

Prop. 106 L

(2016–2017)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i straffeprosessloven (biometrisk autentisering)

*Tilråding fra Justis- og beredskapsdepartementet 5. april 2017,
godkjent i statsråd samme dag.
(Regjeringen Solberg)*

1 Proposisjonens hovedinnhold

Departementet foreslår i denne proposisjonen endringer i straffeprosessloven § 199 a. Lovforslaget vil gi politiet adgang til å pålegge enhver som har befatning med et datasystem som er gjensstand for ransaking og beslag å åpne datasystemet ved biometrisk autentisering og, om nødvendig, å benytte tvang for å få gjennomført autentiseringen.

2 Bakgrunnen for lovforslaget

Høyesterett avsa en kjennelse 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.

Departementet ønsker å legge til rette for at politiet har de nødvendige virkemidlene til effektivt å kunne etterforske straffbare handlinger, samtidig som tilstrekkelig hensyn må tas til borgernes vern mot inngrep. Som følge av den teknologiske utviklingen oppstår det fra tid til annen spørsmål om politiets adgang til å utnytte slik teknologi i etterforskningen. Biometrisk autentisering, for eksempel ved bruk av fingeravtrykk og iris-

gjenkjenning, blir stadig mer utbredt som adgangsnøkkel til datasystem. Dette gjelder mobiltelefoner, men også andre datasystemer som nettbrett og datamaskiner.

Med bakgrunn i kjennelsen vist til ovenfor, sendte departementet 14. desember 2016 på høring et forslag til endringer i straffeprosessloven § 199 a. Formålet med forslaget var å gi en klar hjemmel for at politiet ved ransaking eller beslag av datasystem har adgang til på nærmere vilkår å bruke tvang overfor mistenkte eller tredjemann for å få tilgang til datasystemet ved biometrisk autentisering. Det ble også foreslått at politiet ved ransaking eller beslag av datasystem kan pålegge enhver å gi tilgang til systemet ved bruk av biometrisk autentisering.

Høringsnotatet ble sendt til følgende høringsinstanser:

Departementene

Høyesterett

Lagmannsrettene

Tingrettene

Domstoladministrasjonen

Riksadvokaten

Statsadvokatembetene

Generaladvokaten

ØKOKRIM

Den nasjonale enhet for bekjempelse av organisert kriminalitet (Kripos)

Politidirektoratet

Politiets sikkerhetstjeneste (PST)

Regjeringsadvokaten

Stortingets ombudsmann for forvaltningen (Sivilombudsmannen)

Stortingets kontrollutvalg for etterretnings-, overvåkings- og trygghetstjenester

Advokatforeningen

Amnesty International Norge

Datatilsynet

Den norske Dommerforening

Direktoratet for forvaltning og IKT (Difi)

Folkehelseinstituttet

Forsvarergruppen av 1977

Gatejuristen

Juridisk rådgivning for kvinner (JURK)

Jushjelpa i Midt-Norge

Juss-Buss

Jussformidlingen i Bergen

Jusshjelpa i Nord-Norge

Kontrollutvalget for kommunikasjonskontroll

Nasjonal kommunikasjonsmyndighet

Norges Juristforbund

Norges nasjonale institusjon for menneskerettigheter

Norsk forening for kriminalreform – KROM

Norsk Presseforbund

Politiets Fellesforbund

Politijuristene

Rettspolitisk forening

Statsadvokatenes forening

Stine Sofies Stiftelse

Det juridiske fakultet ved Universitetet i Oslo

Det juridiske fakultet ved Universitetet i Bergen

Det juridiske fakultet ved Universitetet i Tromsø

Institutt for kriminologi og rettssosiologi ved Universitetet i Oslo

Norsk senter for menneskerettigheter

PolitiHøgskolen

3 Tvangsgjennomføring av biometrisk autentisering

3.1 Gjeldende rett

Myndighetenes bruk av tvang overfor den enkelte krever hjemmel i lov etter legalitetsprinsippet, 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 kapittel 12 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. Høyesteretts kjennelser i 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 og andre typer 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 vilkårene 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, kan politiet ha behov for bistand for å kunne gjennomføre ransakingen. Ved ransaking av datasystemer kan politiet etter straffeprosessloven § 199 a pålegge enhver som har befattning 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 eller 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 mfl., Straffeprosessloven kommentarutgave (2011) 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 av beslaglagt datasystem.

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, Rettsikker radikaler: Festskrift til Ståle Eskeland 2013 side 266–283 med videre henvisninger til rettspraksis.

Spørsmålet om tvang for å få åpnet et datasystem vil særlig være 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 straffeprosessloven kapittel 16 om beslag som uttrykkelig gir politiet adgang til å anvende tvang for å få åpnet et datasystem.

Politiloven § 6 fjerde ledd 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 bestemmelsen 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 et datasystem, kan anses omfattet av politiets rett og plikt til å benytte makt ved utøvelsen av tjenestemessige oppgaver. Dette er ikke helt ulikt situasjonen der politiet må tvangsflytte den som sperer 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 Internasjonale forpliktelser

Den europeiske menneskerettskonvensjonen (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.

I vilkåret om at inngrepet må være nødvendig i et demokratisk samfunn ligger et krav om at inngrepet er nødvendig og forholdsmessig. For vurderingen her innebærer det at de samfunnshensyn som ligger bak forslaget om tvangsbruk ved biometrisk autentisering for å få tilgang til datasystem, må stå i et rimelig forhold til interessen til den som blir utsatt for inngrepet.

Selvinkrimineringsvernet er innfortolket i EMK artikkel 6 nr. 1 og følger av Den internasjonale konvensjon om sivile og politiske rettigheter (SP) artikkel 14 nr. 3 bokstav g. Den som er «siktet» i en straffesak, kan på ulike måter bli bedt om å bidra til sakens opplysning, for eksempel gjennom plikt til å svare på spørsmål, til å legge frem dokumenter eller gjenstander, eller plikt til å medvirke til ulike former for undersøkelser. Det er den selvinkrimineringen som skjer under ulike former for tvang mv., siktede er vernet mot. Selvinkrimineringsvernet setter ikke skranker for innhenting av bevis som den siktede frivillig overbringer til offentlige myndigheter. Også på andre måter er vernet begrenset.

EMD har sondret mellom bevis som knytter seg til den siktedes vilje og bevis som eksisterer uavhengig av viljen. Innhenting av bevis som eksisterer uavhengig av siktedes vilje, for eksempel blod, urin-, DNA-, eller utåndingsprøver, strider som den klare hovedregel ikke mot taushetsretten, jf. for eksempel Saunders mot Storbritannia, 17. desember 1996 (nr. 19187/91) avsnitt 69. Andre bestemmelser i EMK kan imidlertid tenkes å sette skranker for innhenting av bevis uten siktedes medvirkning, som EMK artikkel 3 og 8. Der som slike prøver eller andre bevis innhentes ved metoder som krenker EMK artikkel 3, kan det dessuten tenkes at også vernet mot selvinkriminering etter EMK artikkel 6 nr. 1 må anses krenket dersom opplysningene senere brukes som bevis i straffesaken.

3.3 Andre nordiske lands rett

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 til 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 Ny straffeprosesslov 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 overfor enhver for å sikre tilgang både til sted og datasystem, jf. utkastet til § 14-6 annet ledd. Bestemmelsen åpner også for bruk av biometrisk autentisering som selvstendig tvangstiltak, «for å verifisere at vedkommende har tilgang til stedet eller datasystemet». 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.»

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 politiet adgang til å benytte tvang i forbindelse med biometrisk autentisering, og foreslår derfor endringer i gjeldende straffeprosesslov i proposisjonen her. Utvalgets mer omfattende forslag, herunder spørsmålet om bruk av biometrisk autentisering som selvstendig tvangstiltak, vil bli grundig vurdert i forbindelse med oppfølgingen av NOU 2016: 24 Ny straffeprosesslov.

5 Forslaget i høringsnotatet 14. desember 2016

I høringsnotatet 14. desember 2016 foreslo departementet å gi politiet en hjemmel for bruk av tvang for å få tilgang til datasystemer som åpnes med biometrisk autentisering. Departementet foreslo en teknologinøytral bestemmelse, både med hensyn til datasystem og type biometrisk autentisering:

«Departementet foreslår at bestemmelsen gjøres teknologinøytral, jf. «datasystem». Den bør ikke bare omfatte fingeravtrykksavlesning, men også andre typer biometrisk autentisering, som irisgjenkjenning, netthinnegjenkjenning og kanskje i fremtiden, DNA-gjenkjenning.»

En bestemmelse om bruk av tvang til å gjennomføre biometrisk autentisering ble foreslått tatt inn som et nytt annet ledd i straffeprosessloven § 199 a. I tillegg foreslo departementet en endring i § 199 a første ledd slik at det fremgår at enhver som har befatning med et datasystem plikter å bruke biometrisk autentisering for å gi politiet tilgang. Departementet foreslo dermed at straffeprosessloven § 199 a kunne lyde:

«Ved ransaking av et datasystem kan politiet pålegge enhver som har befatning 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 ble videre foreslått at det i kapitlet om beslag (straffeprosessloven kapittel 16) henvises til § 199 a så langt den passer, slik at politiets adgang til å anvende makt også skal gjelde når ransakingen har gått over til beslag.

Departementet pekte på at for enkelte typer av biometrisk autentisering vil tvang kunne være vanskelig å gjennomføre eller komme i strid med selvinkrimineringsvernet, men at dette må vurderes i hvert enkelt tilfelle.

Når det gjelder hvem politiet kan tvinge til å gjennomføre autentiseringen, foreslo departementet å begrense det til mistenkte samt andre enn mistenkte når deres datasystem er gjenstand for ransaking. Departementet ba særlig om høringsinstansenes syn på bestemmelsens rekkevidde på dette punktet.

Departementet foreslo at kompetansen til å treffe beslutning om tvang skulle legges til politiet:

«Departementets foreløpige syn er at beslutningen om å anvende makt overfor mistenkte for å få åpnet datasystemet, kan treffes av politiet på stedet, på samme måte som politiet 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.»

6 Høringsinstansenes syn

6.1 Innledning

Følgende høringsinstanser har uttalt seg om lovforslaget:

Riksadvokaten, Det nasjonale statsadvokatembetet (NAST), Oslo statsadvokatembeter, Kripos, Nordland politidistrikt, Oslo politidistrikt, Politidirektoratet, Politiets sikkerhetstjeneste (PST), Sør-Øst politidistrikt, Troms politidistrikt, Vest politidistrikt, ØKOKRIM, Advokatforeningen, Datatilsynet, Politiets Fellesforbund, Politijuristene og Politihøgskolen. Det har også innkommet høringsuttalelse fra *professor Ørnulf Øyen*.

Et flertall av høringsinstansene støtter forslaget om å gi politiet en klar lovhjemmel for å få tilgang til datasystemer som åpnes ved bruk av biometrisk autentisering, om nødvendig ved bruk av tvang, og mener det haster med å få på plass en slik hjemmel. Følgende uttalelse fra *Troms politidistrikt* er illustrerende for den generelle støtten:

«Troms politidistrikt slutter seg som nevnt til departementets vurderinger om behovet for hjemmel som nevnt, jf. over. En er videre enig i at det er nødvendig å innføre en slik hjemmel relativt raskt, ved endring i någjeldende straffeprosesslov. Det vil etter vår mening være utilfredsstillende å avvente innføring av slik hjemmel til ikrafttredelse av ny straffeprosesslov.»

Vest politidistrikt støtter imidlertid ikke lovforslaget:

«Det er flere spørsmål som bør utredes og avklares nærmere før man vedtar en lov som foreslått. Spørsmålet er om behovet for lovendring er så påtrengende at rettsstaten ikke har tid til å avvente en grundigere utredning i forberedelsen av ny straffeprosesslov.»

Blant høringsinstansene er det ulike syn på hvordan hjemmelen bør utformes, særlig knyttet til hvor vidt hjemmelen bør rekke. *Datatilsynet* og *Advokatforeningen* mener forslaget i høringsnotatet rekker for langt på flere punkter.

Av høringsinstansene som har uttalt seg om plasseringen av hjemmelen i straffeprosessloven § 199 a, støtter alle, med unntak av *professor Ørnulf Øyen*, departementets forslag. Også forslaget om at hjemmelen skal gjelde tilsvarende for datasystem som er tatt i beslag, får støtte av høringsinstansene.

6.2 Bør hjemmelen begrenses til visse typer autentiseringsmetoder og datasystemer?

Advokatforeningen mener en lovhjemmel for å gjennomføre biometrisk autentisering ved tvang bør begrenses til avtrykksautentisering, typisk fingeravtrykk, og uttaler:

«Noen former for biometrisk identifisering vil etter sin art kunne være utelukket fra gjennomføring ved tvang. Det kan dreie seg om en identifisering som det ikke er mulig å fremtvinge fysisk, for eksempel stemmegjenkjenning. (...)»

Spørsmålet som kan reises er om nødvendighets- og forholdsmessighetsbegrensningen er tilstrekkelig all den stund den foreslåtte tvangshjemmel i prinsippet åpner for tvangsgjennomføring av enhver form for biometrisk autentisering, og hvor det synes lagt opp til at politiet kan avgjøre hvor grensene skal settes. (...)

De her påpekte forhold reiser spørsmål som ikke synes tilstrekkelig vurdert av departementet. Etter Advokatforeningens skjønn er temaet så omfattende at arbeidet med å utforme et regelverk for tvangsgjennomføring av enhver form for biometrisk autentisering bør skje i tilknytning til det pågående arbeid med ny straffeprosesslov.»

Datatilsynet mener bestemmelsen bør utformes mer presist:

«Departementet har foreslått en lovbestemmelse som etter sin ordlyd egentlig bare sier at tilgang til datasystemet ved biometrisk autentisering skje ved bruk av tvang så lenge tvangen er nødvendig og forholdsmessig. Vi mener det her kan stilles spørsmål ved om en slik lovbestemmelse er presis nok. Ut fra lovens ordlyd vil det iallfall ikke være enkelt å få grep om grensene for den lovlige maktutøvelsen. *Datatilsynet* ønsker derfor at departementet gir en mer presis bestemmelse.»

Vest politidistrikt mener begrepet «datasystem» bør presiseres, og uttaler videre:

«Uten nærmere og grundigere utredning, bør lovhjemmelen – for tilfelle at man finner at man ikke kan avvente utfallet av forslaget til ny straffeprosesslov – avgrenses til noen helt konkrete og praktiske type-tilfeller som blir navngitt og spesifisert slik vi kjenner dem i dag (eksempelvis elektronisk lås til hus, lås til datamaskin og mobiltelefon).»

Oslo statsadvokatembeter, Politidirektoratet, Oslo politidistrikt, Troms politidistrikt og Politijuristene mener bestemmelsen bør gjøres teknologinøytral. *Oslo statsadvokatembeter* uttaler i den forbindelse:

«Videre er det nødvendig at bestemmelsen utformes på en slik måte at den omfatter andre typer biometrisk autentisering enn fingeravtrykksavlesning, som var aktuelt i saken som ble behandlet i Høyesterett, og at bestemmelsen gjelder datasystemer generelt, herunder mobiltelefoner og andre lagringsmedier.»

Politidirektoratet uttaler:

«Politidirektoratet er videre enig i at lovbestemmelsen må være teknologinøytral, jf. «datasystem». Vi støtter *Oslo politidistrikts* uttalelse om at bestemmelsen må omfatte «alle typer datasystemer eller dataenheter og også applikasjoner, låste filer, virtuelle lagre/containere, tjenestetilgang (eks. virtuelt datalager i skyen/cloud), og også fremtidige datasystemer som bærere av informasjon». *Troms politidistrikt* har påpekt det samme, og bedt om at det i tillegg vurderes å innta begrepet *lagringsmedier* i lovteksten for å unngå uklarheter knyttet til hva som skal være omfattet.

Som angitt av departementet må bestemmelsen ikke bare omfatte fingeravtrykksavlesning, men også andre og fremtidige former for biometrisk autentisering.»

6.3 Overfor hvem bør tvangshjemmelen gjelde?

Advokatforeningen og *Datatilsynet* mener tvangshjemmelen bør begrenses til å gjelde overfor mistenkte. *Datatilsynet* uttaler:

«*Datatilsynet* ser at det kan være gode grunner for å åpne for tvang overfor andre enn mistenkte, men mener samtidig det er grunn til å være mer skeptisk her. Etter vårt syn er det grunn til å tro at hva som er et forholdsmessig inngrep står i en noe annen stilling overfor uskyldige tredjeparter enn den/de som er under mistanke, alt etter omstendighetene.»

NAST, Oslo statsadvokatembeter, Riksadvokaten, PST, Politidirektoratet, Kripos, Nordland politidistrikt, Oslo politidistrikt, Sør-Øst politidistrikt, Troms politidistrikt, ØKOKRIM, Politijuristene og Politiets Fellesforbund mener tvangshjemmelen bør gjelde overfor «enhver». *PST* uttaler i den forbindelse:

«I departementets foreløpige vurdering gis det ikke adgang til tvang overfor personer som har tilgang til et datasystem gjennom biometri, men som ikke er mistenkt og hvor ransakingen ikke skjer i «deres» datasystem. Begrunnelsen som er gitt er at maktanvendelsen kan oppleves mer integritetskrenkende. Etter *PSTs* syn bør hensynet til en effektiv straffeforfølgning her veie tyngre.»

Politijuristene uttaler:

«Det er for oss vanskelig å se at det er mer inn-gripende at tredjemann blir tvunget til å åpne siktedes datasystem enn at han blir tvunget til å åpne sitt eget – snarere tvert imot. På denne bakgrunn mener vi at tvangshjemmelen bør «speile» påleggshjemmelen, slik at tvang kan benyttes overfor enhver som har befatning med datasystemet.»

6.4 Hvem bør ha kompetanse til å beslutte tvangsgjennomføring?

Det er delte meninger om hvem som bør ha kompetanse til å bestemme bruk av tvang. *Vest politi-*

distrikt mener bruk av tvang bare bør kunne skje etter forutgående domstolsprøving. *Advokatforeningen* mener det bør vurderes å legge kompetansen til retten for avgjørelser om tvang for visse metoder for biometrisk autentisering. *Datatilsynet* foreslår at kompetansen legges til domstolen, eventuelt med hastekompetanse for påtalemyndigheten eller politiet. *Datatilsynet* uttaler:

«At beslutningen skal treffes av noen andre enn politifolkene på stedet, kan være med på hindre overilte beslutninger i en opphetet ransakingssituasjon. Det vil også bidra til bedre forholdsmessighetsvurderinger.»

Nordland politidistrikt, *Oslo politidistrikt*, *Sør-Øst politidistrikt* og *Politijuristene* mener primærkompetansen bør ligge hos påtalemyndigheten, eventuelt med hastekompetanse for politiet. *Politijuristene* uttaler:

«Kompetansen til å treffe beslutning om bruk av tvang bør etter vår oppfatning legges til påtalemyndigheten. I den forbindelse vises det til at det er påtalemyndigheten som har sekundærkompetansen ved beslutning om ransaking og primærkompetansen ved beslutning om beslag, og at hensynet til sammenheng og konsekvens i regelverket tilsier at beslutningsnivået bør ligge der også for den metodebruken som er til drøftelse her. Maktutøvelsen må vurderes under iakttagelse av forholdsmessighetskravet, og det er naturlig at påtalemyndigheten foretar denne vurderingen, eventuelt samtidig som beslutningen om ransaking og/eller beslag blir truffet. Politiet bør imidlertid gis hastekompetanse for de tilfellene hvor det er fare ved opphold.»

Riksadvokaten, *NAST*, *Oslo statsadvokatembeter*, *Politidirektoratet*, *PST*, *Kripos*, *Troms politidistrikt*, *ØKOKRIM* og *Politiets Fellesforbund* mener kompetansen bør legges til politiet, *Troms politidistrikt* med en tilføyelse om at kompetansen eventuelt bør legges til påtalemyndigheten med hastekompetanse for politiet. *NAST* uttaler i den forbindelse:

«Selv om påtalemyndighetens beslutning om å innhente adgang til et datasystem med tvang relativt raskt kan innhentes ved hjelp av beslutning fra jourhavende jurist i påtalemyndigheten, ser en ikke avgjørende rettssikkerhetsmessige motforestillinger mot å legge kompetansen til polititjenestemenn. Det vises for

øvrig til at en polititjenestemann har hastekompetanse ved ransaking og beslag dersom vilkårene etter straffeprosessloven §§ 198 og 206 er til stede.»

Politidirektoratet uttaler:

«Etter Politidirektoratets syn er det gode grunner til at politiet på stedet bør ha kompetanse til å beslutte bruk av tvang overfor mistenkte og tredjepersoner som nekter å medvirke.

Det vises til at den enkelte polititjenesteperson i dag har adgang til å anvende makt under sin tjenesteutførelse, herunder i forbindelse med gjennomføringen av et besluttet tvangstiltak som for eksempel ransaking, jf. Politiloven § 6. (...) Selv om kompetansen legges til påtalemyndigheten er det uansett politiet på stedet som må gjennomføre tvangsbruken, og i den forbindelse foreta en fortløpende forholdsmessighetsvurdering.»

6.5 Internasjonale forpliktelser

Flere høringsinstanser uttaler seg særskilt om forholdet til EMK. *Advokatforeningen* mener forslaget kan være problematisk blant annet vurdert opp mot EMK artikkel 8:

«Etter Advokatforeningens syn legger forslaget opp til en for generelt utformet tvangshjemmel ettersom den er ment å omfatte enhver form for biometrisk autentisering. I henhold til individets vern etter Grunnloven § 102 og EMK bør en eventuell hjemmel for maktutøvelse i bevissikringsøyemed definere nærmere grensene for tvangsutøvelsen, særlig for de tilfeller hvor autentisering mot vedkommendes vilje betinger hard maktbruk og/eller risiko for skade overfor den som utsettes for tvangen.»

Datatilsynet antar at forslaget ikke i seg selv bryter med EMK artikkel 8, men stiller spørsmål om forslag til lovbestemmelse er presist nok:

«Vi er klar over at det neppe lar seg gjøre å gi helt presis beskrivelse av akseptabel tvangsbruk, og det er heller ikke påkrevd etter EMK art. 8, men etter vårt syn bør det kunne la seg gjøre å være noe mer presis.»

NAST, *Kripos* og *Politidirektoratet* mener lovforslaget ikke vil være i strid med EMK artikkel 8.

Vest politidistrikt mener forholdet til selvinkrimineringsvernet etter EMK artikkel 6 nr. 1 bør

utredes nærmere. *NAST, Kripas, Politidirektoratet* og *professor Ørnulf Øyen* mener lovforslaget ikke vil være i strid med selvinkrimineringsvernet etter EMK artikkel 6 nr. 1.

Når det gjelder selvinkrimineringsvernet, mistenktes rett til taushet og stemmegjenkjenning uttaler *Politidirektoratet* følgende:

«Det fremgår av innspillene fra Kripas og Oslo politidistrikt, at retten til taushet/selvinkrimineringsvernet ikke på generelt grunnlag kan sies å hindre bruk av stemmegjenkjenning til å åpne et datasystem. Oslo politidistrikt mener at i den grad et opptak, herunder politiavhør tatt opp på lyd og bilde, teknisk sett kan brukes som biometrisk autentisering, bør det være rettslig adgang til å bruke det. Politidirektoratet viser til at kjernen i selvinkrimineringsvernet går ut på at en mistenkt ikke er forpliktet til å bidra til å opplyse saken mot seg. Samtidig er Politidirektoratet enig med Politihøgskolen i at bruk av lydopptak etter omstendighetene kan anses som en omgåelse av selvinkrimineringsvernet, og at det derfor kan være hensiktsmessig å klargjøre hvilke typer opptak av mistenkte som eventuelt kan benyttes for autentiseringsformål vedrørende mistenkte.»

6.6 Øvrige innspill om utformingen m.m.

Riksadvokaten, NAST og *Kripas* mener forslaget til presisering i lovteksten om at tvangsbruken må være nødvendig og forholdsmessig synes overflødig, da det alminnelige forholdsmessighetsprinsipp gjelder for bruk av alle tvangsmidler.

Riksadvokaten, Kripas og *Oslo politidistrikt* foreslår en annen formulering av bestemmelsen. *Riksadvokaten* foreslår følgende:

«Riksadvokaten ber departementet vurdere om man klarere bør skille mellom pålegget om å gi tilgang og fullbyrdelse ved tvang dersom pålegget ikke etterkommes frivillig, eksempelvis ved at annet ledd første punktum formuleres slik:

“Dersom mistenkte nekter å etterkomme pålegg som nevnt i første ledd, kan autentiseringen gjennomføres med tvang [dersom tvangsbruken er nødvendig og forholdsmessig].”»

I tillegg til endringer i straffeprosessloven, tar *Riksadvokaten* og *Oslo politidistrikt* til orde for at det vurderes endringer i straffeloven knyttet til de

foreslåtte endringene i straffeprosessloven. *Oslo politidistrikt* uttaler om dette:

«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 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.»

7 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om at politiet ved ransaking eller beslag av datasystem kan pålegge enhver som har befattning med datasystemet å åpne det ved bruk av biometrisk autentisering, jf. forslaget til endringer i § 199 a første ledd. Foruten et innspill om den språklige utformingen, har det i høringsrunden ikke kommet innvendinger til dette forslaget.

Når det gjelder innføringen av en tvangshjemmel for biometrisk autentisering, har departementet merket seg at enkelte høringsinstanser mener dette forslaget krever en grundigere utredning og bør utstå til arbeidet med oppfølgingen av NOU 2016: 24 Ny straffeprosesslov. Departementet mener imidlertid, i likhet med de fleste høringsinstansene, at det haster med å få på plass en slik hjemmel, og at det ikke er tilfredsstillende å vente til ikrafttreddelsen av ny straffeprosesslov. Departementet opprettholder forslaget i høringsnotatet, men med visse justeringer, nemlig at tvangen kan skje overfor enhver og at primærkompetansen til å beslutte tvang legges til påtalemyndigheten. I tillegg gjøres visse språklige endringer.

I denne omgangen nøyer departementet seg med å foreslå biometrisk autentisering, om nødvendig med bruk av tvang, som et aksessorium til det opprinnelige tvangsmiddelet, nemlig ransaking eller beslag av datasystem. En nærmere vurdering av et mer generelt forslag, herunder om hjemmelen skal gjelde tilgang til «sted», vil bli gjort som ledd i departementets oppfølging av NOU 2016: 24 Ny straffeprosesslov.

Departementet har vurdert å begrense hjemmelen til avtrykksautentisering, typisk fingerav-

trykksautentisering, slik blant annet Advokatforeningen tar til orde for, men har kommet til at en slik begrensning er lite hensiktsmessig. Det er allerede i dag utviklet mobiltelefoner som benytter irisgjenkjenning i stedet for fingeravtrykksautentisering. Grunnet den raske teknologiske utviklingen på området, må det antas at også andre autentiseringsmåter vil være vanlig i løpet av kort tid. Dersom bestemmelsen begrenses til visse typer biometrisk autentisering, vil den raskt bli utdatert. Departementet fastholder dermed at bestemmelsen ikke begrenses til visse typer biometrisk autentisering.

Videre fastholder departementet forslaget om at tilgangen skal gjelde «datasystem». Betegnelsen brukes allerede i straffeprosessloven § 199 a samt flere andre steder i straffe- og straffeprosesslovgivningen. Enkelte høringsinstanser har tatt til orde for at bestemmelsen begrenses til visse typer innretninger. På samme måte som for metode for biometrisk autentisering, vil en bestemmelse som presiserer type innretning til for eksempel mobiltelefon eller nettbrett, raskt bli utdatert på grunn av utviklingen på området. En vurdering av om bestemmelsen bør utvides til å gjelde tilgang til annet enn datasystemer vil ikke gjøres i denne omgangen, men vil kunne inngå som del av oppfølgingen av NOU 2016: 24 Ny straffeprosesslov.

I høringsnotatet foreslo departementet at tvangshjemmelen skulle begrenses til å gjelde overfor mistenkte samt andre enn mistenkte når deres datasystem er gjenstand for ransaking eller beslag. Departementet ba særlig om høringsinstansenes syn på dette punktet. Alle høringsinstanser som har uttalt seg om spørsmålet, med unntak av Advokatforeningen og Datatilsynet, mener hjemmelen bør gjelde overfor enhver. Etter nærmere vurdering har departementet kommet til at bestemmelsen bør gjelde overfor enhver som har befatning med et datasystem som er rettslig tilgjengelig gjennom reglene om ransaking og beslag. Slik Politijuristene påpeker, er det ikke nødvendigvis mer inngripende å bli tvunget til å åpne andres datasystem enn sitt eget. Hvor inngripende tvangsgjennomføringen er for den som blir utsatt for inngrepet, vil uansett inngå som del av den konkrete forholdsmessighetsvurderingen, jf. straffeprosessloven § 170 a. Også hensynet til en effektiv strafforfølgning taler for at bestemmelsen bør gjelde overfor enhver.

Departementet foreslo i høringsnotatet at politiet skulle ha kompetansen til å beslutte bruk av tvang, men ba særlig om høringsinstansenes syn på om kompetansen burde løftes opp et nivå, det

vil si til påtalemyndigheten. De fleste høringsinstansene som har uttalt seg om kompetansespørsmålet, støtter departementets forslag. Noen høringsinstanser mener imidlertid at primærkompetansen bør løftes opp ett eller to nivå, eventuelt kombinert med hastekompetanse for politiet.

Departementet har etter en fornyet vurdering kommet til at kompetansen bør løftes opp et nivå, slik at primærkompetansen legges til påtalemyndigheten i politiet, med sekundærkompetanse for politiet når det haster. En slik løsning vil, som noen høringsinstanser er inne på, kunne bidra til en grundigere forholdsmessighetsvurdering, samtidig som politiets behov for å handle når det haster, vil bli ivaretatt gjennom hastekompetansen. Departementet viser for øvrig til at Straffeprosessutvalget i NOU 2016: 24 Ny straffeprosesslov legger beslutningskompetansen for alle tvangstiltak til retten, men med hastekompetanse for påtalemyndigheten, jf. lovutkastet § 14-3. Selv om det i praksis skulle vise seg at politiet benytter hastekompetansen ofte, betyr ikke det at primærkompetansen bør legges til politiet. Utgangspunktet bør etter departementets mening være beslutning fra påtalemyndigheten.

Departementet anser at forslaget her, som gjør det klart at politiet ved ransaking og beslag av datasystem kan bruke tvang for å åpne datasystemet ved biometrisk autentisering, ikke er i strid med EMK artikkel 8. Inngrepet vil oppfylle lovkravet, være begrunnet i hensynet til etterforskning og oppklaring av kriminalitet, et formål som er legitimt etter konvensjonen, samt anses som nødvendig i et demokratisk samfunn, herunder oppfylle forholdsmessighetskravet, se punkt 3.2.

Generelt må man kunne si at fremtvingelse av identifikasjonshandlinger for å få åpnet et datasystem ved bruk av biometrisk autentisering, innebærer en relativt beskjeden og kortvarig maktanvendelse og et langt mindre belastende inngrep enn det politiet i dag allerede har hjemmel til, for eksempel undersøkelse av kroppens hulrom etter straffeprosessloven § 157. Forslaget her innebærer altså at en ved et relativt lite belastende inngrep kan få tilgang til sentrale bevis og dermed bidra til en effektiv strafforfølgning.

Selv om departementet mener at forslaget til en tvangshjemmel for biometrisk autentisering som sådan ikke er i strid med EMK artikkel 8, herunder kravet om at inngrepet er nødvendig og forholdsmessig, vil dette naturligvis måtte vurderes i hvert enkelt tilfelle. Vurderingen av et inngreps forholdsmessighet i det konkrete tilfellet må gjøres ved enhver bruk av tvangsmidler, jf. straffeprosessloven § 170 a, samt ved politiets

anvendelse av makt, jf. politiloven § 6 fjerde ledd jf. annet ledd. Hvor grensen går, må avgjøres konkret i det aktuelle tilfellet.

Etter departementets syn er forslaget heller ikke i strid med selvinkrimineringsvernet som er innført 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. Det vises til Ørnulf Øyen, Vernet mot selvinkriminering i straffeprosessen (2010), punkt 4.3 side 139 følgende, med videre henvisninger. Kjernen i selvinkrimineringsvernet er at mistenkte ikke har plikt til å forklare seg. Forslaget her gjelder ikke forklaringsplikt, og heller ikke fremtvingelse av en forklaring fra mistenkte. Forslaget gjelder det å utnytte et kjennetegn som utgår fra kroppen for å åpne et datasystem, ikke ulikt det å tvinge mistenkte til å gi fra seg en nøkkel til en lås. Kjennetegnet eksisterer uavhengig av mistenktes vilje og stiller ikke mistenkte overfor et valg om å lyve eller angi seg selv. Det er tale om en faktisk hindring som står i veien for tilgang til informasjon som allerede er rettslig tilgjengelig ved at det er gjenstand for ransaking eller tatt i beslag. Det kan imidlertid ikke utelukkes at det kan oppstå situasjoner der selvinkrimineringsvernet setter en skranke for tvangsgjennomføring av biometrisk autentisering. Også dette må vurderes konkret i det enkelte tilfellet.

Noen høringsinstanser påpeker at grunnkravene om forholdsmessighet og nødvendighet, jf. straffeprosessloven § 170 a, gjelder alle tvangsmidler, og at en presisering av disse grunnkravene i lovteksten i § 199 a synes unødvendig samt bryter med straffeprosesslovens systematikk. Departementet har forståelse for innvendingen og endrer forslaget i tråd med dette.

Det er også gjort visse andre språklige endringer sammenlignet med forslaget i høringsnotatet. Departementet slutter seg til Riksadvokatens innspill om at det kan skilles klarere mellom pålegget om å gi tilgang og fullbyrdelsen ved tvang dersom pålegget ikke etterkommes frivillig.

Forslaget til § 199 a fjerde ledd om at bestemmelsen gjelder tilsvarende ved gransking av et beslaglagt datasystem, innebærer at også plikten til å «gi nødvendige opplysninger» for tilgang til datasystemet, jf. første ledd første alternativ, vil gjelde når ransakingen går over i beslag. Som for biometrisk autentisering, er det ingen grunn til at denne medvirkningsplikten ikke skal være den samme ved gransking av et beslaglagt datasystem som ved ransaking av det.

Når det gjelder enkelte høringsinstansers innspill om å gjøre endringer i straffeloven, har

departementet notert seg dette, men finner ikke grunn til å foreta slike endringer i denne omgangen.

8 Økonomiske og administrative konsekvenser

Forslaget til lovendring vil innebære at politiet kan etterforske mer effektivt og dermed ha en viss kostnadsbesparende effekt. For øvrig vil forslaget ikke få nevneverdige økonomiske eller administrative konsekvenser.

9 Merknader til lovforslaget

Medvirkningsplikten i § 199 a første ledd utvides til å gjelde biometrisk autentisering. Forslaget gir politiet adgang til å pålegge enhver som har befattning med et datasystem å stille sine biometriske kjennetegn til rådighet for å åpne datasystemet. Bestemmelsen vil gjelde ved ransaking av et datasystem samt ved gransking av et datasystem som er tatt i beslag, se merknadene til fjerde ledd. Det betyr at vilkårene for å ransake eller beslaglegge det aktuelle datasystemet må være oppfylt. For forståelsen av gjeldende § 199 a vises det til Ot.prp. nr. 40 (2004–2005) punkt 7.2 side 34 med videre henvisninger.

I § 199 a annet ledd innføres en hjemmel for politiet til å benytte tvang overfor den som er pålagt å åpne datasystemet med biometrisk autentisering, men som ikke etterkommer pålegget. Tvangshjemmelen «speiler» påleggshjemmelen. Tvangen kan benyttes overfor «enhver som har befattning med datasystemet», jf. første ledd. Det omfatter mistenkte og enhver tredjemann, uavhengig av om personen eier datasystemet.

Bestemmelsen er teknologinøytral og omfatter ethvert datasystem og enhver form for biometrisk autentisering. Med «datasystem» menes enhver innretning, bestående av maskinvare og programvare, som foretar behandling av data ved hjelp av dataprogrammer. For eksempel omfattes datamaskiner, nettbrett og smarttelefoner. Betegnelsen brukes allerede i straffeprosessloven § 199 a samt flere andre steder i straffe- og straffeprosesslovgivningen, jf. for eksempel straffeprosessloven § 216 o, og skal forstås på samme måte, se Prop. 68 L (2015–2016) punkt 14.8.7 side 269–271 med videre henvisninger.

I utgangspunktet gjelder bestemmelsen enhver form for biometrisk autentisering, herunder fingeravtrykk, annen avtrykksautentisering

og irisgjenkjenning, se punkt 7. Imidlertid kan noen former for biometrisk autentisering etter sin art være utelukket fra gjennomføring ved tvang. Man kan for eksempel ikke tvinge noen til å uttale noe, slik at tvangsgjennomføring av stemmegjenkjenning vil være lite praktisk. Dersom tvangen gjennomføres overfor mistenkte, kan det ikke utelukkes at selvinkrimineringsvernet vil kunne utgjøre en skranke. Dette må vurderes konkret i det enkelte tilfellet. De biometriske kjenetegnene som fremtvinges, skal kun brukes til å åpne systemet og skal ikke lagres.

Hvert tilfelle av bruk av tvang må vurderes opp mot det alminnelige forholdsmessighetsprinsippet i straffeprosessloven § 170 a. Dette innebærer blant annet at tvangen må være egnet til å gi den ønskede virkningen, det vil si lette gjennomføringen av ransakingen eller beslaget, og at det ikke finnes mindre inngripende, alternative virkemidler som er like egnede. Videre må forholdsmessigheten vurderes, hvilket vil innebære en avveining av flere ulike hensyn. Departementet anser at tvangsgjennomføring av de to autentiseringsmetodene som ser ut til å være de mest aktuelle i dag, fingeravtrykksautentisering og irisgjenkjenning, normalt vil innebære nokså beskjeden maktbruk slik at det ikke kan anses uforholdsmessig. Departementet utelukker likevel ikke at irisgjenkjenning vil kunne innebære et noe større inngrep enn fingeravtrykksautentisering og dermed stille noe større krav til «sakens art og forholdene ellers», jf. straffeprosessloven § 170 a.

Av § 199 a tredje ledd følger det at primærkompetansen til å beslutte tvangsgjennomføring

av biometrisk autentisering er lagt til påtalemyndigheten. Dersom det er fare for at bevismaterialet kan gå tapt i påvente av beslutning fra påtalemyndigheten, kan politiet på stedet treffe beslutningen. Beslutningen må da straks meldes påtalemyndigheten.

Etter § 199 a fjerde ledd gjelder medvirkningsplikten og tvangshjemmelen etter første og annet ledd tilsvarende ved gransking av beslaglagt datasystem. Politiets adgang til å pålegge noen å medvirke til biometrisk autentisering eller anvende makt overfor den som nekter å etterkomme pålegget, bør gjelde uavhengig av om det er tale om fortsatt ransaking av datasystemet eller gransking når ransakingen har gått over til beslag. Det er ingen grunn til at politiet ikke skal ha samme virkemidler ved gransking av et beslaglagt datasystem, som ved ransaking av det. Forslaget til fjerde ledd innebærer at politiet også ved gransking av et beslaglagt datasystem kan pålegge enhver å «gi nødvendige opplysninger» for å få tilgang til datasystemet, jf. første ledd første alternativ. Plikten til å gi nødvendige opplysninger vil altså fortsette å gjelde når ransakingen går over i beslag.

Justis- og beredskapsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om endringer i straffeprosessloven (biometrisk autentisering).

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om endringer i straffeprosessloven (biometrisk autentisering) i samsvar med et vedlagt forslag.

Forslag

til lov om endringer i straffeprosessloven (biometrisk autentisering)

I

I lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker skal § 199 a lyde:

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

Dersom noen nekter å etterkomme et pålegg om biometrisk autentisering som nevnt i første ledd, kan politiet gjennomføre autentiseringen med tvang.

Beslutning om bruk av tvang etter annet ledd treffes av påtalemyndigheten. Er det fare ved opphold kan beslutning treffes av politiet på stedet. Beslutningen skal straks meldes til påtalemyndigheten.

Bestemmelsen gjelder tilsvarende så langt den passer for gransking av datasystem som er tatt i beslag etter kapittel 16.

II

Loven gjelder fra den tid Kongen bestemmer.
