UDI

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Unntatt offentlighet
offl. § 24.3

Deres ref: 14/7082 **Vår ref:** 14/4656-5/UKOT 21.01.2015

Høring - Forslag til endring i politiloven og ekomloven

Vi viser til Justisdepartementets høringsbrev av 04.12.2014 vedrørende Justisdepartementet og Samferdselsdepartementets forslag til endring i politiloven og ekomloven som vil gi politiet myndighet til å gripe inn og forstyrre eller hindre den elektroniske kommunikasjonen i et område som et politioperativt tiltak i særlig situasjoner.

Tiltakene vil kunne benyttes for å forebygge eller avverge kriminalitet. Slik vi forstår forslaget er det således ikke et inngrep etter straffeprosessen, og det vil ikke være krav om rettslig kjennelse.

Bestemmelsene vil gi politiet myndighet til å identifisere mobilkommunikasjonsanlegg og jamme disse, jamme et område, stenge elektroniske systemer, avbryte styringssignaler, avbryte lyd- og billedoverføring, innstille eller avbryte overføring av samtaler eller elektronisk kommunikasjon og stenge anlegg for kommunikasjon m.v. Det foreslås to ulike alternativ for når metodene kan benyttes og videre foreslås en endring i ekomloven som innbærer at metodene kan tas i bruk uten å varsle ekomtilbyderne og tilsynsmyndighet.

Generelt

Lovforslaget reiser viktige prinsipielle spørsmål knyttet til Grunnlovens § 102 og EMK art 8. Bestemmelsen vil gi politiet adgang til å iverksette inngripende metoder for å forebygge og avverge kriminalitet. Tiltaket er integritetskrenkende og vil kunne føre til at et stort omfang uskyldige personer og virksomheter blir krenket. Hensynet til at politiet effektivt kan forebygge og hindre alvorlige straffbare handlinger må således avveies mot hensynet til personvernet og rettsikkerheten. Det er imidlertig også av betydning at man i avveining av kommunikasjonsregulering vurderer konsekvensene for virksomheters drift, beredskap og eventuelle forpliktelser som kan bli skadelidende.

Vi ser at politiet i konkrete, alvorlige tilfeller vil ha behov for å iverksette tiltak som foreslås, men tiltakene er til dels veldig omfattende og vil kunne berøre den elektroniske kommunikasjonen for svært mange uskyldige, både private

Utlendingsdirektoratet
Norwegian Directorate
of Immigration

Hausmanns gate 21
Pb. 8108 Dep. NO-0032 Oslo
+47 23 35 15 00

udi@udi.no, www.udi.no
Bankkontonummer 7694 05 10712
Organisasjonsnummer 974760746

og virksomheter. Slik forslaget er utformet er det en risiko for at politiet kan iverksette tiltak som er for omfattende. En større grad av konkretisering vil kunne redusere denne risikoen.

Ut over dette velger Utlendingsdirektoratet (UDI) ikke å diskutere de rettsikkerhetsmessige og personvernrettslige problemstillingene ved forslaget. Vi kommentere heller ikke de to ulike alternativene. UDI har valgt å ha fokus på mulige konsekvenser av bestemmelsene for vår virksomhet.

Konsekvenser for UDI

De inngrep som forslagene gir adgang til, vil kunne ramme både privat bruk av mobile- og elektroniske systemer, og det vil kunne ramme UDIs systemer dersom hensynet til samfunnets behov for beskyttelse tilsier det. Vi mener det er uklart om den foreslåtte bestemmelsen i politilovens § 7 b også omfatter kabelbaserte løsninger, og ikke kun trådløs kommunikasjon. Videre oppfatter vi at regelverket kan åpne for avlytting, og ikke kun jamming / stenging.

Politilovens § 7 b vil kunne innebære at UDIs datasystemer og mobilkommunikasjon kan bli tatt ned, jammet eller avbrutt i en politiaksjon uten at vi blir informert om det, dersom vilkårene for øvrig er til stede. UDIs lokaler er sentralt plassert i Oslo der det må forventes at det kan forekomme alvorlig kriminalitet, og hvor regulering dermed kan bli iverksatt.

Konsekvenser for våre internasjonale forpliktelser?

UDI har vurdert om forslaget vil kunne være i strid med våre internasjonale forpliktelser etter VIS og Eurodac regelverket, dersom disse EU-systemene blir berørt av rettshåndhevende myndigheters inngrep i den elektroniske kommunikasjonen. Dette er kabelbaserte løsninger, og vil kun berøres dersom forslaget også omfatter dette.

Rettshåndhevende myndigheters tilgang til VIS og Eurodac reguleres henholdsvis av VIS-forordningen artikkel 3 og Eurodacforordningen artikkel 6. Felles for begge systemer er at tilgang til data for politiformål er begrenset til å forhindre, avsløre eller etterforske terrorisme eller annen alvorlig kriminalitet. Hva som utgjør terrorisme eller annen alvorlig kriminalitet er nærmere definert i Eurodac-forordningen artikkel 2 nr. 1 bokstavene j og k.

Ordlyden i begge forslagsalternativene til politilovens § 7 b er i utgangspunktet vid, men slik UDI forstår forslaget til lovendringer handler det om å begrense eller avbryte kommunikasjon, ikke om å sikre seg tilgang til kommunikasjonen eller dataene som kommuniseres. Vi forutsetter derfor at forslaget ikke medfører en utvidelse av dagens tilgang til systemene for rettshåndhevende myndigheter. Det er følgelig ikke nødvendig å gå nærmere inn på forholdet mellom i hvilke tilfeller rettshåndhevende myndigheter kan gis tilgang til VIS eller Eurodac, og alternativ 1 og 2 for når politiet skal kunne benytte de foreslåtte tiltakene.

Dersom signalforstyrrelser eller blokkering som foreslått skulle opptre hyppig eller over lengre tid, vil det kunne få konsekvenser for forventningene om

oppetid for de nasjonale delene av EU-systemene. Vi er forpliktet til på nasjonalt nivå å sørge for størst mulig grad av kontinuerlig og korrekt drift.

VIS-forordningen artikkel 32 og Eurodac-forordningen artikkel 34 oppstiller strenge krav til nasjonalstatens overholdelse av ulike sider ved datasikkerhet. Særlig kravene til kommunikasjonskontroll og transportkontroll (VIS art. 32 bokstavene h og j, Eurodac art. 34 bokstavene h og j) kan tenkes å bli utfordret ved forstyrring / avbrytelse av datakommunikasjon som foreslått.

Tekniske og driftsmessige konsekvenser

UDI mener at kommunikasjonsregulering som foreslått vil kunne ramme UDIs kommunikasjon med mobiltelefon både intern og eksternt, vårt trådløse nettverk internt og ev også UDIs kommunikasjon med kablet nett.

Vi kan her peke på sårbarhetene, men ikke fastslå konsekvensene av at våre kommunikasjonsnett blir tatt ned. Det krever en grundigere analyse. En slik analyse med forslag til tiltak bør gjennomføres av virksomheten dersom forslaget vedtas.

Vi er fullt ut avhengig av elektronisk kommunikasjon i vår daglige virksomhet, også i beredskapssituasjoner. Det gjør oss sårbare dersom politiet velger å ta ned kommunikasjonsnettet for eksempel ved en trussel mot UDI. Politiet bør dermed også være kjent med disse sårbarhetene for å kunne foreta den nødvendige konkrete avveining.

Mobiltelefon:
UDI bruker i dag kun mobilnettet. En eventuell blokkering av mobiltrafikken vil kunne forhindre nødvendig kommunikasjon ved eventuell evakuering eller i andre beredskapssituasjoner.

Kritiske feil på våre datasystemer varsles også over mobilnettet. Gjeldende varslingssystem vil således ikke kunne benyttes.

To faktor autentisering for pålogging av systemene eksternt brukes av mobilnettet. Det betyr at i berørte områder vil brukere ikke kunne logge seg på fra eksterne lokasjoner.

Sentralbordet vil være i drift, men det vil ikke være mulig å sette over samtaler til mobiltelefonene.

Kablet nett:
Dersom sentrale kommunikasjonshubber for kablet nett også stenges, vil UDI i perioder kunne bli helt isolert, og UDI vil ikke kunne foreta ordinær saksbehandling. Det kan også medføre at Politiets grensekontroll vil være utilgjengelig.

Trådløst nett:
UDIs trådløse nett er per i dag ikke virksomhetskritisk, og kan være utilgjengelig i perioder uten store konsekvenser.

Oppsummering:

Lovforslaget (begge alternativ til ny politilov § 7 b) vil kunne medføre konsekvenser for UDIs produksjon, våre internasjonale forpliktelser og vår beredskapssituasjon. Hyppighet og tidsaspekter på kommunikasjons-reguleringen vil selvfølgelig påvirke konsekvensene.

Politiet bør være kjent med konsekvensene for virkomheten for å foreta en konkret avveining.

I etterkant av en slik situasjon, vil vår virksomhet måtte foreta noe opprydding og sjekk av systemer, evt saksbehandling for å verifisere at man er tilbake i normal drift.

Med hilsen

Stephan Mo
avdelingsdirektør

Marius Mølmen Moen
seksjonssjef

Kopi : Justis- og beredskapsdepartementet v/Innvandringsavdelingen

Dokumentet er godkjent elektronisk i Utlendingsdirektoratet og har derfor ingen signatur. Brevet sendes kun elektronisk.