POLITIET
KRIPOS

Politidirektoratet
Postboks 8051 Dep.
0031 OSLO

NCIS Norway

Deres referanse:	Vår referanse:	Sted, dato
	201900341-2	Oslo, 29.1.2019

HØRINGSUTTALELSE – NORSK KRYPTOPOLITIKK

Det vises til høringsanmodning mottatt 18. januar 2019 fra Politidirektoratet om Forsvarsdepartementets utkast (mottatt i form av notat) til revidert norsk kryptopolitikk.

Våre innspill begrenser seg til kriminalitetsbekjempelse, og tar hovedsakelig til orde for to tiltak:

- Samarbeid politi/kryptoindustri
- Gjeninnføring av straffesanksjon for brudd på strpl. § 199a

Nedenfor følger Kripos' grunnlag for å vurdere disse tiltakene.

Kripos stiller seg bak de overordnede mål for norsk kryptopolitikk; utnyttelse av kryptoteknologi til beskyttelse av informasjon blant annet for å ivareta nasjonale sikkerhetsinteresser og sikker bruk av digitale løsninger i offentlig og privat sektor. Bedre informasjonssikkerhet er en fordel, forutsatt at formålet er å verne lovlig aktivitet.

Innhenting av elektronisk lagret informasjon fra ulike kilder er sentralt for politiets kriminalitetsbekjempelse, herunder i forbindelse med etterforskning, forebygging og operative tiltak. Kildenes bruk av kryptert lagring og/eller kryptert kommunikasjon forhindrer politiets lovlige tilgang til den aktuelle informasjonen. Politiet har over lengre tid sett en normalisering og økning i bruken av krypteringsløsninger i samfunnet generelt, også blant kriminelle. Denne utviklingen ble påpekt allerede av Metodekontrollutvalget[1], og er senere lagt til grunn for vedtakelsen av straffeprosessloven § 216 o (dataavlesning)[2].

[1] NOU 2004:6 side 207
[2] Jf. Prop. 68L (2015-2016) side 259-261

Kripos/

Post: Pb. 2094 Vika, 0125 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.politi.no/kripos

Telefon: (+47) 23 20 80 00
Telefaks: (+47) 23 20 88 80
E-post: kripos@politiet.no

Org. nr: 974 760 827

Straffeprosessloven § 216 o gir politiet hjemmel for avlesning av informasjon i et datasystem, der politiet også gis adgang til, om nødvendig, å bryte eller omgå beskyttelse, for eksempel kryptering, i datasystemet. Bestemmelsen stiller strenge krav til hvilke straffbare handlinger som kvalifiserer for bruk av metoden. Norsk politi er fortsatt i startgropen hva gjelder anvendelse av metoden. Kripos arbeider kontinuerlig med utvikling av verktøy til gjennomføring av metoden, og har så langt selv utviklet enkelte fungerende verktøy. Vi erfarer at dette arbeidet er meget ressurskrevende, både hva gjelder kompetanse og kostnader, og etterspør en større satsning på området. I den forbindelse er det interessant å merke seg Regjeringens satsning på samarbeid mellom Forsvaret og norsk kryptoindustri. En tilsvarende satsning på samarbeid mellom norsk politi og kryptoindustri for å utvikle verktøy til bruk i kriminalitetsbekjempelsen bør også vurderes.

Utover dataavlesning, og eventuelt frivillig overlevering, kan politiet oppnå tilgang til kryptert informasjon ved bruk av tiltak som (åpen eller skjult) ransaking og utleveringspålegg, jf. straffeprosessloven kapittel 15 og §§ 210a flg. Ved bruk av "elektronisk" ransaking har politiet også hjemmel til å bryte eller omgå beskyttelse, herunder kryptering, jf. strpl. § 200 annet ledd 3. punkt. For øvrig er politiet avhengig av at den som har rådigheten over aktuelle krypterte opplysninger kan- og er villig til å dekryptere informasjonen og overlate denne til politiet, alternativt overlate kryptert informasjon og krypteringsnøkkel til politiet.

Personer som mistenkes for straffbare handlinger er gjennomgående lite interessert i å bidra med informasjon. Også en mistenkt kan pålegges å gi tilgangsopplysninger etter strpl. § 199a, dog begrenses opplysningsplikten av selvinkrimineringsvernet. Når det gjelder tredjeparter som måtte ha rådighet over krypterte opplysninger som politiet ønsker tilgang til, opplever Kripos varierende grad av samarbeidsvilje og evne. Dette gjelder typisk tilbydere av krypterte lagrings- og kommunikasjonstjenester mv. Noen tjenestetilbydere vegrer seg mot samarbeid med politiet, primært fordi et slikt samarbeid kan komme i konflikt med tjenestetilbydernes kommersielle interesser. Beskyttelse av informasjonen er for enkelte kundegrupper, herunder kriminelle, selve salgsvaren. I forlengelsen av dette erfarer Kripos også at enkelte tjenestetilbydere velger teknologiske løsninger som innebærer at den etterspurte informasjonen også er utilgjengelig for tjenestetilbyder, og således under enhver omstendighet ikke kan utleveres politiet, med mindre informasjonen tilgjengeliggjøres via kunden.

Det bemerkes at etter at straffeloven (1902) § 339 ikke ble videreført i ny straffelov, ble straffeprosessloven § 199a annet ledd opphevet[3]. Følgelig kan heller ikke tredjeparter straffes for brudd på opplysningsplikten etter § 199a. Departementet vurderte at det ikke lenger er behov for å ramme slike handlinger med straff[4], og viste til Delutredning VII til ny straffelov[5], hvor det fremgår at:

---

[3] Jf. Prop 64L (2014-2015) pkt. 12.5
[4] Jf. ot.prp. nr. 8 (2007-2008) pkt. 9.16
[5] NOU2002:4 side 416-417

"Bestemmelsen antas i dag å ha liten praktisk betydning. Årsaken til dette er at opplysningsplikt etter særlovgivningen – som er meget utbredt – som regel rammes av egne straffetrusler i de ulike særlovene….

Kommisjonen er av den mening at det i utgangspunktet er god grunn til å ha straffetrusler bak pålegg om opplysningsplikter til det offentlige. På den annen side er dette neppe nødvendig i alle sammenhenger….

Når strl § 339 nr 1 foreslås sløyfet i straffeloven, kan det føre til at man i noen tilfeller blir stående uten mulighet for straffereaksjon… Utkastet til ny straffelov forutsetter at det foretas en bred gjennomgåelse av særlovgivningen, også i forhold til kriminaliseringsspørsmål…I den sammenheng bør også behovet for straffetrusler tilsvarende strl § 339 nr 1 tas opp til drøftelse."

På bakgrunn av ovennevnte bør det gjøres en ny vurdering av behovet for en straffetrussel for brudd på opplysningsplikten etter straffeprosessloven § 199a.

Med hilsen

Vigleik Antun
ass. sjef Kripos

Saksbehandler:
Stein Damman