen "ikke er omfattende nok til å forebygge de risikoer politiet har vist til – eller til å gi politiet tilstrekkelig og tilsvarende evne til avverging og etterforsking av kriminell aktivitet på datasenterområdet som på andre områder". Kripos mener det er behov for at reguleringen må utvides og skjerpes ytterligere, og at konsekvenser av og risikoer ved datasenternæringen bør utredes i vesentlig større omfang.

Politidirektoratet støtter Kripos' synspunkter, og viser til høringsuttalelsen fra Kripos i sin helhet.

[1] Se PODs høringssvar i høring om forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften (deres ref. 21/3980).

Departementet har innledningsvis i høringsnotatet vist til at man på noe sikt vil vurdere om enkelte datasenter har så stor betydning for nasjonale sikkerhetsinteresser, at sikkerhetsloven bør gjøres gjeldende for disse, men at dette ikke er en del av kravene som foreslås innført nå. Etter Politidirektoratets oppfatning er det behov for en nærmere vurdering og avklaring av dette. Det må forventes at enkelte skjermingsverdige informasjonssystemer i dag ligger på enkelte av de eksisterende datasentrene.

Forslaget til ny ekomlov § 1-5 nr. 36 *Datasenteroperatør*

Politidirektoratet støtter forslaget om at politiet ikke skal omfattes av definisjonen i § 1-5 nr. 36. Politiet har et behov for å skjerme informasjon om hvilke datasentre vi benytter. Det er et klart behov for å kunne hemmeligholde både lokasjon og innhold i disse datasentrene. Vi vil også gjøre oppmerksom på at forslaget i ekomforskriften § 1-9 nr. 8 om at datasenteroperatører skal registrere hvilke statlige, fylkeskommunale og kommunale myndigheter, organer og virksomheter som er kunder hos datasenteret, vil innebære at det behandles opplysninger som har et beskyttelsesbehov.

Forslaget til ny ekomlov § 3-9 *Krav om politiattest*

Direktoratet stiller seg positiv til at det etableres en hjemmel for å kunne kreve fremlagt politiattest av personer som skal ha tilgang til datasenter med vesentlig betydning for sikkerheten i nett eller tjenester. Som både Kripos og PFT understreker i sine høringsinnspill er det imidlertid behov for at det sikres mulighet for å innhente *uttømmende og utvidet politiattest* jf. politiregisterloven § 41, ettersom ordinær politiattest ikke anses som tilstrekkelig for å ivareta behovet for beskyttelse av sensitive opplysninger og kontroll av personell med tilgang til viktig datainfrastruktur. Politidirektoratet støtter dette synspunktet.

Videre gjør Politidirektoratet oppmerksom på at trusselbildet knyttet til innsidervirksomhet tilsier at det samtidig bør etableres en hjemmel om botid, slik at det også kan avkreves politiattest av EØS-borgere fra deres hjemland jf. politiregisterloven § 36 første ledd nr. 1 jf. andre ledd. Botidskravet bør etter vår oppfatning settes til 5 år.

Forslaget til ny ekomforskrift § 1-10 *Terskelverdi for datasenteroperatører*

Departementet har i sitt høringsbrev bedt om innspill på bestemmelsen om terskelverdier for datasenteroperatører, samt muligheten for å omgå regelverket. Politidirektoratet er positiv til å legge bestemmelsen til forskriften for å sikre at denne lettere kan justeres over tid dersom det blir nødvendig. Vi mener samtidig at det må vurderes om terskelverdien skal utformes slik at en datasenteroperatør blir registreringspliktig dersom den eier flere datasenter som i sum overstiger den foreslåtte terskelverdien. Dette vil sørge for at man unngår tilfeller hvor datasenteroperatører oppretter flere datasentre under terskelverdien, for å unngå registreringsplikten.

Med hilsen

Kristine Langkaas
Seksjonssjef

Mathias Muren Lade
Rådgiver

Dokumentet er elektronisk godkjent uten signatur.

Vedlegg:
Høringsinnspill - Tilleggshøring til ny ekomlov - datasenterregulering - Politiets fellestjenester
Høringssvar - datasenterregulering
VEDLEGG til høring - datasenterregulering

Kopi:

Justis- og beredskapsdepartementet	Postboks 8005 Dep	0030	Oslo

POLITIET

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Politiets fellestjenester

Deres referanse:	Vår referanse:	Dato:
	22/129918 - 14	06.09.2022

Innspill til tilleggshøring til ny ekomlov - datasenterregulering

Vi viser til høring om ny ekomlov – datasenterregulering oversendt i brev av 21. juli 2022 og med frist til 25. august 2022 til å komme med innspill. Vi beklager at fristen er oversittet.

Politiets Fellestjenester, vil som ansvarlig for politiets eiendom herunder politiets datasenter støtte beslutningen om at politiet ikke er underlagt ekomloven jf. utkastets § 1-5. Politiet har et særlig behov for å kunne hemmeligholde både lokasjon og innhold i sine datasentre, både der politiet eier og der politiet er leietaker.

Vi støtter også at det stilles krav til politiattest til personer som skal personer som skal ha tilgang til datasenter med vesentlig betydning for sikkerheten i nett eller tjenester jf. utkastets § 3-9. Dette som en følge av en generell endring i trusselbildet i samfunnet.

I utkastet stilles det krav til ordinær politiattest. En ordinær politiattest vil etter vår vurdering ikke være tilstrekkelig for å ivareta kontroll av personell som gis tilgang til viktig datainfrastruktur. Vi foreslår at det også åpnes for at det kan stilles krav for utvidet uttømmende politiattest, slik at også siktelser, tiltaler og forelegg, og dommer som ikke er rettskraftig avgjort også kan bli tatt inn i vurderingen om vedkommendes skikkethet.

Ut over dette har ikke Politiets Fellestjenester kommentarer til lovutkastet.

Med hilsen

Marianne Haahjem
Avdelingsdirektør

Dokumentet er elektronisk godkjent uten signatur.

Kopi:
Helge Clem
Morten Algarheim
Sissel Rogneby

POLITIET
KRIPOS

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Kripos

Deres referanse:	Vår referanse:	Dato:
22/129918	22/129918 - 12	31.08.2022

Høringssvar - datasenterregulering (tilleggshøring til ny ekomlov)

Det vises til Kommunal- og distriktsdepartementets (KDD) høringsbrev av 7. juli 2022 om høring av forslag til ny regulering av datasentre i Norge. Dette er en tilleggshøring til forslaget til ny ekomlov, som var på høring høsten 2021. Videre vises det til Politidirektoratets brev vedrørende høringen av 21. juli 2022 og vår dialog med direktoratet vedrørende forlenget frist for merknader.

Innledning
I høringssvar til ny ekomlov uttrykte Kripos klar bekymring knyttet til etablering og drift av datasentre. Som redegjort for der opplever vi store utfordringer på området knyttet til manglende krav til virksomheten og tilhørende manglende muligheter til reell og effektiv myndighetskontroll, hvilket "*svekker politiets evne til å forebygge, avverge og etterforske et bredt spekter av digital kriminell aktivitet som kan gjennomføres på og/eller gjennom norsk territorium og i virksomheter underlagt norsk jurisdiksjon*." Den regulering av virksomheten som ble foreslått i ny ekomlov var etter Kripos' vurdering ikke egnet til å avhjelpe utfordringene. Våre merknader til datasenterstrategien i høring av ny ekomlov har fremdeles relevans og vedlegges[1].

I lys av ovennevnte merknader er Kripos positiv til at departementet gjennom tilleggshøringen ser behov for en ytterliggere og skjerpet regulering. Den regulering som foreslås nå – gjennom forslag til lov- og forskriftsendringer – adresserer i større grad dagens utfordringer, særlig innenfor generelle sikkerhets- og beredskapskrav. Det er bra og viktig. Samtidig er forslagene ikke omfattende nok til å forebygge de risikoer politiet har vist til - eller til å gi politiet tilstrekkelig og tilsvarende evne til avverging og etterforsking av kriminell aktivitet på datasenterområdet som på andre områder.

Departementet påpeker svært tydelig i tilleggshøringen datasentrenes samfunnskritiske betydning og den tilhørende samfunnsrisiko ved fravær av nødvendig regulering. Denne vurdering tiltres av Kripos. Dagens trusler – i form av kriminell aktivitet mot og ved hjelp av datasentertjenester – er svært reelle og aktuelle, og konsekvensene potensielt store og av samfunnskritisk betydning. Kripos er fortsatt bekymret. Vi mener forslagene fremsatt i tilleggshøringen ikke går langt nok - og at regulering må utvides og skjerpes.

[1] Kapitel 7 i Kripos' høringssvar til Politidirektoratet datert - 1.10.2021 (WS 21/82791)

Post: Postboks 2094 Vika, 0125 Oslo
Tlf: (+47) 23 20 80 00
Org. nr: 974760827
E-post: kripos@politiet.no
www.politiet.no

Kripos mener konsekvenser av og risikoer ved datasenteræringen bør utredes i vesentlig større omfang enn det som i dag er tilfelle. Forvaltningen av datasenternæringen i Norge er etter Kripos' oppfatning preget av at næringen er ny og at den har blitt etablert uten at det er tatt tilstrekkelig hensyn til behovet for og mulighetene til å kunne håndheve norsk lov overfor virksomheten. Ønsket om å utnytte næringspotensialet i datasenternæringen for å sikre investeringer og arbeidsplasser i Norge har vært den dominerende kraften, og nødvendige krav til sikkerhet, beredskap og myndighetskontroll er så langt vektlagt i for liten grad.

Næringen er imidlertid allerede etablert. Realitetene gjør at skjerpede regler - i påvente av en mer omfattende utredning - nå må prioriteres. I den anledning vil Kripos i det følgende knytte merknader til de forhold og den regulering som for oss fremstår som viktigst å berøre i forestående lovarbeid.

Generelt om behov og utfordringer

En sentral utfordring med dagens situasjon er at både organiserte kriminelle og avanserte kriminelle aktører tilnærmet fritt kan utføre skadeverk, spionasje og dataangrep både mot Norge og andre nasjoner ved hjelp av norske IP-adresser og servere fysisk plassert på norsk jord, uten at norske myndigheter har reell mulighet for å ettergå hvem som faktisk står bak handlingene.

Trusselaktørenes vilje, evne og muligheter til å gjennomføre digitale angrep mot virksomheter, infrastruktur og tjenester innen elektronisk kommunikasjon utgjør en alvorlig og omfattende trussel som det er viktig å kunne verne Norge imot. Dette enten den kriminelle virksomhet er rettet mot datasystemer i Norge eller ved at datasentre her benyttes til straffbare handlinger i/mot andre land.

Kripos har ved flere anledninger opplevd store utfordringer med å innhente nødvendig informasjon fra tilbydere og virksomheter som opererer innenfor eller i tilknytning til datasentertjenester i Norge. Utfordringene har blant annet bestått i manglende muligheter for å identifisere virksomheter og ansvarlige personer for hosting- og kommunikasjons-infrastruktur og tilhørende tjenester i tilknytning til datasentervirksomhet. Det er etter gjeldende rett ingen krav om identifisering av hverken virksomheter eller ansvarlige personer, og det stilles heller ingen krav til notoritet over hvilke data som er lagret hvor i datasentrene. Manglende krav til fysisk representasjon gjør videre at iverksettelse av nødvendige inngrep vanskeliggjøres ytterligere. De som driver datasentertjenester i Norge bør ha en plikt til å følge prinsippene om "Know your costumer" og herunder ha evne til å identifisere den enkelte kunde i sine anlegg.

Gjeldende regelverk må sikre reell mulighet for myndighetsoppfølging overfor datasenternæringen i samme utstrekning som den regulering og oppfølging som i dag kan gjøres gjeldende overfor annen ekominfrastruktur – herunder tilbydere av ekomnett og -tjenester.

Reguleringen i andre land

Ekomnæring og myndighet har over tid og ved flere anledninger vist til at de er opptatt av at det skal være mest mulig lik regulering og like vilkår for drift av sammenfallende næringer mellom ulike land – dette fordi ulikheter mellom landene blant annet antas å være konkurransevridende. Kripos legger til grunn at dette utgangspunkt og disse hensyn også har relevans for regulering av datasentre, og at en løsere (eller strengere) regulering i Norge enn i

våre "naboland" vil kunne fungere som push/pull-faktorer for etablering og drift. En mindre krevende regulering antas på samme måte å øke risikoen for at kriminelle velger Norge og norske datasentre som aktuelle for sin kriminalitet.

Reguleringen i andre land er ikke berørt i høringen. For Kripos fremstå det som en mangel. En mer omfattende utredning av konsekvenser og risikoer ved næringen bør omfatte slike sammenligninger. Kripos vil – for nærværende høring – bemerke at Kripos gjennom etterforskingssamarbeid med flere land har erfart at de har muligheter til å gjennomføre bevissikring i datasentre som norsk politi ikke har i dag. Et eksempel på dette er Nederland.

Ekomtilbyder v/s datasentre

Flere steder i tilleggshøringen understrekes betydningen av at datasenternæringen skal underlegges krav tilsvarende annen "ekominfrastruktur" eller underlegges regulering tilsvarende "ekomtilbydere" for øvrig. Departementet foreslår samtidig å innføre egne definisjoner av datasenter, datasentertjeneste og datasenteroperatør. Slik lovforslaget er lagt opp fremgår det klart at datasentre ikke anses å omfattes av ekomlovens tilbyderbegrep eller dens definisjon av elektronisk kommunikasjonstjeneste.

Valg av en slik systematikk i lovforslaget fremstår problematisk for politiet, idet mye av den regulering som etablerer forpliktelser i forhold til og gir rettigheter til politiet (og andre myndigheter) er knyttet opp mot tilbyderbegrepet og tilhørende elektronisk kommunikasjonstjeneste.

Et sentralt eksempel og en stor utfordring for politiet knytter seg de datasenteroperatører som tilbyr tjenester som inkluderer internett-aksess. Kripos mener denne delen av datasentervirksomheten idag naturlig omfattes av ekomlovens tilbyderbegrep. Slik aksess vil nå – slik vi oppfatter forslaget – være del av virksomheten til både en tilbyder av elektronisk kommunikasjonstjeneste og en datasentertjeneste. En vesentlig del av de saker Kripos involveres i med denne typen aktører starter med en IP-adresse knyttet til kriminelle handlinger, hvor politiet ønsker å undersøke hvem som benytter IP-adressen og hva den benyttes til. Hvis aktører som leverer norske IP-adresser entydig og eksplisitt defineres som tilbydere, og dermed underlegges de krav og plikter som tilligger disse etter ekomloven, så vil politiets behov for knytning mellom adresse og bruker i det vesentlige være ivaretatt. I dag skjer politiets uthenting av nødvendig informasjon fra tilbyder etter ekomlovens § 2-9 tredje ledd (ny ekomlov § 3-2), og fra 1. januar 2023 i etterforsking gjennom bruk av det nye IP-lagringsregelverket i ekomloven § 2-8a og 2-8b (ny ekomlov §§ 3-4 og 3-5). Ingen av disse nåværende eller nye regler omfatter i praksis eller formelt datasentervirksomhet, og med den regelverks-tilnærming departementet har valgt synes det klart at datasentervirksomheten positivt må fremgå av konkret bestemmelse ved siden av "tilbyder" for at virksomheten skal være forpliktet etter regelverket.

Der vanskelig for oss å få full oversikt over hva dette innebærer, men slik vi oppfatter forslaget vil dette altså blant annet få som følge at ekomlovens taushetspliktsbestemmelse og tilhørende regler om utlevering av abonnentsopplysninger (ny lov § 3-2) samt ekomlovens regler om lagring og utlevering av IP-adresser (ny lov §§ 3-4 og 3-5) ikke vil gjelde for datasentervirksomhet. Det samme vil være tilfellet for ekomlovens regler for tilrettelegging for lovbestemt tilgang til informasjon (ny lov § 3-6).

Dette er eksempler på helt avgjørende og sentrale regler for politiets evne til forebygging, avverging og etterforsking. Dersom datasenternæringen går klar av regelverk som dette vil

politiet ikke kunne ivareta sine oppgaver på feltet. En slik situasjon vil stå i tydelig kontrast til departementets risikobeskrivelser og dets uttalte målsetting om å regulere denne næringen *"….på lik linje med annen ekominfrastruktur".*

Kripos mener at den lovgivningstekniske tilnærmingen burde vært vurdert grundigere. Dersom valg av lovgivningsteknikk fastholdes, understrekes det tydelig fra Kripos at man i tilknytning til nåværende lovarbeid må sørge for en regelgjennomgang som sikrer at sentralt regelverk som etablerer forpliktelser i forhold til og gir rettigheter til politiet (og andre myndigheter) også vil omfatte datasentervirksomhet. Herunder nevnte regler om taushetsplikt, IP-lagring og tilrettelegging.

Definisjonen av datasenter i § 1-5
Forslaget til definisjon av datasenter i § 1-5 nr 34 er i utgangspunktet en vid og generell definisjon som dekker alt fra et enkelt datarom til virksomheter som i høringsnotatet er omtalt som en såkalt «hyperscale» datasenterinstallasjon. Dette er en definisjon som i utgangspunktet utelukkende er knyttet til datasentrenes funksjon. Hvilke datasentervirksomhet som "til slutt" omfattes av regelverket vil i praksis avklares gjennom de tilhørende definisjoner av datasentertjeneste og datasenteroperatør.

Fra Kripos' ståsted synes definisjonen i for stor grad å være utformet ut i fra ønske om å ha oversikt over de datasenter/datasentertjenestene som er av en slik størrelse og omfang at de antas å ha betydelig samfunnskritisk betydning, mens mindre aktører ikke er tatt med. Det vises blant annet til betydningen av den terskelverdi som oppstilles i forslag til forskrift § 1-10 og dennes knytning til definisjonen av datasenteroperatør i lovforslagets § 1-5 nr 36. Kraftforbruk som terskelverdi synes for øvrig lite egnet av den grunn at stadig større datamengder/informasjon gradvis vil antas å kunne lagres med mindre kraftforbruk.

Kripos vil understreke at selv "små" datasentre kan benyttes til svært omfattende og alvorlig kriminalitet og behovet for å kunne håndheve norsk lov overfor disse er like stor som hos de datasentrene som nå foreslås omfattet. Basert på vår sakserfaring vil derfor en løsning som foreslått ikke være god nok for ivaretakelse av politiets oppgaver og samfunnets beskyttelsesbehov. Også her antas for øvrig fravær av nødvendig regulering for "mindre" aktører å øke risikoen for at kriminelle velger Norge og norske datasentre som aktuelle for sin kriminalitet. Igjen synes grensesnittet mot tilbyderbegrepet og valgt lovteknikk relevant, idet ekomloven åpenbart *ikke* skiller på "store" og "små" tilbydere hva gjelder regelverk som etablerer forpliktelser i forhold til og gir rettigheter til politiet (og andre myndigheter).

Kripos støtter forøvrig forslaget om at definisjonen av datasenteroperatør ikke omfatter tilbydere av elektronisk kommunikasjon som utelukkende realiserer tjenesteproduksjon av egne tjenester. Det sentrale bør etter Kripos sin oppfatning være om det tilbys slike tjenester til andre mot eller uten vederlag.

Til sist bemerkes til forslaget til regelutforming i § 1-5 nr 36 at formuleringen *"..inkludert Politiets sikkerhetstjeneste.."* uansett bør utgå. Det fremgår klart av politiloven at PST er en inkludert del av politiet. Det er således unødvendig å understreke dette i bestemmelsen. En slik (unødvendig) understreking har det problemet ved seg at den gir grunnlag for feilaktige antitetiske tolkninger av bestemmelser i annen lovgivning hvor PST ikke nevnes særskilt.

Registreringsplikt
Kripos støtter forslaget om registreringsplikt for datasenteroperatør på lik linje med ekombransjen for øvrig, og vi ser stor nytte av en oversikt over næringens operatører. Som høringsforslaget fremhever vil dette avhjelpe politiets behov for å komme i kontakt med aktuelle datasentre. Vi vil samtidig gjenta vår merknad fra avsnittet over hva gjelder definisjon av datasenter og hvilke virksomheter som omfattes. Politiets behov for kontakt med virksomheter vil ikke styres av deres størrelse.

Kripos vil peke på to sentrale mangler ved forslaget til registreringsplikt, henholdsvis fravær av krav om at operatør må ha oversikt over senterets kunder og hvor i senteret kundens virksomhet foregår, samt fraværet av krav til fysisk representasjon i Norge for operatør.

En helt sentral forutsetning for effektiv og forholdsmessig kriminalitetsbekjempelse er – på dette som på andre områder - at politiet rent faktisk gjøres i stand komme i inngrep med den/de som er involvert der hvor virksomheten utøves. Forebygging, avverging og etterforsking av den type kriminalitet det her er snakk om forutsetter svært ofte bruk av tiltak, tvangsmidler og andre metoder som rettes mot konkrete fysiske adresser eller spesifikke deler av et senters virksomhet. Uten en fysisk representant for datasenteroperatør å forholde seg til, og uten ytterligere krav til oversikt over kunder og hvor i senteret deres virksomhet drives fra vil politiet møte store utfordringer til effektiv kriminalitetsbekjempelse.

Foreslått registreringsplikt bør derfor suppleres med krav om at operatør må ha oversikt over senterets kunder og hvor i senteret kundens virksomhet foregår, samt krav til fysisk representasjon i Norge for operatør.

Kripos bemerker for øvrig at det legges opp til at registreringsplikten - som for ekomtilbydere – innebærer plikt til registrering "*hos myndigheten*". Det vil si registrering hos Nkom. For at politiet skal kunne nyttiggjøre seg opplysningene er det sentralt at Nkoms oversikt gjøres lett tilgjengelige for politiet - gjerne ved direkte tilgangsløsning. Kripos forutsetter at slik tilgang er uproblematisk. I den grad departementet mener tilgang krever særlig hjemmel, må slik hjemmel klart fremgå som del av reguleringen.

Politiattest
Det er positivt at departementet ser behovet for å klargjøre at krav om politiattest også kan settes av datasenteroperatør - jf ny ekomlov § 3-9. Det er rimelig å anta at bedret personell-kontroll vil ha en positiv betydning for sikkerheten i både nett og tjenester.

Kripos vil imidlertid gjenta og understreke våre anførsler til denne bestemmelsen, inntatt i vårt høringssvar til ny ekomlov (punkt 8.7). Bestemmelsen – slik den er utformet nå – ivaretar ikke i tilstrekkelig grad behovet for beskyttelse av sensitive opplysninger. Som nærmere redegjort for i vårt høringssvar til ny ekomlov mener Kripos at;

- det bør sikres mulighet for å innhente *uttømmende og utvidet politiattest*, jf politiregisterloven § 41. Mange forhold påføres kun *ordinær* politiattest dersom de er ilagt mindre enn tre år før utstedelsen.
- det et bør tas inn et krav om attest utstedt fra annet EØS-land, alternativt krav om botid. Norsk politiattest har ingen verdi dersom aktuell person har kortvarig tilknytning til Norge. Dette er en ytterst reell problemstilling for flere med tilgang til sensitive opplysninger ved datasentre. Botidskravet bør settes til fem år.

Departementet understreker i tilleggshøringen faren for innsidetrusler og den risiko denne representerer for samfunnskritisk virksomhet. Tilgangssikring – herunder krav om politiattest - er et sentralt tiltak i så henseende. Det er imidlertid helt avgjørende at reguleringen er reell i den forstand at den treffer utfordringene. I tillegg til ovennevnte forhold mener Kripos man bør vurdere å pålegge at attest *skal* legges frem i de aktuelle situasjoner. Lovforslaget bruker i dag formuleringen "*kan kreve fremleggelse*". For Kripos fremstår dette for "svakt" som redskap for ivaretakelse av den sensitivitet og forebyggelse av den risiko departementet adresserer. Skal man ha befatning med opplysninger "*med vesentlig betydning for sikkerheten*" bør ikke attestasjon for vandel være noe datasenteroperatør kan velge bort.

Tillatte bruksbegrensninger
Kripos støtter departementets forslag om å klargjøre at datasenteroperatør omfattes av reglene om bruksbegrensinger i ny ekomlov § 3-12. Reglene i første og andre ledd er helt nødvendige for nasjonal sikkerhet og andre viktige samfunnsinteresser.

Kripos kan bemerke at vi – som internasjonalt kontaktpunkt - i enkelte tilfelle mottar informasjon fra samarbeidene myndigheter som nødvendiggjør umiddelbar varsling av utsatte virksomheter. Dette kan typisk være opplysninger som begrunner en nødsituasjon, eller representerer alvorlige trusler mot liv eller helse, nasjonal sikkerhet mv. og som også kan forutsette pålegg om bruksbegrensninger. Politiet har inngreps- og påleggshjemler i politiloven som kan være anvendelige i slike situasjoner, men vi tilstreber rutinemessig å varsle og samarbeide med fagmyndighetene gjennom samarbeidet i Felles Cyber Koordinerings Senter (FCKS).

Med hilsen

Ketil Haukaas
assisterende sjef Kripos

Dokumentet elektronisk godkjent uten signatur.

Saksbehandler
Knut Jostein Sætnan
politiadvokat

Vedlegg:
VEDLEGG til høring - datasenterregulering

VEDLEGG
(Kap 7. i Kripos' høringssvar av 1.10.2021 til ny ekomlov.)

7. Datasenterstrategi

Regjeringen lanserte den 11.8.2021 strategien "Norske datasenter - berekraftige, digitale kraftsenter". I kapitel 4.1.2 vedr. "Regulering av datasenter" er det opplyst at Regjeringen tar sikte på å høre en rammehjemmel for datasentervirksomhet i forbindelse med forslaget til ny ekomlov. Kripos antar at det i det vesentlige er bestemmelsene i forslaget til ny ekomlov § 3-8 tredje og sjette ledd det siktes til i denne sammenhengen.

Regjeringen har i strategien lagt særlig vekt på at Norge har et godt utgangspunkt hva gjelder å være et attraktivt land å investere i når det gjelder etablering av datasentre, og de viser i denne sammenheng særlig til at vi har god og sikker tilgang til fornybar kraft, en solid digital infrastruktur, høy kompetanse og stabile rammevilkår. Regjeringen vil derfor arbeide for økt vekst i datasenternæringen. Det er i strategien videre lagt vekt på at denne utviklingen skal skje på en bærekraftig måte.

Kripos vil påpeke viktigheten av at slik virksomhet må innrettes med tilstrekkelig fokus på kontroll og tilsyn, og at politiet gis reelle muligheter til å håndheve norsk lov. Slik er det ikke nå og det synes heller ikke som om at strategien i tilstrekkelig grad tar hensyn til hvilken risiko som følger med en storstilt etablering av datasentre i Norge.

Kripos har ved flere anledninger opplevd store utfordringer med å innhente tilstrekkelig informasjon fra tilbydere og virksomheter som opererer innenfor eller i tilknytning til datasentertjenester i Norge. Utfordringene har bestått i manglende muligheter for å identifisere virksomheter og ansvarlige personer for hosting- og kommunikasjonsinfrastruktur og tilhørende tjenester i tilknytning til datasentervirksomhet. Det er etter gjeldende rett ingen krav om identifisering av hverken virksomheter eller ansvarlige personer. Det stilles heller ingen krav i dag til notoritet over hvilke data som er lagret hvor i datasentrene. Dette svekker politiets evne til å forebygge, avverge og etterforske et bredt spekter av digital kriminell aktivitet som kan gjennomføres på og/eller gjennom norsk territorium og i virksomheter underlagt norsk jurisdiksjon.

Med dagens lovverk er norske myndigheter i mange sitiuasjoner forhindret fra å effektuere lovlig fattede beslutninger. Sett fra Kripos' ståsted synes samtidig nasjonale tilsynsmyndigheter å mangle muligheter til effektiv og tilstrekkelig kontroll.

Ved at Norge blir et mer attraktivt marked for datasentre, vil det også tiltrekke seg utenlandske aktører. Vi må påregne at antall anmodninger fra utenlandske samarbeidspartnere om etterforskning av informasjon i norske datasentre vil øke. Et fravær av effektiv kontroll kan medføre at Norge blir en frihavn for IKT-relatert kriminalitet. I ytterste konsekvens kan sågar statlige aktører misbruke norske datasentre i angrep mot tredjeland.

VEDLEGG
(Kap 7. i Kripos' høringssvar av 1.10.2021 til ny ekomlov.)

Det opplyses i strategien at regjeringen vil følge opp regulering av datasentre gjennom dialog med datasenternæring og relevante styresmakter. I tilknytting til dette vil Kripos fremheve politiet som en åpenbart relevant styresmakt i denne henseende. Vi konstaterer imidlertid at hverken forarbeidene til ny ekomlov eller den aktuelle datasenterstrategi omtaler disse forhold i særlig grad eller omtaler politiet som sentral adressat for nevnte dialog.

Det er i strategien eksplisitt uttalt at "*Regjeringa vil at datasenter blir vurderte for regulering i ekomregelverket og anna relevant regelverk for å ivareta digital tryggleik og nasjonale tryggleiksinteresser.",* og at "*Regjeringa vil delta aktivt i europeisk samarbeid for å bidra til formålstenlege, og primært felleseuropeiske, løysingar for å vareta digital tryggleik, kamp mot kriminalitet og nasjonale tryggleiksinteresser knytt til datasenterverksemd*." Til det siste er det opplyst at NIS 2-direktivet, som omhandler slike problemstillinger, for tiden er til behandling i europaparlamentet og rådet. Kripos er bekymret for at dette betyr at det ikke vil skje noe med disse utfordringene før arbeidet med NIS 2-direktivet er avsluttet eller i alle fall har fått en tydelig "retning".

Kripos opplever at kriminalitetsbekjempelse tilknyttet datasentervirksomhet i Norge hindres av klare regulatoriske mangler, som eksempelvis manglende mulighet til å spore datatrafikken fra datasenter i Norge.

Dersom det ikke snarlig tas hensyn til disse utfordringene vil datasentre i Norge kunne tiltrekke seg kriminalitet fra hele verden. En datasenterstrategi som ikke i tilstrekkelig grad tar tak i de ovenfor nevnte utfordringer, vil i vesentlig grad kunne forsterke uønsket utnyttelse av datasentervirksomhet i Norge og medføre store utfordringer både nasjonalt og internasjonalt.

Slik Kripos leser forslaget til ny § 3-8 det fokuseres det i det alt vesentlige på datasikkerhetssiden og regelen gir i liten grad rom for tiltak som vil bidra til politiets forebyggende eller kriminalitetsbekjempende arbeid.