

Høringsnotat

Lovavdelingen
Desember 2016
Snr. 16/7883

Høring – bruk av tvang overfor mistenkte eller tredjemann for å få tilgang til innhold i datasystem ved bruk av biometrisk autentisering

1 Innledning

Justis- og beredskapsdepartementet sender med dette på høring forslag til endringer i straffeprosessloven.

Forslaget har sin bakgrunn i en kjennelse fra Høyesterett 30. august 2016 (HR-2016-1833-A), hvor det fremgår at straffeprosessloven § 157 om kroppslig undersøkelse ikke gir hjemmel til bruk av tvang overfor mistenkte for å få tilgang til innholdet på mistenktes mobiltelefon ved bruk av fingeravtrykksautentisering.

2 Bakgrunn

Departementet ønsker å legge til rette for at politiet har de nødvendige virkemidlene til effektivt å kunne etterforske straffbare handlinger. Som følge av den teknologiske utviklingen oppstår det fra tid til annen spørsmål om politiets adgang til å utnytte slik teknologi som ledd i etterforskningen. Biometrisk autentisering, for eksempel ved bruk av fingeravtrykk og iris- eller stemmegjenkjenning, blir stadig mer utbredt som adgangsnøkkel til datasystem. Dette gjelder kanskje særlig mobiltelefoner, men også andre datasystemer som nettbrett og datamaskiner.

Biometrisk autentisering bruker biometriske kjennetegn. Dette er kjennetegn som utgår fra kroppen, som er unike for hver enkelt og samtidig permanente eller stabile over tid. Ved å måle disse kjennetegnene kan de benyttes til å gjenkjenne en person eller bekrefte en persons påståtte identitet.

Biometrisk autentisering som adgangsnøkkel gir politiet særlige utfordringer ved ransaking av et datasystem, der politiet forsøker å få tilgang til systemet og mistenkte ikke vil medvirke. Et særlig spørsmål er om politiet i slike tilfeller kan benytte tvang overfor mistenkte for å åpne systemet.

Spørsmålet kom på spissen i kjennelsen vist til ovenfor (HR-2016-1833-A) og som ligger til grunn for forslaget. Saken gjaldt konkret om politiet har hjemmel i straffeprosessloven § 157 til ved tvang å bruke mistenktes finger til å få tilgang til innhold på hans mobiletelefon. Dette besvarte et enstemmig Høyesterett benektende. Avgjørelsen er fulgt opp i senere høyesterettspraksis, jf. HR-2016-2006-U.

3 Gjeldende rett

3.1 Straffeprosessloven

Myndighetens bruk av tvang overfor den enkelte krever hjemmel i lov, jf. Grunnloven § 102 og § 113 og Den europeiske menneskerettskonvensjon (EMK) artikkel 8. Når det dreier seg om straffeprosessuelle tvangsmidler, må det i tillegg kreves at hjemmelen er nokså klart og presist utformet, jf. for eksempel Rt. 2014 side 1105.

Straffeprosessloven § 157 gir politiet adgang til å foreta «kroppslig undersøkelse» av person som med skjellig grunn mistenkes for en handling som etter loven kan medføre frihetsstraff. Bestemmelsen står i kapitlet om *gransking*.

Ordlyden i § 157 tilsier at det kan foretas undersøkelser av kroppen, med siktemål å bruke kroppen eller det som måtte befinne seg i den som reelt bevismiddel, men ikke undersøkelser av andre objekter med bruk av kroppen. En slik forståelse er naturlig også sett hen til plasseringen av bestemmelsen i granskingskapitlet. Bestemmelsen kan ikke tolkes utvidende til å omfatte bruk av tvang for å åpne en mobiltelefon med mistenktes fingeravtrykk jf. HR-2016-1833-A og HR-2016-2006-U. Det må legges til grunn at Høyesteretts vurdering av straffeprosessloven § 157 vil ha overføringsverdi til andre typer biometrisk autentisering på andre type datasystemer.

I de nevnte kjennelsene fra Høyesterett hadde lagmannsretten bygd sin avgjørelse på en tolkning av straffeprosessloven § 157, og det falt utenfor Høyesteretts kompetanse å ta stilling til om inngrepet hadde hjemmel i andre bestemmelser.

Straffeprosessloven kapittel 15 gir politiet adgang til å *ransake* datasystem dersom de grunnleggende vilkår for tvangsmiddelbruk er oppfylt, herunder kravet om skjellig grunn til mistanke og forholdsmessighet. Ransaking er i utgangspunktet en kortvarig aksjon som avsluttes når ransakingsobjektet er gjennom søkt.

Som følge av tekniske løsninger som begrenser tilgangen til systemet, har politiet behov for bistand for å kunne gjennomføre ransakingen. Ved ransaking av datasystemer kan politiet etter straffeprosessloven § 199 a pålegge enhver som har befatning med datasystemet å gi nødvendige opplysninger for å få tilgang til systemet. Bestemmelsen omfatter etter sin ordlyd også mistenkte, jf. «enhver», selv om det er mest nærliggende å rette pålegget mot IT-personell/systemoperatører. Bestemmelsen åpner imidlertid ikke for bruk av tvang.

Et datasystem hvis innhold antas å ha betydning som bevis, kan bli gjenstand for *beslag* etter straffeprosessloven § 203. Departementet legger til grunn at skjellig grunn til mistanke om et straffbart forhold er et vilkår for beslag etter bestemmelsen, selv om dette ikke er kommet direkte til uttrykk i lovteksten, jf. Bjerke m.fl, kommentarutgave til straffeprosessloven, fjerde utgave side 713 med videre henvisninger. Beslag er nært knyttet til ransaking og retter seg mot ting man finner under en slik aksjon. Alt etter det konkrete etterforskningsformålet og de konkrete omstendighetene kan det variere hvor ransakingen stopper og avløses av et beslag i bevis med sikte på gransking. Straffeprosessloven § 199 a som

omhandler «ransaking» av datasystem, er i så måte illustrerende. Undersøkelsen som denne bestemmelsen viser til, kunne like gjerne vært å anse som gransking.

Når det gjelder data, er det i juridisk teori anført at rettspraksis legger til grunn at ransaking kan pågå over en lengre periode, og at beslutningen om beslag skytes ut til man har avdekket relevant informasjon. Det vises til Inger Marie Sunde, Straffeprosessuelle metoder rettet mot elektroniske bevis, Rettssikker radikaler: Festschrift til Ståle Eskeland 2013 s. 266-283 - (FEST-2013-se-266) med videre henvisninger til rettspraksis. Avgjørelsene det særlig vises til i artikkelen, gjaldt speilkopier av data.

Slik departementet ser det, vil spørsmålet om tvang for å få åpnet et datasystem være særlig aktuelt i forbindelse med ransaking av datasystem. Men et datasystem som er funnet under en ransaking, kan også tas i beslag etter reglene i straffeprosessloven kapittel 16. I den nevnte kjennelsen fra Høyesterett (HR-2016-1833-A) og som ligger til grunn for forslaget her, hadde politiet etter ransaking tatt mobiltelefonen i beslag. Det er heller ingen bestemmelse i straffeprosesslovens kapittel 16 om beslag som uttrykkelig gir politet adgang til å anvende tvang for å få åpnet et datasystem.

Politielloven § 6 gir politiet hjemmel til å anvende makt ved iverksettelse og gjennomføring av straffeprosessuelle tvangsmidler, der det er nødvendig og forsvarlig. Bestemmelsen gir ikke politiet en selvstendig hjemmel for bruk av makt. Det er en forutsetning at den bestemmelse som hjemler selve beslutningen eller pålegget som politiet skal gjennomføre, direkte eller indirekte forutsetter at det kan gjennomføres ved bruk av fysisk makt. I den sammenheng kan det reises spørsmål om tvangsgjennomføring av biometrisk autentisering ved ransaking for å få åpnet mistenktes datasystem, kan anses omfattet av politiets rett og plikt til å benytte seg av makt ved utøvelsen av politiets tjenestemessige oppgaver. Dette er ikke helt ulikt situasjonen der politiet må tvangsflytte mistenkte som sperrer for inngangsdøren til et hus som skal ransakes. I begge tilfeller er det tale om å overkomme en faktisk hindring for å skaffe tilgang til informasjon som i prinsippet er rettslig tilgjengelig. Fremtvingelsen av identifikasjonshandlingen for å få gjennomført ransakingen må da anses som et aksessorium til det opprinnelige tvangsmidlet. Det er imidlertid usikkert hvor langt dette synspunktet rekker. Det er blant annet den forskjell at man ved å bruke makt ved biometrisk autentisering, tvangsmessig gjør bruk av mistenktes personopplysninger.

3.2 Nærmere om forholdet til Den europeiske menneskerettighetskonvensjonen (EMK)

Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8 oppstiller et forbud for staten mot inngrep i privatlivet. Det kan gjøres unntak fra forbudet dersom tre vilkår er oppfylt. Inngrepet må ha hjemmel i lov, fremme ett av de uttømmende legitime formål i bestemmelsen og være nødvendig i et demokratisk samfunn.

Departementet kan ikke se at en lovbestemmelse som gjør det klart at politet gis adgang til ved tvang å få tilgang til datasystem ved biometrisk autentisering, vil være i strid med EMK artikkel 8. Inngrepet vil være begrunnet i hensynet til

etterforskning og oppklaring av kriminalitet, et formål som er legitimt etter konvensjonen.

EMK artikkel 8 oppstiller i tillegg et krav om at inngrepet er nødvendig og forholdsmessig. De samfunnshensyn som ligger bak forslaget om bruk av mistenktes finger ved tvang for å få tilgang til innhold på mobiltelefon, må stå i et rimelig forhold til interessen til den som blir utsatt for inngrepet.

Departementet anser et forslag som gjør det klart at politiet ved ransaking og eventuelt beslag av en mobiltelefon kan bruke mistenktes finger ved tvang for å få tilgang til innhold på mistenktes mobiltelefon, å ligge innenfor forholdsmessighetskravet. Tilsvarende vil normalt også gjelde ved fremtvingelse av andre identifikasjonshandlinger for å få åpnet et datasystem. Det vil være snakk om en relativt beskjedne og kortvarig maktanvendelse og et langt mindre belastende inngrep enn det politiet i dag har hjemmel til, for eksempel undersøkelse av kroppens hulrom etter straffeprosessloven § 157. Informasjon som ligger lagret på en mobiltelefon eller andre datasystemer vil ofte være viktig for å oppklare kriminalitet, særlig i mer alvorlige saker som organisert narkotikakriminalitet og annen gjengrelatert kriminalitet, men også i mindre alvorlige saker.

Etter departementets syn er forslaget heller ikke i strid med selvinkrimineringsvernet som er innfortolket i EMK artikkel 6 nr. 1 og som følger av Den internasjonale konvensjon om sivile og politiske rettigheter (SP) artikkel 14 nr. 3 bokstav g. Dette vernet retter seg først og fremst mot å fremtvinge selvinkriminerende forklaringer fra mistenkte og mot å bruke slike forklaringer som bevis i straffesak mot ham. Det er ingen analogi mellom spørsmålet om forklaringsplikt og spørsmålet om å underkaste seg en biometrisk autentisering. Forslaget her gjelder tilfeller der det er spørsmål om å utnytte et kjennetegn som utgår fra kroppen og stiller ikke mistenkte overfor et valg om å lyve eller angi seg selv. Kjennetegnet eksisterer uavhengig av mistenktes vilje.

Avhengig av tvangens karakter og grad kan forbudet etter omstendighetene også ramme fremtvingelse eller bruk av fremtvungne selvinkriminerende dokumentbevis eller andre former for realbevis, men terskelen for at fremtvingelse eller bruk av slike bevis skal rammes, er relativt høy. Tvangen må være umenneskelig eller på annen måte ha karakter av overgrep mot mistenkte, jf. Rt. 2011 side 487 avsnitt 35 med videre henvisninger og Rt. 2011 side 800. Tvangen som forslaget her legger til rette for, vil normalt være beskjedne og kortvarig og etter departementets syn vanskelig kunne karakteriseres som umenneskelig eller på annen måte utgjøre et overgrep mot mistenkte.

3.3 Rettstilstanden i andre nordiske land

Så langt departementet kjenner til, har ingen av de øvrige nordiske land bestemmelser i sin straffeprosesslovgivning som uttrykkelig gir politiet adgang til ved tvang å få tilgang mistenktes datasystem ved hjelp av biometrisk autentisering.

4 Forslaget i NOU 2016: 24 Ny straffeprosesslov

Straffeprosessutvalget, som avga sin utredning 3. november 2016, har som følge av Høyesteretts kjennelse 30. august 2016 drøftet spørsmålet om tvangshjemmel for biometrisk autentisering, jf. NOU 2016: 24 punkt 14.3.6 side 315. Et samlet utvalg går inn for at det i ny straffeprosesslov bør åpnes for å benytte tvang for å gjennomføre biometrisk autentisering, ikke bare overfor mistenkte, men overfor enhver, jf. utkastet til § 14-6 annet ledd. Bestemmelsen åpner også for bruk av biometrisk autentisering som selvstendig tvangstiltak. Bestemmelsen er inntatt i lovutkastet kapittel 14, om tvangstiltak – grunnvilkår og fellesregler, og lyder:

Enhver kan pålegges å medvirke til biometrisk autentisering, ved bruk av fingeravtrykk eller andre biologiske kjennetegn, for å sikre tilgang til sted eller datasystem når det er nødvendig for å gjennomføre et tvangstiltak, eller for å verifisere at vedkommende har tilgang til stedet eller datasystemet. Motsetter vedkommende seg autentiseringen, kan den gjennomføres med tvang.

Bestemmelsen er inntatt sammen med en hjemmel for påtalemyndigheten til å pålegge enhver med vitneplikt til å medvirke til gjennomføring av tvangstiltak.

Straffeprosessutvalgets utredning ble sendt på høring 5. desember 2016 med høringsfrist 6. juni 2017. Departementets oppfølging av utredningen vil nødvendigvis ta tid. Departementet mener det haster med å få på plass en klar hjemmel som gir politet adgang til å benytte tvang i forbindelse med biometrisk autentisering, og sender derfor på høring et forslag om endring i gjeldende straffeprosesslov. Utvalgets mer omfattende forslag, herunder spørsmålet om bruk av biometrisk autentisering som selvstendig tvangstiltak, vil bli grundig vurdert i forbindelse med høringen av NOU 2016: 24.

5 Departementets foreløpige vurdering

Etter departementets syn er det viktig at politiet har nødvendige hjelpemidler tilgjengelig for å oppklare kriminalitet. Politiet har etter gjeldende rett adgang til å ransake og beslaglegge datasystem, dersom det foreligger skjellig grunn til mistanke om et straffbart forhold som etter loven kan medføre frihetsstraff. Gjennomføringen av ransakingen, eventuelt beslaget, blir imidlertid vanskelig når systemet er adgangsbeskyttet, og politiet ikke får hjelp til å komme seg inn i systemet.

Departementet anser det tvilsomt om politiloven § 6 gir politiet tilstrekkelig hjemmel til å anvende tvang i disse tilfellene. Forslaget som departementet nå sender på høring, vil gi politiet en klar hjemmel til enklere tilgang til datasystemer som åpnes ved biometrisk autentisering.

Departementet foreslår at bestemmelsen gjøres teknologinøytral, jf. «datasystem». Den bør ikke bare omfatte fingeravtrykksavlesning, men også andre typer biometrisk autentisering, som irisgjenkjenning, netthinne-gjenkjenning og kanskje i fremtiden, DNA-gjenkjenning. Bestemmelsen bør heller ikke begrenses til mobiltelefoner. Også andre datasystemer bør omfattes, som datamaskiner, nettbrett mv.

For enkelte typer av biometrisk autentisering kan imidlertid tvang være vanskelig å gjennomføre eller komme i strid med selvinkrimineringsvernet. For eksempel vil mistenktes rett til taushet stå i veien for å gjennomføre stemmegjenkjenning. Selvinkrimineringsvernet vil naturlig oppstille en skranke for fremtidige autentiseringsformer man i dag ikke har oversikt over, og hvor en fremtvingelse av identifiseringen vil representere et overgrep mot mistenkte. Dette må vurderes selvstendig i hvert enkelt tilfelle.

Det kan heller ikke utelukkes nye metoder for biometrisk autentisering, der maktanvendelsen ikke står i rimelig forhold til interessen til den som blir utsatt for inngrepet. På den bakgrunn er det tatt inn en presisering i lovforslaget om at tvangsbruken må være nødvendig og forholdsmessig, noe som allerede følger av EMK og straffeprosessloven § 170 a.

Departementet mener bestemmelsen naturlig kan tas inn som et nytt annet ledd i straffeprosessloven § 199 a, som omhandler ransaking av datasystem. I tilknytning til dette er det naturlig å foreta en endring i det som blir bestemmelsens første ledd om at enhver som har befatning med datasystemet kan pålegges å gi opplysninger som gir tilgang til systemet. Dette omfatter etter ordlyden ikke biometrisk autentisering, som for eksempel fingeravtrykk, bare opplysning om kode, passord og liknende. Det foreslås derfor en presisering i første punktum om at enhver som har befatning med datasystemet plikter å bruke biometrisk autentisering for å gi politiet tilgang til systemet. Det kan for eksempel tenkes at en systemansvarlig kan åpne mistenktes datasystem med sitt fingeravtrykk. Da bør politiet kunne gi personen pålegg om å gjøre dette. Departementet er i tvil om det i disse tilfellene bør gis hjemmel for å gjennomføre autentiseringen med tvang.

Straffeprosessutvalget går i sitt forslag inn for at tvang kan benyttes overfor enhver som motsetter seg autentisering når det er nødvendig for å gjennomføre et tvangstiltak, men departementet er i tvil om tvangshjemmelen bør rekke så langt. Etter departementets syn bør det riktignok innenfor de rammer som følger av selvinkrimineringsvernet og kravet til forholdsmessighet, være adgang til om nødvendig å bruke tvang overfor andre enn mistenkte for å få tilgang til informasjon på et datasystem som er rettslig tilgjengelig gjennom reglene om ransaking og beslag. Til sammenlikning er det i dag adgang til å dekryptere eller bryte opp låser. På den annen side forutsetter tvangen i dette tilfellet en fysisk maktanvendelse for å gjøre bruk av personopplysninger. Det kan oppleves som mer integritetskrenkende enn en lås som dekrypteres eller brytes opp.

Departementet går i forslaget imidlertid inn for at politiet gis adgang til å bruke tvang overfor *andre enn mistenkte* når *deres* datasystem er gjenstand for ransaking. Straffeprosessloven kapittel 15 åpner – om enn i begrenset utstrekning – for ransaking av tredjemanns datasystem, jf. § 192 annet ledd. Selv om slik ransaking er mindre praktisk, er departementets foreløpige syn at det også i disse tilfellene kan være grunn til å åpne for bruk av tvang for å gi politiet tilgang til datasystemet.

Dersom mistenkte ikke er til stede under ransakingen, eller politiet ikke finner det hensiktsmessig å åpne datasystemet på stedet, vil politiet ta med seg datasystemet for å undersøke det senere. Som nevnt, er det holdepunkter i rettspraksis for at videre undersøkelser av data vil bli vurdert som ledd i en fortsatt ransaking. Men

spørsmålet om politiet bør ha adgang til å tvangsgjennomføre biometrisk autentisering, kan også reise seg for beslaglagte datasystemer. Det er ingen grunn til at politiet ikke skal gis samme adgang til å anvende makt for å få åpnet datasystemet ved granskning av beslaglagt datasystem, som ved ransaking av det.

Departementets foreløpige syn er at beslutningen om å anvende makt overfor mistenkte for å få åpnet datasystemet, kan treffes av politet på stedet, på samme måte som politet kan beslutte å fjerne mistenkte som sperrer for inngangsdøren ved en husransaking. Om kompetansen til å treffe beslutning om dette bør løftes opp et nivå, til påtalemyndigheten, er likevel et spørsmål som departementet særlig ber om høringsinstansenes syn på.

Departementet ber om høringsinstansenes syn på behovet for endringer i straffeprosesslovens regler i tråd med ovennevnte og på plassering og utforming av bestemmelsene.

Det bes særlig om høringsinstansenes syn på hvem som bør ha kompetanse til å treffe beslutning om bruk av tvang og om tvangshjemmelen bør gjelde generelt overfor «enhver» eller begrenses til mistenkte og tredjemann der ransaking foretas i hans datasystem.

Departementet legger avslutningsvis til at Straffeprosessutvalgets utkast til tvangshjemmel ved biometrisk autentisering for gjennomføring av tvangsmidler, omfatter også tilgang til «sted» og ikke kun datasystem. Bestemmelsen er i tillegg inntatt i et generelt kapittel som gjelder alle tvangsmidlene (der omtalt som tvangstiltak). Utvalgets forslag legger opp til en annen systematikk enn gjeldende lov. Departementet ser at det kan være gode grunner for utvalgets utforming og avgrensning av sitt forslag. For eksempel vil fingeravtrykksautentisering for å få åpnet en safe, et hus eller en bil være omfattet. En slik bredere og mer generell tvangshjemmel vil imidlertid bli vurdert etter at høringen av NOU 2016: 24 er avsluttet og i forbindelse med en ny straffeprosesslov, jf. punkt 4.

6 Administrative og økonomiske konsekvenser

Forslaget til lovendring vil ikke få nevneverdige administrative konsekvenser. Forslaget vil innebære at politiet kan etterforske mer effektivt, noe som må forventes å ha en viss kostnadsbesparende effekt.

7 Forslag til lovendringer

En regel som gir politiet adgang til å pålegge enhver som har tilgang til et datasystem å åpne det ved biometrisk autentisering og som åpner for bruk av tvang overfor mistenkte eller tredjemann som ransakingen skjer hos, kan tas inn i gjeldende straffeprosesslov § 199 a.

Paragraf 199 a kan da for eksempel lyde:

Ved ransaking av et datasystem kan politiet pålegge enhver som har befattning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet *eller å åpne det ved bruk av biometrisk autentisering.*

Overfor mistenkte kan et pålegg om å gi tilgang til datasystemet ved biometrisk autentisering skje ved bruk av tvang, dersom tvangsbruken er nødvendig og forholdsmessig. Det samme gjelder overfor andre enn mistenkte, dersom ransaking foretas i deres datasystem.

Det foreslås videre at det i kapitlet om beslag (straffeprosessloven kapittel 16) henvises til § 199 a så langt den passer.