



POLITIET
OSLO POLITIDISTRIKT

Politidirektoratet
Postboks 8051 Dep
0031 OSLO

OSLO POLICE DISTRICT

Deres referanse:
201604978

Vår referanse:
201610210-3 008

Sted, Dato
Oslo, 26.01.2017

HØRINGSVAR - BRUK AV TVANG OVERFOR MISTENKTE ELLER TREDJEMANN FOR Å FÅ TILGANG TIL INNHOLD I DATASYSTEM VED BRUK AV BIOMETRISK AUTENTISERING

Det vises til oversendelse av 28. desember 2016 fra Politidirektoratet av Justisdepartementets høringsnotat vedrørende bruk av tvang for å skaffe politiet adgang til datasystemer. Det foreslås at politiet skal få hjemmel for slik tvangsbruk ved en endring i strprl. § 199a. Bakgrunnen for forslaget er at Høyesterett i kjennelse høsten 2016 konkluderte med at politiet ikke hadde hjemmel for denne typen tvangsbruk i nåværende straffeprosesslov. Politiet er gitt frist til 27. januar 2017 med å avgi uttalelse.

Det er vist til at politiet har behov for en slik hjemmel, idet biometrisk autentisering blir stadig mer utbredt, for å låse opp/skaffe tilgang til mobiltelefoner, nettbrett osv, og også adgangskontroll. Det er også pekt på at i forslaget til ny straffeprosesslov er hjemmel for tvang for innhenting inntatt. Dette forslaget er imidlertid mer omfattende enn det departementet finner grunn til å foreslå nå, inntil ny straffeprosesslov er ferdig behandlet og ikraftsatt.

Oslo politidistrikt støtter forslaget til positiv lovhjemmel, og mener det er nødvendig med en lovendring i forkant av at utkast til ny straffeprosesslov skal behandles. Uten en slik lovendring er det fare for at politiet ikke får tilgang til viktig bevismateriale i straffesaker.

Vi er enig med departementet i at dette vil være et beskjedent tvangsinngrep sammenliknet med andre tvangsinngrep som politiet i dag har adgang til å gjennomføre. Kravet til forholdsmessighet, samt en vurdering om inngrepet er nødvendig og forsvarlig må i hvert tilfelle vurderes.

I juni 2016, det vil si før Høyesterett avgjorde at straffeprosessloven § 157 ikke hjemler slik tvang, besluttet Oslo politidistrikt å åpne en telefon med tvang ved å bruke siktedes fingeravtrykk som "nøkkel". Dette ble gjort i en sak der siktelsen gjaldt seksuelle overgrep mot mindreårige. Det ble funnet overgrepsmateriale på siktedes lagringsmedier. Undersøkelsene ble midlertidig stanset fordi siktede begjærte beslaget opphevet. Undersøkelsene er foreløpig ikke gjenopptatt fordi spørsmålet så langt ikke er endelig avgjort i rettsapparatet. Denne saken illustrerer hvor viktig det er å få tilgang til lagringsenheter som politiet har lovlig adgang til å ransake.

Oslo politidistrikt

91 Strategisk Stab
Post: Postboks 8101 Dep, 0032 OSLO
Besøk: Grønlandsleiret 44, 0190 OSLO

Tlf: 22 66 90 50
Faks: 22 66 87 01
E-post:

Org. nr.: 961398142
Giro: 7694.05.08319
www.politi.no

Erfaringen vår fra seriesaker der ungdom er fornærmet, er at ungdommene i liten grad selv oppsøker politiet. I all hovedsak blir de fornærmede identifisert gjennom analyser av chattellogger, bilder eller annet bevismateriale. Når de så blir innkalt til avhør, er forklaringene ofte så upresise at om vi ikke hadde hatt chattellogger eller bilder, ville en del alvorlige straffbare forhold ikke vært avdekket.

I nettovergrepssaker kan chattellogger og bilder for eksempel være avgjørende for om det kan tas ut tiltale for voldtekt. I slike saker vil gjerningspersonen ofte starte med å forlede fornærmede til å sende nakenbilder av seg selv. Deretter blir disse bildene brukt til å presse fornærmede til å utføre seksuelle handlinger på webkamera. Hvis fornærmede blir truet eller presset til å utføre handlinger med seg selv som tilsvarer seksuell omgang, så er dette å regne som voldtekt. I chattellogger og i bildemateriale kommer dette ofte tydeligere fram enn i fornærmedes forklaring i ettertid. Mange fornærmede kan ha kommunisert med flere personer og kan derfor ha problemer med å huske detaljer fra kommunikasjonen som politiet ønsker belyst. Det skal også understrekes at politiets eneste reelle mulighet til å avdekke innhold fra kommunikasjon via nettjenester er å sikre det fra en databærer. Tjenesteleverandørene (Skype, Facebook, Instagram osv.) leverer som regel ikke innholdsdata, og hvis de gjør det, så tar det minst ett år før politiet får tilgang til materialet. Dette vil være svært skadelig for etterforskningen og saksfremdriften, men også for fornærmede i sakene i forhold til evt. iverksetting av nødvendige andre tiltak.

Uten mulighet for biometrisk autentisering vil det kunne oppstå situasjoner hvor det er nødvendig å be om/benytte varetektsfengsling, benytte andre tvangsmidler, også kanskje rettet mot flere, fram til tilgang er skaffet på andre måter. Dette kan være metoder som er vesentlig mer tid- og ressurskrevende, og uten noen sikkerhet for at dette vil føre fram. Dette gjelder både etterforskning av alvorlig sedelighetskriminalitet og annen alvorlig kriminalitet.

Etter straffeprosessloven § 199a har politiet anledning til å pålegge enhver å gi opplysninger som gir tilgang til datasystemer som skal ransakes. Dette er et lite effektivt virkemiddel overfor en siktet, fordi den siktede helt uten sanksjoner kan nekte å etterkomme et slikt pålegg.

Overtredelse av strpl. § 199a var for andre enn siktede straffsanksjonert etter strl 1902 § 339 nr 1, jf Ot.prp. nr. 40 (2004-2005) pkt 7.2. Dette ble ikke videreført i ny straffelov, på grunnlag av departementets forslag og at ingen høringsinstanser kommenterte dette. Det vises til Prop. 64 L (2014-2015) jf. pkt 6.7.3.1 og pkt 6.7.3.2, som viser videre til høringsnotatet (ift straffeloven 2005) og Ot.prp. nr. 8 (2007-2008) pkt 9.16;

"Forslaget om ikke å videreføre § 338 om straff for den som inngår ekteskap mv. når vilkårene er tilsidesatt, begrunnes med at det ikke lenger er behov for å ramme slike handlinger med straff med mindre handlingen er så alvorlig at den også rammes av andre og strengere straffebud, jf. Delutredning VII side 416. Det samme gjelder forslaget om ikke å videreføre straffeloven § 339 nr. 1 som setter straff for den som ikke oppfyller en lovbestemt plikt om å gi opplysninger til en offentlig myndighet.

Det synes som om en ikke kunne identifisere situasjoner der slik straffsanksjonering kunne ha betydning. Sett hen til at en nå vil innføre adgang til bruke tvang ift biometriske autentisering, bør det eventuelt vurderes å gjeninnføre det som tidligere var nedfelt i strl 1902 § 339 nr 1.

Oslo politidistrikt antar at det er hensiktsmessig å plassere en tvangshjemmel som et nytt ledd i samme paragraf som hjemler pålegg. Vi er enig i forslaget om å endre bestemmelsen om

pålegg til også å omfatte biometrisk autentisering.

Vi er også enig i at bestemmelsen må være teknologinøytral. Den bør omfatte flere former for biometrisk autentisering enn fingeravtrykk, også fremtidige. Den må også gjelde alle typer datasystemer eller dataenheter og også applikasjoner, låste filer, virtuelle lagre/containere, tjenestetilgang (eks. virtuelt datalager i skyen/cloud), også her fremtidige datasystemer som bærere av informasjon.

Oslo politidistrikt er videre enig i at det ikke er noen motstrid mellom vern mot selvinkriminering og spørsmålet om å underkaste seg en biometrisk autentisering. Vi ønsker allikevel å knytte en kommentar til merknadene om at forslaget gjelder spørsmål om å utnytte et kjennetegn som utgår fra kroppen, og ikke stiller den mistenkte overfor valg om å lyve. Dette er en sannhet med modifikasjoner, fordi det forutsetter at politiet faktisk kjenner kjennetegnet og ikke trenger medvirkning. Et konkret eksempel her er at den mistenkte kan opplyse at kjennetegnet er høyre tommel, men kjennetegnet faktisk er venstre pekefinger. Dagens låsemekanismer kan stilles inn slik at dersom man forsøker med falsk/feil biometrisk autentisering tre ganger, slettes alle data på enheten – enheten igangsetter en egensletting og tilbakestilling.

Oslo politidistrikt er enig i at man ikke bør kunne tvinge noen til å snakke slik at et datasystem kan gjenkjenne vedkommendes stemme. Vi mener likevel at stemmegjenkjenning bør kunne brukes, så fremt vedkommende som skal gi politiet tilgang ikke blir *tvunget* til å snakke. I noen tilfeller vil man for eksempel allerede ha et lydopptak av at vedkommende snakker. Mange politiavhør tas opp på lyd og bilde. I den grad opptaket teknisk sett kan brukes som biometrisk autentisering, bør det også være rettslig adgang til å bruke det.

På grunn av uklare grenser mellom hva som er gransking av beslag og hva som er ransaking av et datasystem, er Oslo politidistrikt enig med departementet i at det bør tas inn en henvisning til straffeprosessloven § 199a i kapittelet om beslag.

I mange tilfeller bør de innledende dataundersøkelsene gjøres på stedet før strømmtilførselen kuttes og lagringsenhetene bringes til politiets lokaler. Det er derfor viktig at politiet får muligheten til å åpne enhetene ute på stedet der de befinner seg. Oslo politidistrikt mener imidlertid at primærkompetansen til å beslutte tvangsmessig åpning i utgangspunktet bør ligge hos påtalemyndigheten. Det er påtalemyndigheten som har primær- eller hastekompetanse for de fleste tvangsmidlene. Det er vanskelig å se at det er behov for å gjøre unntak på dette området.

Der ransaking skjer etter beslutning fra retten eller påtalemyndighet, vil objekt(er) for ransaking være angitt i beslutningen. Dagens BL-mal omfatter bla edb, slik at en utvidelse slik det foreslås enkelt kan implementeres. Samtidig vil dette sikre den nødvendige klarhet ovenfor den som pålegges å medvirke.

Samtidig er det ikke tvil om at behovet for å pålegge tvang er avhengig av at behovet er identifisert, samt at det er praktisk mulig å gjennomføre tvang. Først under en ransaking vil behovet avdekkes når datasystemet identifiseres. Dersom personen som har mulighet til å gi adgang ved biometriske data kan identifiseres og er til stede, synes dette å være en beslutning som kan tillegges politimyndigheten som er tilstede. Dette forutsetter dog at det er praktisk mulig å gjennomføre innhenting ved tvang. Det bør i den sammenheng kreves at beslaglagt objekt, som tvangen knyttes til, konkretiseres, jf strpl § 206 første ledd. Den som tar beslutningen, må sørge for at pålegget nedtegnes, jf f.eks strpl § 197 tredje ledd if.

Tilsvarende hva gjelder ransaking i straffeprosessloven § 198 må polititjenesteperson kunne gjennomføre tvangsmiddelet når mistenkte treffes eller forfølges på fersk gjerning eller ferske spor, eller når det er fare for at tilgangen ikke oppnås uten umiddelbar bruk av biometrisk autentisering.

Det vil ikke være hensiktsmessig å legge primærkompetansen til domstolen. Det vil som beskrevet forsinke og hemme politiets arbeid å måtte avvente domstolens avgjørelse. Hasteelementet vil som regel være framtreddende fordi man står midt i en ransaking, eller fordi det vil være fare for at muligheten til å bruke biometrisk autentisering forsvinner hvis det går for lang tid.

Som beskrevet i høringsnotatet er det når det gjelder data, i juridisk teori med holdepunkter i rettspraksis, lagt til grunn at videre undersøkelser av data for å avdekke relevant informasjon kan skyves ut som fortsatt ransaking av beslaglagte datasystemer, til relevant informasjon er avdekket. Her ønsker vi igjen å presisere at låsefunksjoner ved bruk av biometrisk autentisering ikke nødvendigvis begrenser seg til den fysiske enheten og låsefunksjonen der, men at det like fullt kan være biometrisk autentisering for eksempelvis applikasjoner, filer, virtuelle lagre/containere mv. som kan inneholde like relevant informasjon. Vi er enige i at muligheten for å anvende makt for å få åpnet datasystem ved bruk av biometrisk autentisering også må gjelde den fortsatte ransaking av innholdet i beslaglagt datasystem.

Oslo politidistrikt mener at tvangshjemmelen må gjelde generelt overfor "enhver" som har mulighet til å gi tilgang til et datasystem/dataenhet. Dette vil for eksempel kunne medføre at en som er ansatt for å drifte et IT-system kan tvinges til å gi politiet tilgang til systemet når ransakingen gjennomføres hos vedkommendes arbeidsgiver. Den siste delen av forslaget til ny ordlyd i straffeloven § 199 a, hvor det begrenses til "*andre enn mistenkte dersom ransaking foretas i deres datasystem*" mener vi må utvides til å gjelde enhver.

Videre angående forslag til ordlyd i § 199a første ledd foreslås "*eller å åpne det ved bruk av*" uten at det i høringsnotatet vises hvordan er kommet frem til den konkrete formuleringen. Ved bruk av "*eller*" fremstår det som om "å gi ... opplysninger" og "å åpne" er likeverdige alternativer. Dette synes naturlig sett hen til at bare "å åpne" er handling som skal kunne gjennomføres uavhengig av vilje.

Såtidig synes "å gi adgang til datasystem ved biometrisk autentisering" å være en måte for å få tilgang til datasystem. I dette perspektiv synes "herunder å åpne det ved bruk av biometrisk autentisering" å være mer treffende.

Med vennlig hilsen



Sveinung Sponheim
visepolitimester

Saksbehandler:
Cecilie Gulnes/ Trond Austad
/RB