UiT Norges arktiske universitet

Det juridiske fakultet

Straffeprosessloven § 199 a – dens rekkevidde og begrensninger.

Går ønsket om teknologinøytralitet på bekostning av kravet til en presis hjemmel?

Mads Mikal Stornes

Masteroppgave i rettsvitenskap …. JUR-3902 …. desember 2019

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstillinger

Denne avhandlingens tema vil dreie seg om dualiteten mellom vide og teknologinøytrale straffeprosessuelle tvangshjemler på den ene siden og kravet til hjemmelens presisjon på den andre siden. Nærmere bestemt vil avhandlingen ta utgangspunkt i straffeprosessloven § 199 a som er en slik teknologinøytral tvangshjemmel, og undersøke og klarlegge rekkevidden av bestemmelsen og dens skranker.[1]

Strpl. § 199 a er en hjemmel for et tvangsmiddel. Bestemmelsen i sin helhet lyder som følger:

> «**§ 199 a.** 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.»[2]

Bestemmelsen hjemler politiets adgang til å kunne gi et pålegg om utlevering av informasjon for å få låst opp et datasystem som skal ransakes og systemet er låst. Pålegget kan rettes mot den som har befatning med systemet. Pålegget strekker seg også til å låse opp et system ved hjelp av biometrisk autentisering og kan gjennomføres ved tvang dersom noen nekter å etterkomme pålegget.

Tvangsmidlene etter straffeprosesslovens fjerde del har et krav til tilstrekkelig presisjon og klarhet. Dette klarhetskravet utledes av det generelle legalitetsprinsippet som etter

[1] Lov av 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker, heretter forkortet strpl.
[2] Strpl. § 199 a.

grunnlovsendringen er nedfelt i Grunnloven § 113, sammenfattet med høyesterettspraksis.[3] Klarhetskravet medfører at tvangshjemler ikke kan gjøres for vide eller vage. Imidlertid vil hensynene til kriminalitetsbekjempelse, den materielle sannhet og en effektiv etterforskning tilsi at hjemlene ikke kan bli for snevre. Det er dette spennet mellom effektive hjemler og presisjonskravet avhandlingen vil søke å belyse, spesielt med blikket rettet mot teknologiske nyvinninger og ønsket om teknologinøytralitet i lovverket.

Det finnes ingen entydig definisjon for uttrykket «teknologinøytral», verken i lovverk, forarbeid eller innen juridisk teori. Dette til tross for at lovgiver i økende grad har gitt uttrykk for at lover og bestemmelser skal være teknologinøytrale.[4] Etter Kaltenborns forståelse ønsker lovgiver at ulike teknologier likestilles.[5] Hovlid formulerer det på en annen måte: «Med teknologinøytral lovgivning forstås lovgivning som ikke tillegger teknologien betydning.»[6] Til syvende og sist baserer teknologinøytralitet seg på å bruke et samlebegrep for alle typer teknologi for samme bruksområde. Slik jeg ser det er dette ønsket om at teknologier likestilles et uttrykk for lovgivers ønske om at like tilfeller skal behandles likt.

Lovgivers ønske om og behov for teknologinøytralitet har sammenheng med stadig nye teknologiske fremskritt, og arbeidet med å tilpasse lovverket til slike fremskritt. Den raske teknologiske utviklingen gjør det ekstra krevende å ha effektive hjemler uten at det går på bekostning av presisjonskravet.

Avhandlingen vil ut fra det foregående søke å belyse to hovedproblemstillinger. Den første problemstillingen er om ordlyden i strpl. § 199 a oppfyller intensjonen om teknologinøytralitet. Den andre problemstillingen er om utformingen av bestemmelsen innebærer at den oppfyller legalitetsprinsippets krav til presis lovhjemmel.

---

[3] Lov av 17. mai 1814 Kongeriket Norges Grunnlov, heretter forkortet Grl. For Høyesteretts innfortolkning av klarhetskravet se eksempelvis Rt. 2014 s. 1105 (acta) avsnitt 30, HR-2016-1833-A (fingeravtrykk-kjennelsen) avsnitt 15 - 18 og 22 og HR-2018-104-A (Mirmotahari) avsnitt 24.
[4] NOU 2003:27 s.10, Prop. 106 L (2016-2017), Prop. 6 L (2016-2017) samt en rekke andre. Et søk på lovdata med emnet «teknologinøytral» for utredninger og proposisjoner gir per skrivende øyeblikk 172 treff på tvers av mange rettsområder.
[5] Jul Fredrik Kaltenborn, «Teknologinøytralitet og datakriminalitet – Særlig om klassifiseringen av begrepet datasystem», *Tidsskrift for strafferett*, 02/2019 (volum 19) s. 148-167 på s. 149.
[6] Ellen Lexerød Hovlid, «Betydningen av teknologiutvalg for grensen mellom lovlige og ulovlige ytringer», *Lov og rett*, 10/2017 (volum 56) s. 609-626 på s. 610, med videre henvisning til Kyrre Eggen, *Ytringsfrihet: vernet om ytringsfriheten i norsk rett*, Oslo 2002 s. 420 flg.

Bestemmelsen reiser også menneskerettslige underproblemstillinger. Herunder vil forbudet mot tortur, umenneskelig og nedverdigende behandling, vernet av privatlivet og selvinkrimineringsvernet problematiseres.

1.2 Bakgrunn og aktualitet

Den teknologiske utviklingen går i et svært raskt tempo. På 1980-tallet var internettet i sin barndom, og det ble ikke introdusert på det private markedet før tiåret etter. Samtidig var fingeravtrykkskannere og retinaskannere fortsatt science fiction.

Sammenlignet med den teknologiske utviklingen har lovgiverprosessen ikke gått i samme tempo. Innen straffeprosessen fikk vi en ny straffeprosesslov i 1981. Til tross for at arbeidet er startet med å utforme ny straffeprosesslov, er den fortsatt ikke vedtatt.[7] Lovgiver har imidlertid oppdatert den eksisterende straffeprosesslov underveis, ved behov.

Sikkerhetsteknologien har kommet med fremskritt for å ivareta vårt stadig økende behov til å beskytte vårt privatliv. Fra enkle hukommelsesbaserte pinkoder og passord til eksterne nøkkelkort og kodebrikker. Fingeravtrykklås og ansiktsgjenkjenning på mobilen er noe som har kommet i den senere tiden. Det er praktiske, enkle og raske metoder å verifisere vår identitet på, slik at det er sannsynligvis teknologier som er kommet for å bli.

For at politiet og påtalemyndigheten skal kunne gjøre sin jobb så effektiv som mulig, er det viktig at lovgiver holder følge med den teknologiske utviklingen. Lovverket må samtidig sørge for å beskytte det enkelte individ mot uforholdsmessig bruk av tvangsmidler og sørge for at privatlivet til den enkelte blir beskyttet.

Strpl. § 199 a ble vedtatt i 2005. Bestemmelsen hjemlet at politiet kunne gi pålegg om at personer skulle gi tilstrekkelig informasjon til politiet slik at de kunne få åpnet et datasystem og ransake det. Av særlig viktighet var det at bestemmelsen var teknologinøytral.[8]

Hjemmel for åpning av datasystemer ved hjelp av biometrisk autentisering, og om nødvendig ved tvang, var ikke i kraft før 2017. Bakgrunnen for hjemmelen er å finne i fingeravtrykk-

[7] NOU 2016:24.
[8] Ot. prp. nr. 40 (2004-2005) s. 34.

kjennelsen. I fingeravtrykk-kjennelsen var spørsmålet om politiet hadde adgang til, med tvang, å bruke fingeravtrykket til en person for å låse opp mobilen hans. Siden daværende strpl. § 199 a ikke inneholdt egen hjemmel for å låse opp datasystemer med fingeravtrykk ved tvang, prosederte påtalemyndigheten på at strpl. § 157 gav hjemmel for dette. Argumentasjonen var at ordlyden «kroppslig undersøkelse» gav tilstrekkelig hjemmel for å kunne benytte tvang for åpne en mobiltelefon med fingeravtrykklås, blant annet fordi den hjemlet mer inngripende tiltak som undersøkelse av kroppslige hulrom og blodprøvetaking under tvang. Tingretten og lagmannsretten som behandlet saken var enige med påtalemyndigheten.[9] Høyesterett var imidlertid ikke enig med denne argumentasjonen, fordi siktemålet for strpl. § 157 var å undersøke kroppen for realbevis, ikke for å benytte kroppen til å få tilgang til andre slike bevis.[10] Høyesterett konkluderte enstemmig at strpl. § 157 ikke gav tilstrekkelig hjemmel for å bruke tvang for å låse opp en mobiltelefon med fingeravtrykklås.

Høyesteretts konklusjon fremprovoserte tiltak hos lovgiver.[11] Det ble behov for en klar lovhjemmel slik at politiet og påtalemyndigheten kunne, om nødvendig med tvang, låse opp mobiler med fingeravtrykklås. Igjen påpekte lovgiver viktigheten av at hjemmelen skulle være teknologinøytral.[12] Fingeravtrykk-kjennelsen er et eksempel på at utøvende makt trenger oppdaterte virkemidler for å effektivt kunne ransake det digitale rom for kriminalitetsbekjempelse.

1.3 Metode og rettskildebilde

Avhandlingen vil benytte seg av rettsdogmatisk metode for å finne frem til hva som er gjeldende rett.[13]

Ett særtrekk innen straffeprosessen er at som følge av Norges internasjonale forpliktelser, vil konvensjoner også være av viktighet for å avklare gjeldende rett. To konvensjoner er av

[9] TJARE-2016-43883 og LG-2016-62717.
[10] Fingeravtrykk-kjennelsen avsnitt 22.
[11] Prop. 106 L (2016-2017) s. 1.
[12] Prop. 106 L (2016-2017) s. 4 og 10.
[13] Jan Fridthjof Bernt og David R. Doublet, *Vitenskapsfilosofi for jurister – en innføring*, 6. opplag, Bergen 2008 s. 13.

viktighet for avhandlingens tema, og vil følgelig benyttes som rettskilder. Den første konvensjonen er Den europeiske menneskerettighetskonvensjon (heretter EMK).[14]

Siden EMK benyttes, er det viktig å klargjøre forholdet mellom EMK og norsk rett. Etter menneskerettsloven § 2 nr. 1 har EMK blitt inkorporert i norsk rett.[15] Det følger av mrl. § 3 at ved motstrid med norsk lov skal EMK ha forrang. Det vil med andre ord si at dersom noe i norsk særlov strider imot bestemmelser i EMK, skal EMK legges til grunn som gjeldende rett. Dette gjelder imidlertid ikke grunnlovsbestemmelser, jf. *lex superior*-prinsippet og høyesterettspraksis.[16]

At EMK ikke kan ha forrang over Grunnlovsbestemmelser er i utgangspunktet et statsrettslig spørsmål. Det bygger på at Grunnloven har gitt lovgiver kompetanse til å lage nye lover, men lovgiver er ikke gitt kompetanse til å gi lover som kan stride mot Grunnloven.[17] Imidlertid er det slik at etter Grunnlovsendringen i 2014 er menneskerettighetene nedfelt i Grunnloven. Mange av bestemmelsene har svært lik ordlyd som sine paralleller i EMK. Etter høyesterettspraksis er det slik at ordlyden i menneskerettsbestemmelsene i Grunnloven skal tolkes i lys av sine paralleller.[18] Høyesterett forankrer sitt synspunkt med å vise til Grl. § 92.[19] Etter Grl. § 92 skal statens myndigheter (herunder både domstolene og lovgiver) sørge for å sikre at menneskerettighetene både etter Grunnloven og EMK bli overholdt og hensyntatt. Imidlertid uttaler Høyesterett samtidig følgende:

> «(...) men likevel slik at fremtidig praksis fra de internasjonale håndhevings-organene ikke har samme prejudikatsvirkning ved grunnlovstolkningen som ved tolkningen av de parallelle konvensjonsbestemmelsene: Det er etter vår forfatning Høyesterett – ikke de internasjonale håndhevingsorganene – som har ansvaret for å tolke, avklare og utvikle Grunnlovens menneskeretts-bestemmelser.».[20]

---

[14] Europarådets konvensjon av 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter.
[15] Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (mrl.).
[16] HR-2016-2554-P avsnitt 70, se også Smith (2017) s. 205 om *lex superior*-prinsippet.
[17] Eivind Smith, *Konstitusjonelt demokrati: Statsforfatningsretten i prinsipielt og komparativt lys*, 4. utgave, Bergen 2017 (Smith 2017) s. 205.
[18] Rt. 2015 s. 93 (Maria-dommen) avsnitt 57, Rt. 2015 s. 155 (Rwanda) avsnitt 40 og Rt. 2014 s. 1292 avsnitt 14.
[19] Høyesteretts uttalelse i Rt. 2014 s. 1292 avsnitt 14 samt Maria-dommen avsnitt 59.
[20] Maria-dommen avsnitt 57.

Det er med andre ord Høyesterett som er prejudikatsdomstol for hvordan Grunnlovens bestemmelser skal tolkes, ikke Den europeiske menneskerettsdomstolen (heretter EMD) eller andre internasjonale domstoler.

Den andre konvensjonen avhandlingen vil benytte som rettskilde er konvensjon om datakriminalitet.[21] Konvensjonen er ikke inkorporert i norsk rett. Den er imidlertid transformert gjennom endringer i straffeloven og straffeprosessloven.[22]

Forholdet mellom denne konvensjon og norsk rett gjøres klart gjennom *presumsjonsprinsippet*. Der det er motstrid mellom norsk rett og Norges forpliktelser etter folkeretten, er norsk rett gjeldende. Dette er på grunn av det dualistiske prinsipp innen statsretten. I tilfeller der det ikke er noen direkte motstrid, presumeres norsk internrett å være sammenfallende med de internasjonale forpliktelsene.[23]

1.4 Begrepsavklaringer og avgrensninger

Biometrisk autentisering er en type sikkerhetsteknologi som gjør at et datasystem eller «innholdsdata» som er låst kan åpnes ved hjelp av gjenkjenning av en biometrisk markør.

Avhandlingen legger til grunn Sundes forståelse av begrepet innholdsdata. [24] Sunde sondrer ikke mellom begrepene innholdsdata og «primærdata».

Til tross for at forarbeidene benytter begrepet «biometrisk autentisering» er det ikke gitt noen definisjon annet enn en eksemplifisering gjennom enkelte biometriske markører. Avhandlingen vil derfor legge til grunn Store norske leksikons forståelse av begrepet.[25] Biometrisk autentisering (eller biometrisk gjenkjenning) er altså gjenkjenning av et menneske ved hjelp av kroppen.

I prinsippet kan alle unike trekk ved ens kropp gjøres om til en biometrisk markør. Ansiktsgjenkjenning er allerede i utstrakt bruk i dag på mobiltelefoner. Likeså med

---

[21] Europarådets konvensjon av 23. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons og kommunikasjonsteknologi, heretter konvensjon om datakriminalitet.
[22] Lov 20. mai 2005 nr. 28 om straff (strl.) og NOU 2003: 27.
[23] Smith (2017) s. 141.
[24] Inger Marie Sunde, *Lov og rett i cyberspace*, Bergen 2006 (Sunde 2006) s. 265, jf. s. 131 og s 272 flg.
[25] Eirik Rossen, «biometrisk gjenkjenning», *Store norske* leksikon (2019), https://snl.no/biometrisk_gjenkjenning (Rossen 2019).

irisgjenkjenning.[26] Ganglagsanalyse er allerede begynt å bli benyttet av kinesiske myndigheter i kriminalitetsbekjempelse.[27] Stemmegjenkjenning har vært implementert i Norge allerede i 2002.[28] Andre former for biometriske markører som kan tenkes brukt for autentisering er per i dag lite utbedt på konsumentnivå, men den teknologiske utviklingen åpner for nye og ukjente metoder i fremtiden.

Avhandlingen vil konsekvent benytte begrepet «siktede», til tross for at noen drøftelser også vil kunne omhandle en mistenkt eller tiltalt. Dette begrunnes med at avhandlingen omhandler en hjemmel som aktiveres ved ransaking, jf. strpl. § 199 a, jf. strpl. § 192. Etter strpl. § 82 vil en mistenkt få status som siktet når det er besluttet eller foretatt ransaking.

Avhandlingen vil avgrense mot noen utførlig drøftelse av det generelle legalitetsprinsippets materielle krav, altså at en hjemmel må være nedfelt i lov eller forskrift gitt i medhold av lov. Dette gjøres fordi avhandlingen tolker en bestemmelse som *er* nedfelt i lov, og det materielle krav kan derfor ikke problematiseres. Avhandlingen vil heller fokusere på det kvalitative krav, altså krav til tilstrekkelig klar og presis ordlyd.

1.5 Fremstillingen videre

For å kunne forstå rekkevidden av strpl. § 199 a må de overordnede normene som utgjør skranker til bestemmelsen klarlegges. Avhandlingen vil derfor i kapittel 2 gjøre rede for bestemmelsens skranker. Herunder vil det bli gjort rede for forbudet mot tortur og umenneskelig og nedverdigende behandling, vernet av privatlivet og den personlige integritet, kravet til en tilstrekkelig presis og klar hjemmel samt selvinkrimineringsvernet. Skrankene vil bli redegjort for i avhandlingens andre kapittel.

I avhandlingens kapittel 3 vil innholdet i strpl. § 199 a klarlegges. Bestemmelsens ordlyd inneholder en begrepsbruk som må tolkes for å kunne si noe om innholdet i bestemmelsen. Det vil også være nødvendig å drøfte konsekvensen av at noen nekter å etterkomme pålegget. Deretter vil det undersøkes hvem som innehar kompetansen til å bestemme et pålegge eller

[26] Prop.106 L (2016-2017) første avsnitt s. 9.
[27] Chiara Giordano, «Chinese police use surveillance technology to identify people by their walking style», *The Independent*, 26. februar 2019, https://www.independent.co.uk/news/world/asia/china-police-walking-gait-technology-surveillance-ai-suspect-a8797836.html (Giordano 2019).
[28] Se Rossen (2019) under overskriften «talegjenkjenning».

ilegge tvang. Til sist vil det drøftes jurisdiksjon, all den tid den digitale verden er globalisert og nettverk kan krysse landegrenser.

I avhandlingens kapittel 4 vil det bli foretatt avsluttende vurderinger. Her vil det bli tatt en oppsummering av avhandlingens funn. Det vil også bli vurdert om det er hensiktsmessig å gjøre endringer i bestemmelsen.

Det vil fortløpende bli foretatt sammenligninger mellom gjeldende rett og forslag til ny straffeprosesslov i NOU 2016: 24 der det er relevant.

2 Skrankene til straffeprosessloven § 199 a

Ved alle inngrep i privatlivet vil menneskerettighetsbestemmelser både etter Grunnloven og EMK sette skranker for myndighetenes inngrep overfor den enkelte. Forbudet mot tortur, umenneskelig og nedverdigende behandling er en absolutt skranke uansett inngrep, og dette vil bli gjort rede for i 2.1.

Vernet av privatlivet og den personlige integritet står også sentralt for avhandlingens tema. Dette vernet vil bli gjort rede for i 2.2.

Klarhetskravet i legalitetsprinsippet er noe som går til kjernen i avhandlingens tema og er en skranke for hvordan rettsanvendere skal tolke bestemmelser. Klarhetskravet vil bli gjort rede for i avhandlingens 2.3.

Enkelte former for biometrisk autentisering vil potensielt være problematisk i forhold til selvinkrimineringsvernet. Selvinkrimineringsvernet vil derfor fungere som en skranke for hvilke biometriske autentiseringer som kan påtvinges av offentlig myndighet, og vil bli gjort rede for i 2.4.

2.1 Forbudet mot tortur, umenneskelig og nedverdigende behandling

Etter Grl. § 93 og EMK art. 3 er det satt et absolutt forbud mot tortur og umenneskelig eller nedverdigende behandling. Det må derfor være en absolutt ytre grense for hvor langt tvangen

i strpl. § 199 a annet ledd kan gå. Det er på det rene at Grl. § 93 er konstruert etter modell fra EMK art. 3.[29] I det følgende vil dermed begge bestemmelsene drøftes under ett.

Torturforbudet gjør at det ikke er mulig å benytte tvang for å innhente passord, da den eneste måten å tvinge noen til å oppgi informasjon på er ved hjelp av tortur eller trussel om tortur. Trussel om tortur er imidlertid ikke å anse som tortur men umenneskelig behandling, men det er fortsatt et absolutt forbud mot dette.[30] EMD reserverer begrepet tortur til «(…) deliberate inhuman treatment causing very serious and cruel suffering».[31] Terskelen må her sies å være høy. Dette illustreres i Irland v. Storbritannia der Britiske myndigheter utsatte IRA-fanger for flere forhørsteknikker («de fem teknikker»).[32] Her ble fangene utsatt for søvnmangel, utsulting, fysiske plager, støy og sensorisk deprivasjon. EMD vurderte det slik at denne behandlingen ikke var å anse som tortur men umenneskelig behandling, til tross for at kommisjonen var av den oppfatning at dette var tortur.[33] Terskelen for tortur er med andre ord svært høy, på den andre siden er det vanskelig å se tilfeller der en person ikke blir utsatt for svært ille behandling for å få ut informasjon ufrivillig. Behandling som er ille nok til at det er aktuelt å vurdere torturforbudet kan tenkes å falle inn under umenneskelig eller nedverdigende behandling.

Dette forhindrer imidlertid ikke politiet fra å søke etter og ta beslag i notater der passord eller annen relevant informasjon er skrevet ned. Dersom slik fysisk nedskrevet informasjon eksisterer er det tilgang til å granske denne informasjonen, på lik linje med andre ransakings eller beslagsobjekter. Man ser derfor en forskjell mellom ren kunnskapsbasert informasjon og informasjon som er skrevet ned eller lagret.

Ut over torturforbudet vil forbudet mot umenneskelig eller nedverdigende behandling sette en skranke for hvilke typer biometriske markører som kan innhentes med tvang. Dette fordi visse typer biometriske markører krever omfattende tvang for å innhentes og det vil videre potensielt krenke en persons personlige integritet, jf. Grl. § 102. Et spørsmål som kan stilles

---

[29] Dok. nr. 16 (2011-2012) s. 109.
[30] EMDs Storkammerdom av 1. juni 2010, *Gäfgen v. Germany*, 22978/05 (Gäfgen v. Tyskland) avsnitt 90, 91 og 108.
[31] EMDs dom av 18. januar 1978, *Ireland v. The United Kingdom*, 5310/71 (Irland v. Storbritannia 1978) avsnitt 167.
[32] Irland v. Storbritannia avsnitt 96 - 107, se også Jørgen Aall, *Rettsstat og menneskerettigheter*, 5. utgave, Bergen 2018 (Aall 2018) s. 190 og David Harris m.fl., *Law of the European Convention on Human Rights*, 4. utgave, Oxford 2018 side 268 (Harris m.fl. 2018) s. 241.
[33] Irland v. Storbritannia avsnitt 165 - 168, se også Aall (2018) s. 191 og Harris m.fl. (2018) s. 241.

her er hvor den nedre grensen går for hva som kan sies å være umenneskelig eller nedverdigende behandling.

Etter ordlyden må begrepene tilsi at det må være behandling som tjener til å ydmyke eller være umenneskelig, og bestemmelsen kan ikke aktiveres ved enhver dårlig behandling. Et slikt syn har støtte i EMD som har fastslått at:

> «[a]s was emphasised by the Commission, ill-treatment must attain a minimum level of severity if it is to fall within the scope of Article 3 (art. 3). The assessment of this minimum is, in the nature of things, relative; it depends on all the circumstances of the case, such as the duration of the treatment, its physical or mental effects and, in some cases, the sex, age and state of health of the victim, etc.» [34]

Med andre ord må den aktuelle behandlingen inneholde et slags minimum av alvorlighetsgrad for at det skal betraktes som umenneskelig eller nedverdigende. Grensen er relativ og må vurderes ut fra hver enkelt sak, der opplistede momenter inngår i vurderingen. Listen er ikke uttømmende, jf. «etc.».[35] Dette kriteriet var introdusert i 1978 i saken Irland v. Storbritannia, og EMD har ikke fraveket dette kriteriet.

I saken Jalloh v. Tyskland har EMD kommet med uttalelser av generell art om hva som er å anse som umenneskelig og nedverdigende behandling.[36] Saken er dessuten illustrerende for hvordan EMD betrakter bruk av medisinske inngrep for å innhente bevis i forhold til EMK art. 3. I dommens avsnitt 67-74 presiseres vurderingene om hva som er brudd på art. 3 til en test, under henvisning til tidligere praksis.[37] Hva som vurderes til *umenneskelig* behandling drøftes i avsnitt 68:

> «Treatment has been held by the Court to be 'inhuman' because, *inter alia,* it was premeditated, was applied for hours at a stretch and caused either actual bodily injury or intense physical and mental suffering (...)».[38]

---

[34] Irland v. Storbritannia (1978) avsnitt 162.
[35] Irland v. Storbritannia (1978) avsnitt 162.
[36] EMDs storkammerdom av 11. juli 2006, *Jalloh v. Germany*, 54810/00 (Jalloh v. Tyskland). Det er dissens 10-7 hva gjelder det materielle resultat, ved enkelte vurderinger er det imidlertid enstemmighet.
[37] I Jalloh v. Tyskland avsnittene 67-74 er alle dommerne enstemmig.
[38] Jalloh v. Tyskland avsnitt 68.

Ved vurderingen om en behandling er umenneskelig må det altså vurderes om behandlingen var gjort med hensikt, over flere timer av gangen og resulterte i kroppslig skade eller intens fysisk eller psykisk smerte. Listen er ikke uttømmende, jf. «*inter alia*».[39] Det betyr dermed at andre momenter kan spille inn.

Om hva som er *nedverdigende* behandling:

> «Treatment has been considered 'degrading' when it was such as to arouse in its victims feelings of fear, anguish and inferiority capable of humiliating and debasing them and possibly breaking their physical or moral resistance (...), or when it was such as to drive the victim to act against his will or conscience (...).»[40]

Nedverdigende behandling foreligger altså når behandlingen har vekket frykt, angst eller mindreverdighet. Denne frykten, angsten eller mindreverdigheten må være egnet til å ydmyke eller nedverdige, eller egnet til å bryte ned personens fysiske/psykiske motstandsevne. Eller at behandlingen hadde som formål å få offeret til å handle mot sin vilje eller samvittighet.

Faktum i Jalloh v. Tyskland kan oppsummeres slik: Tysk politi mistenkte en person for å ha solgt narkotika. Når de skulle ransake ham, svelget han en pose som politiet mistenkte inneholdt det narkotiske stoffet. Siden de ikke fant noe annet narkotisk stoff på hans person under ransaking, gav påtalemyndigheten ordre om å gi den siktede brekningsmiddel. Den siktede ville ikke innta midlet frivillig. Det ble så besluttet å gi ham det med tvang. Dette ble gjort ved at den siktede ble holdt fast av fire politibetjenter, mens legen førte en tube gjennom siktedes nese og inn til magesekken. Det ble så pumpet to forskjellige typer brekningsmidler gjennom tuben. Den siktede ble så holdt under observasjon og vakt til innholdet i magen kom opp.

Flertallet i Jalloh v. Tyskland la til grunn at det medisinske inngrepet ikke var nødvendig og at det fantes mindre inngripende tiltak.[41] De kunne ventet til posen med narkotikaen ble passert naturlig gjennom kroppen hans. Flertallet la videre til grunn at behandlingen ikke hadde til hensikt å redde den siktedes liv eller helse, men heller å innhente bevis.[42] Flertallet

[39] Jalloh v. Tyskland avsnitt 68.
[40] Jalloh v. Tyskland avsnitt 68.
[41] Jalloh v. Tyskland avsnitt 77.
[42] Jalloh v. Tyskland avsnitt 75.

fant det tilstrekkelig bevist at det fantes en betydelig helserisiko ved den medisinske metoden som ble benyttet, til tross for at de anerkjente at det er uenighet om dette i fagmiljøet.[43]

Dersom hensikten med et slik medisinsk inngrep som i Jalloh v. Tyskland er å redde den ikke-samtykkende part for liv og helse, er det ikke i strid med artikkel 3.[44]

En annen dom som er relevant å se til for hva som er brudd på EMK art. 3 er Bouyid v. Belgia.[45] Dommen er avsagt under dissens 14-3. Flertallet legger til grunn at:

> «[a]ny interference with human dignity strikes at the very essence of the Convention (see paragraph 89 above). For that reason any conduct by law-enforcement officers *vis-à-vis* an individual which diminishes human dignity constitutes a violation of Article 3 of the Convention. That applies in particular to their use of physical force against an individual where it is not made strictly necessary by his conduct, whatever the impact on the person in question.»[46]

Videre legger flertallet til grunn at dette gjelder spesielt i tilfeller der personen er anholdt og under kontroll av politimyndighet.[47]

Med andre ord går all behandling som berører menneskelig verdighet til selve kjernen av EMK art. 3. Videre gjelder dette spesielt bruk av fysisk makt mot et individ når han ikke har gjort dette nødvendig med sin væremåte eller oppførsel, spesielt når makten utføres av politimyndigheten og den berørte er under deres kontroll.

I Bouyid v. Belgia var det tale om at politibetjenter hadde slått en siktet i ansiktet med flat hand.[48] Flertallet fant det ikke bevist at den siktedes oppførsel hadde vært slik at det var nødvendig med en smekk i ansiktet, og at det derfor forelå brudd på art. 3.[49]

---

[43] Jalloh v. Tyskland avsnitt 78.
[44] Harris m.fl. (2018) med videre henvisning til EMDs dom av 7. oktober 2008, *Bogumil v. Portugal*, 35228/03 (Bogumil v. Portugal) avsnitt 77.
[45] EMDs storkammerdom av 28. september 2015, *Bouyid v. Belgium*, 23380/09 (Bouyid v. Belgia)
[46] Bouyid v. Belgia avsnitt 101.
[47] Bouyid v. Belgia avsnitt 88 med videre henvisning til tidligere praksis.
[48] Flere steder i dommen blir det beskrevet at politiet tildelte et «slap». Det legges til grunn at det med «slap» må forstås slag med flat hand. Det understrekes at det er min oversettelse av hvordan faktum beskrives. For rettens vurdering av faktum forøvrig se Bouyid v. Belgia avsnitt 91 - 113.
[49] Bouyid v. Belgia avsnitt 102.

Fysisk maktbruk av politimyndigheten der personens verdighet berøres, må derfor betraktes som brudd på EMK art. 3. Dette gjelder spesielt når det ikke gjøres nødvendig av en persons oppførsel eller væremåte og personen er under politiets kontroll.

I Jalloh v. Tyskland var det tale om svært omfattende inngrep i en persons fysiske integritet, mens det i Bouyid v. Belgia ikke var tale om like omfattende inngrep. Rettsutviklingen ser dermed ut til å gå i retning av at det skal svært lite maktbruk til for at det foreligger et brudd. Dette må tas til inntekt for at det må utvises forsiktighet ved innsamling av biometriske markører. Inngrep for å hente biometriske markører som går på bekostning av menneskelig verdighet er det dermed satt en skranke for.

2.2 Vernet av privatlivet og den personlige integritet

Vernet av privatlivet er lovfestet i Grl. § 102 og EMK art. 8. Bestemmelsene tar sikte på å sikre borgere privatliv, personvern og beskyttelse mot inngrep i den personlige integritet. Et slikt vern er «(...) grunnleggende i et liberalt demokrati».[50] Vernet av den personlige integritet er i likhet med forbudet mot tortur, umenneskelig og nedverdigende behandling relevant i forhold til hvilke biometriske markører som kan innhentes ved tvang. Hva gjelder personvernet er det relevant fordi det taler til hvilken adgang, hvis noen, norske myndigheter har til å lagre datamateriale som blir samlet inn ved tvangsmessig bruk av biometrisk autentisering. I motsetning til forbudet mot tortur, umenneskelig og nedverdigende behandling er imidlertid vernet av privatlivet ikke en absolutt skranke, dette vil bli redegjort for etter innholdet av skranken er undersøkt.

Før inkorporeringen av EMK var det kun et begrenset lovfestet vern for husransakelser etter Grl. § 102. Det fantes imidlertid en *ulovfestet* alminnelig rett til personvern som Høyesterett etablerte allerede i dommen inntatt i Rt. 1952 s. 1217.[51] Ved grunnlovfestingen av vernet av privatlivet går det klart frem av forarbeidene at bestemmelsen i den nye Grl. § 102 er inspirert av EMK art. 8.[52] Samtidig går det frem av forarbeidene at grunnlovfestingen av privatlivet ikke skulle medføre noen endring i den gjeldende rett som fulgte av de ulovfestede reglene

[50] Smith (2017) s. 385.
[51] Rt. 1952 s. 1217 på side 1219, se også dok. 16 (2011-2012) s. 73.
[52] Dok. 16 (2011-2012) s. 175.

samt den internasjonale og nasjonale lovgivning.[53] Grunnlovfestingen skulle synliggjøre rettighetene og forankre dem på grunnlovs nivå.[54] Vernet av den personlige integritet går ikke eksplisitt frem av ordlyden etter EMK art. 8, slik den gjør i Grl. § 102. Imidlertid har EMD gitt uttrykk for at EMK art. 8 inneholder et slikt vern av den personlige integritet i flere avgjørelser. I det følgende avhandlingen se på noen slike dommer for å forklare hvilke inngrep som berører beskyttelsen av privatlivet.

I 1985 fastslo EMD for første gang at inngrep i den personlige integritet kunne medføre brudd på EMK art. 8.[55] I saken med X og Y v. Nederland fant EMD at voldtekt medførte brudd av EMK art. 8 til tross for at det var en privatperson og ikke en tjenestemann som hadde forgrepet seg på fornærmede.[56] Det hører med til faktum at fornærmede var handicappet.[57] Det var konstatert brudd fordi daværende straffelov i Nederland ikke gav adekvat strafferettslig beskyttelse overfor den fornærmede.[58]

I Y.F. v. Tyrkia konstaterte EMD at inngrep i den personlige integritet er beskyttet, uansett om inngrepet er av liten viktighet:

> «The Court observes that Article 8 is clearly applicable to these complaints, which concern a matter of 'private life', a concept which covers the physical and psychological integrity of a person (…). It reiterates in this connection that a person's body concerns the most intimate aspect of private life. Thus, a compulsory medical intervention, even if it is of minor importance, constitutes an interference with this right (...)»[59]

Faktum i Y.F. v. Tyrkia var slik at det var tale om en gynekologisk undersøkelse. Avhandlingen legger imidlertid til grunn at en tvangsundersøkelse av en persons genitalier ikke er av mindre viktighet, men heller et relativt stort inngrep i privatlivet. I Peters v. Nederland konstaterte EMD at også urinprøver tatt mot en persons vilje vil gjøre ett inngrep

[53] Dok. 16 (2011-2012) s. 175.
[54] Dok. 16 (2011-2012) s. 175.
[55] Harris m.fl. (2018) s. 505 med videre henvisning til EMDs dom av 26. mars 1985, X and Y v. The Netherlands, 8978/80 (X og Y v. Nederland).
[56] Aall (2018) s. 219.
[57] Harris m.fl. (2018) s. 505.
[58] X og Y v. Nederland avsnitt 29 og 30.
[59] EMDs dom av 22. juli 2003, *Y.F v. Turkey*, 24209/94 (Y.F. v. Tyrkia) avsnitt 33.

etter art. 8.[60] Rettsutviklingen ser ut til å gå i retning av at alle inngrep i den fysiske integritet vil utgjøre et inngrep etter art. 8. Aall konstaterer at pålegg om å avgi blodprøve også vil være et klart inngrep i privatlivet.[61] Imidlertid vil ikke et medisinsk inngrep utført med samtykke utgjøre et inngrep i art. 8.[62] Høyesterett legger til grunn at også innhenting av fingeravtrykk vil gjøre ett inngrep i en persons privatliv, jf. EMD praksis.[63]

I avhandlingens kapittel om forbudet mot tortur, umenneskelig og nedverdigende behandling ble Bogumil v. Portugal og Jalloh v. Tyskland drøftet. I Bogumil v. Portugal ble det heller ikke konstatert krenkelse av art. 8, i likhet med vurderingen av art. 3. Det var uklart om det forelå samtykke til behandlingen, men det var lagt til grunn at behandlingen var gjort for å redde personens liv ikke samle bevis.[64] På grunn av at den primære årsaken til behandlingen var for å redde liv i motsetning til å samle bevis var det ikke ansett som et inngrep i den fysiske integritet.

I Jalloh v. Tyskland ble det ikke vurdert om behandlingen den mistenkte ble utsatt for var å anse som et brudd på EMK art. 8. Årsaken til at art. 8 ikke ble vurdert var imidlertid fordi EMD kom frem til at det behandlingen var et brudd etter art. 3.[65] Det kan derfor tolkes slik at vernet av den fysiske integritet og forbudet mot umenneskelig og nedverdigende behandling er delvis overlappende. En slik tolkning har støtte i juridisk teori. I Harris m.fl. (2018) gis det uttrykk for at det i praksis påberopes brudd på art. 8 når behandlingen ikke har nådd terskelen til art. 3.[66] Saken i Irland v. Storbritannia etablerte som nevnt at det måtte et vist minimum av alvorlighets grad til for å betraktes som brudd på art. 3. Harris m.fl. (2018) påpeker videre at det er ikke helt klart hvor grensedragningen går mellom art. 8 og art. 3, og at EMD i senere tid har i sine drøftelser startet å vurdere brudd på art. 3 og dersom brudd konstateres vil det ikke være noen separat redegjørelse for art. 8.[67]

---

[60] EMDs kjennelse av 6. april 1996, *Peters v. The Netherlands*, 21132/93 (Peters v. Nederland) avsnitt 8 under overskriften «The law».
[61] Aall (2018) s. 219.
[62] Harris m.fl. (2018) s. 522 med videre henvisning til EMDs dom av 16. juni 2005, *Storck v. Germany*, 61603/00.
[63] Fingeravtrykk-kjennelsen avsnitt 14-16, med videre henvisning til EMDs storkammerdom av 4. desember 2008, *S. and Marper v. The United Kingdom*, 30562/04 og 30566/04 (S. og Marper v. Storbritannia).
[64] Harris m.fl. (2018) s. 523.
[65] Jalloh v. Tyskland avsnitt 86.
[66] Harris m.fl. (2018) s. 519.
[67] Harris m.fl. (2018) s. 519 og 520.

Gjeldende rett kan i alle tilfelle sies å være at alle inngrep ved en persons fysiske integritet vil berøre hans privatliv. Det vil imidlertid ikke utgjøre et inngrep i en persons privatliv om det utføres et medisinsk inngrep der personen samtykker, eller det er gjort for å berge personens liv. Rettstilstanden kan med andre ord sies å være at innhenting av biometrisk informasjon er noe som går til kjernen av det art. 8 beskytter.

Hva gjelder personvernet fastslo EMD i S. og Marper v. Storbritannia at lagring av fingeravtrykk, DNA og celleprøver etter straffesaken mot dem var ferdige, var et inngrep i personvernet.[68] Lagring av medisinsk informasjon er også ett inngrep i art. 8.[69] Lagring av fotografier av personer vil også være et inngrep av vernet i artikkelen.[70]

Rettighetene etter Grl. § 102 og EMK art. 8 er imidlertid, til forskjell fra Grl. § 93 og EMK art. 3, som nevnt ikke absolutte. Etter EMK art. 8 nr. 2 går det frem direkte etter ordlyden at vernet ikke er absolutt. Inngrep kan gjøres på bekostning av privatlivet når det oppfyller gitte vilkår. Etter EMK art. 8 nr. 2 kan det ikke gjøres noe inngrep i rettighetene etter art. 8 nr. 1 unntatt når det er hjemlet i lov, det tjener formål som beskytter interessene listet i bestemmelsen og at det er forholdsmessig. Kravet til forholdsmessighet ledes ut av ordlyden «necessary in a democratic society».[71] Til tross for ordlyden i Grl. § 102 gir inntrykk for at det er et absolutt vern, er det etablert i rettspraksis at dette ikke er tilfelle.[72] Etter Høyesterettspraksis gjelder de samme krav til lov, formål og forholdsmessighet i inngrep i Grl. § 102 som i EMK art. 8.[73] Bestemmelsene drøftes derfor under ett. I det følgende vil det ikke drøftes noe om formålskravet eller kravet til lovhjemmel, men fokusere på kravet til forholdsmessighet.[74]

---

[68] S. og Marper v. Storbritannia avsnitt 68 - 86, med videre henvisning til tidligere praksis hva gjelder DNA- og celleprøver.
[69] Harris (2018) s. 538, Aall (2018) s. 228 med videre henvisning til EMDs dom av 25. februar 1997, Z. v. Finland, 22009/93 (Z. v. Finland) og Francis Jacobs, Robin White og Clare Ovey, The European Convention on Human Rights, 7. utgave av Bernadette Rainey, Elizabeth Wicks og Clare Ovey, Oxford 2018 (Jacobs, White og Ovey 2017) s. 421 med videre henvisning til Z. v. Finland og L.H. V. Latvia, 52019/07.
[70] Harris (2018) s. 538 med videre henvisning til Murray v. UK og McVeigh, O'Neill and Evans V. UK.
[71] EMK art. 8 nr. 2 se også Jacobs, White og Ovey (2017) s. 359, Aall (2018) s. 151 flg. og Jon Petter Rui, «Grunnlovens krav om forholdsmessighet ved inngrep i grunnlovfestede menneskerettigheter», *Lov og rett*, 03/2018 (volum 57), s. 129-130 (Rui 2018).
[72] Maria-dommen avsnitt 60.
[73] Maria-dommen avsnitt 60, Mirmotahari avsnitt 23 og Acta avsnitt 29-30.
[74] Formålskravet legges til grunn i avhandlingen å være møtt. Hva gjelder krav til lov legger avhandlingen til grunn at det er møtt når det kommer til det materielle aspektet, hva gjelder det kvalitative vil dette bli redegjort for i 2.3.

Rui kategoriserer vurderingen av forholdsmessighet til fire komponenter:

> «1) Et inngrep må vareta et legitimt formål, 2) det må være egnet til å vareta det legitime formålet, 3) det må være nødvendig, og 4) det må være forholdsmessig/proporsjonalt i snever forstand»[75]

De første to komponentene er selvforklarende. Med den tredje komponenten siktes det til at ingen andre mindre inngrep er egnet til å ivareta det legitime formålet. Ved vurderingen av forholdsmessigheten i snever forstand er det tale om å veie inngrepets styrke «(...) opp mot den frihetsinteresse som det gripes inn i».[76]

Samtidig gjør Rui det klart at «[i]nnholdet i kravet om forholdsmessighet kan systematiseres på ulike måter.»[77] Innen den juridiske teorien er det andre måter å forklare innholdet i forholdsmessighetsvurderingen på.[78] Avhandlingen vil imidlertid benytte Ruis fire komponenter.

Avgjørelsen i Peters v. Nederland, som avhandlingen har allerede undersøkt, kan benyttes som et illustrerende eksempel på forholdsmessighetsvurderingen. I avgjørelsen ble det vurdert slik at saken ikke ble tillatt fremmet fordi selv om urinprøven var et inngrep i privatlivet var det et forholdsmessig inngrep.[79] Det hører med til faktum i saken at den klagende part var innsatt i fengsel, og de ansatte mistenkte ham for å være påvirket av narkotika. Inngrepet ble kjent forholdsmessig fordi kriminalitetsbekjempelse kan begrunne videre inngrep i privatlivet til en som er innsatt i fengsel enn andre som er frie. Det er ikke utrykt noe mer eksplisitt om EMDs forholdsmessighetsvurdering. Imidlertid kan vi se implisitt at det legitime formålet er kriminalitetsbekjempelse, og at urinprøve for å avdekke narkotikaovertredelser i fengsel var egnet til å vareta kriminalitetsbekjempelse. Det legges videre til grunn at EMD vurderte det slik at ingen andre mindre inngrep var egnet til å ivareta formålet samt at det var et proporsjonalt inngrep i forhold til den innsattes frihetsinteresser.

---

[75] Rui (2018) 4. avsnitt.
[76] Rui (2018) 6. avsnitt.
[77] Rui (2018) 4. avsnitt.
[78] Se for eksempel Aall (2018) s. 150 flg. og Jacobs, White og Ovey (2017) s. 359 flg. med videre henvisning til EMDs dom av 25. mars 1983 Silver v. United Kingdom.
[79] Peters v. Nederland i kjennelsens siste avsnitter.

2.3 Legalitetsprinsippets krav til presis lovhjemmel

Alle former for inngrep det offentlige kan gjøre overfor en privat part må ha grunnlag i lov, jf. Grl. § 113 og EMK art. 8 nr. 2. Dette er det *generelle legalitetsprinsippet*. Prinsippet har to sider ved seg, det *materielle* kravet og det *kvalitative* kravet.[80] Det materielle kravet sikter til at en lovhjemmel må være materiell, altså nedfelt i lov eller i forskrift medgitt av lov. Dette følger av ordlyden til Grl. § 113. Det kvalitative kravet (eller *klarhetskravet*) er et krav til tilstrekkelig klar og presis hjemmel, jf. EMD og høyesterettspraksis.[81] Jo større inngrep, jo større krav til hjemmelens presisjon.

Avhandlingen tar for seg en bestemmelse som er nedfelt i lov. Det er derfor ikke behov for å gå ytterligere i dybden på det materielle kravet samt forskjellen mellom borgernes beskyttelse etter Grunnloven vis-à-vis EMK. Avhandlingen vil dermed i det følgende fokusere på klarhetskravet.

Det generelle legalitetsprinsipp er i dag lovfestet i Grl. § 113. Før Grunnlovsendringen i 2014 var dette en «(...) sedvanebasert rettsregel med grunnlovs rang, såkalt *konstitusjonell sedvanerett*».[82] I motsetning til torturforbudet i Grl. § 93 har ikke lovgiver gitt uttrykk for at det generelle legalitetsprinsippet skulle utformes etter modell fra EMK.[83] Det var foreslått en ny Grl. § 115 etter modell fra EMK, som skulle være en generell begrensningshjemmel i de rettighetene som ikke var absolutte.[84] Denne generelle begrensingshjemmelen ble imidlertid ikke vedtatt. Ved Grunnlovsendringen i 2014 ville lovgiver grunnlovfeste legalitetsprinsippet uten at det skulle være noen endring i rettstilstanden. Prinsippet skulle synliggjøres som en reell skranke overfor myndighetsutøvere.[85]

Imidlertid må det sies at legalitetsprinsippet etter Grunnloven i sin kjerne har en svært lik formulering som sin motpart etter EMK art. 8 nr. 2, dersom man ser bort i fra kravet til et legitimt formål for inngrepshjemmelen etter EMK art. 8 nr. 2. Inngrepshjemmelen

---

[80] Ørnulf Øyen, *Straffeprosess*, 2. utgave, Bergen 2019 (Øyen 2019) s. 58 og Aall (2018) s. 145
[81] Acta avsnitt 30, fingeravtrykk-kjennelsen avsnitt 15 - 18 og Mirmotahari avsnitt 24. For klarhetskrav etter EMK se Jacobs, White og Ovey (2017) s. 345 med videre henvisning til EMDs dom av 26. mars 1987, *Leander v. Sweden*, 9248/81.
[82] Dok. nr. 16 (2011-2012) s. 246.
[83] Dok. nr. 16 (2011-2012) s. 246-250.
[84] Dok. nr. 16 (2011-2012) s. 72-74 og s. 260.
[85] Dok. nr. 16 (2011-2012) s. 248.

avhandlingen omhandler har formål om kriminalitetsbekjempelse. Kriminalitetsbekjempelse er et legitimt formål og byr således ikke på noen problematisering i avhandlingen.

Som allerede nevnt i avhandlingens metodekapittel er det et samspill mellom Grunnlovens menneskerettighetsbestemmelser og dens paralleller i EMK, jf. høyesterettspraksis.[86] I det følgende vil dermed begge bestemmelsene hva gjelder klarhetskravet drøftes under ett.

Bruk av makt ved ransaking av en person eller hans kropp vil alltid kreve hjemmel i lov.[87] Dette må også gjelde innhenting av biometrisk autentisering ved tvang for ransaking av datasystemer. Det følger derfor at klarhetskravet også må gjelde i slike tilfeller.

Etter norsk høyesterettspraksis har det skjedd en gradvis skjerping av dette kravet.[88] I 2014 uttalte Høyesterett: «Det gjelder også *kvalitative* krav: Loven må være tilgjengelig og så presis som forholdene tillater.».[89] Mens det i 2018 har utviklet seg til:

> «For lovtolkingsspørsmålet i saken har det imidlertid betydning at hjemmelskravet ikke etterlater nevneverdig rom for å begrense rekkevidden av beslagsforbudet i straffeprosessloven § 204 første ledd, jf. § 119 første ledd utover det som er forenlig med en alminnelig språklig forståelse av lovens ordlyd.»[90]

Etter høyesterettspraksis er det altså slik at det er svært lite rom for utvidende tolkninger. Det kan tenkes at et analogiforbud også gjelder innen straffeprosessen slik som i strafferetten. Et slikt syn kan støttes i juridisk teori: Frøberg gir uttrykk for at det kan tenkes en lignende innskjerping av legalitetsprinsippet i straffeprosessen slik som i strafferetten.[91] Hvis en inngrepshjemmel blir for vag eller vid kan det bli utfordrende for rettsanvendere. Forutberegnelighets- og demokratihensyn vil tale mot utvidende tolkninger av inngrepshjemler.

---

[86] Se avhandlingens metodekapittel og Maria-dommen avsnitt 57.
[87] Dette følger av Grl. § 102 første ledd andre setning og EMK art. 8 nr. 2 og Øyen (2019) s. 162 med videre henvisning til NOU 2004: 6 s. 43 og NOU 2005: 19 s. 26.
[88] Acta avsnitt 30, fingeravtrykk-kjennelsen avsnitt 15-18 og Mirmotahari avsnitt 24.
[89] Acta avsnitt 30.
[90] Mirmotahari avsnitt 24.
[91] Thomas Frøberg, «Nyere praksis om det strafferettslige legalitetsprinsippet», Jussens venner, 01-02/2015 (volum 50) s. 46 - 71 på s. 68 flg.

2.4 Selvinkrimineringsvernet

Etter strpl. § 232 første ledd er det slik at en som er siktet ikke har plikt til å forklare seg under etterforskningen. Det samme gjelder for forklaringer i retten etter strpl. § 90. Det følger også av strpl. § 225 og anklageprinsippet, det er *politiets* oppgave å utføre etterforskning, ikke den som er siktet eller andre forøvrig. At en siktet ikke bidrar til å klare opp mistanken mot seg kan tale imot den siktede. Imidlertid vil dette ikke ha konsekvens for avhandlingens tema, det vil derimot retten til å forholde seg taus ha. Selvinkrimineringsvernet er i den juridiske teori ofte brukt som et samlebegrep for to separate rettigheter, nemlig retten til å forholde seg taus og retten til å ikke bidra til egen domfellelse.[92] Rui påpeker at det er «(...) ikke alltid noen nødvendig sammenheng mellom [dem]».[93] Rui karakteriserer rettighetene som «grunnleggende rettsstatsprinsipper».[94] Retten til å forholde seg taus forankres i strpl. § 232 første ledd.

Strpl. § 232 første ledd lyder slik:

> «Før det foretas avhør av mistenkte, skal han gjøres kjent med hva saken gjelder, og at han ikke har plikt til å forklare seg.»

Etter sin ordlyd er det lite som tilsier at selvinkrimineringsvernet etter bestemmelsen vil aktiveres ved ransaking av datautstyr. Imidlertid har Høyesterett etablert at selvinkrimineringsvernet også strekker seg til at en siktet ikke skal «(...) på annen måte bidra til sin egen straffellelse.»[95] En siktet kan for eksempel ikke pålegges å utlevere bevis til politiet, jf. strpl. § 210. Skal politiet ha bevis må dette søkes etter ved hjelp av ransakelse og beslag. Imidlertid er den siktede pliktig å stille sin egen kropp til disposisjon for fysisk eller psykisk granskning, jf. strpl. §§ 157, 158, 160, 161 og 165.

Til tross for at EMK ikke har noen eksplisitt bestemmelse for selvinkrimineringsvernet, er det en relevant bestemmelse for dette vernet i EMK. Etter EMK art. 6 nr. 1 «(...) har enhver rett til en rettferdig (...) rettergang (...)». EMK art. 6 er en vid bestemmelse som skal sikre rettferdig rettergang for alle i en straffesak, men nøyaktig innholdet i en rettferdig rettergang

---

[92] Jon Petter Rui, «Om retten til å forholde seg taus og retten til ikke å måtte bidra til egen domfellelse», *Tidsskrift for rettsvitenskap*, 01/2009 (volum 122) s. 47-69 (Rui 2009) s. 48, første avsnitt i punkt 2. Begrepsbruk.
[93] Rui (2009) s. 48, andre avsnitt i punkt 2. Begrepsbruk.
[94] Rui (2009) s. 47, første avsnitt i punkt 1. Temaet.
[95] Rt. 2007 s. 932 avsnitt 17 med videre henvisning til rt. 1999 s. 1269.

er ikke nærmere gitt uttrykk for i bestemmelsens ordlyd. Det er imidlertid sikker rett at i retten til en rettferdig rettergang etter EMK art. 6 nr. 1 inneholder et slikt selvinkrimineringsvern.[96]

I Funke v. Frankrike etablerte EMD at selvinkrimineringsvernet inngår i EMK art. 6 nr. 1. Sakens faktum omhandlet en siktet som franske myndigheter påla å oppgi dem kontoutskrifter for utenlandske bankkonti i den pågående etterforskningen mot ham. Franske myndigheter ila mulkt for hver dag den siktede nektet å produsere dokumentene. EMD kom frem til at franske myndigheter brøt EMD art. 6 nr. 1 ved at de forsøkte å tvinge den siktede til å kunne inkriminere seg selv ved å være nødt å utlevere dokumentasjonen som kunne være realbevis i en eventuell sak mot ham.[97]

I Saunders v. Storbritannia konstaterte EMD at selvinkrimineringsvernet også omfattet retten til å forholde seg taus. Denne retten til å forholde seg taus gjelder også i forhold til ytringer og forklaringer som ellers ikke er inkriminerende.[98]

Imidlertid konstaterte EMD også følgende:

> «The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing.»[99]

Det skilles derfor mellom retten til å forholde seg taus og bevis som eksisterer uavhengig av en persons vilje, der sistnevnte kan innhentes med tvangsmidler uten at selvinkrimineringsvernet er brutt.

---

[96] Rt. 1999 s. 1269 nest siste avsnitt s. 1271 med videre henvisning til EMDs dom av 25. februar 1993, *Funke v. France*, 10828/84 (Funke v. Frankrike) og EMDs dom av 17. desember 1996, *Saunders v. United Kingdom*, 19187/91 (Saunders v. Storbritannia).
[97] Funke v. Frankrike avsnitt 44.
[98] Saunders v. Storbritannia avsnitt 71-74.
[99] Saunders v. Storbritannia avsnitt 69.

Selvinkrimineringsvernet vil kunne ha innvirkning på hvilke typer biometrisk autentisering som kan påtvinges. Nærmere bestemt vil vernet kunne være en skranke for tvang av innhenting av visse typer biometriske markører. Dette er også noe som forarbeidene har tatt høyde for:

> «Imidlertid kan noen former for biometrisk autentifisering 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».[100]

Selvinkrimineringsvernet gjelder imidlertid i utgangspunktet kun for mistenkte, siktede og tiltalte. Øvrige vitner har ikke forklaringsplikt til politiet, jf. strpl. § 230, med de unntak som følger av bestemmelsen. Overfor retten, har imidlertid vitner som hovedregel forklaringsplikt, og kan bare påberope selvinkrimineringsvernet dersom forklaringen eller utleveringen av bevis vil kunne implisere dem i en forbrytelse som medfører straff, jf. strpl. § 108, jf. §§ 123 første ledd og 210. Retten kan imidlertid likevel pålegge et vitne forklaring etter nærmere fastsatte vilkår. Avhandlingen vil ikke drøfte unntaksvilkårene nærmere.

Et spørsmål som kan stilles opp er om hvorvidt juridiske personer er beskyttet av selvinkrimineringsvernet. Høyesterett har åpnet for at dette er tilfelle på ulovfestet grunnlag.[101] Avhandlingen legger til grunn at juridiske personer er beskyttet av selvinkrimineringsvernet uten noen videre drøftelse av problemstillingen fordi det ligger utenfor avhandlingens tematikk. Imidlertid kan det nevnes at denne problemstillingen er drøftet i forslag til ny straffeprosesslov, hvor utvalget legger til grunn at selvinkrimineringsvernet ikke skal kunne påberopes av juridiske personer i fremtiden.[102]

Den mest aktuelle biometriske markøren som vil kunne tenkes å være påvirket av selvinkrimineringsvernet er stemmegjenkjenning. Dette vil bli behandlet nærmere i avhandlingens kapittel 3.4.3.

---

[100] Prop. 106 L (2016-2017) s. 10 og 11.
[101] Rt. 2011 s. 800 avsnitt 80.
[102] NOU 2016:24 s. 213, for utvalgets redegjørelse av gjeldende rett se s. 209 flg.

3 Innholdet i Strpl. § 199 a

Dersom et datasystem ransakes og det er låst kreves det egen hjemmel for å kunne låse det opp siden det er ett inngrep i privatlivet. Dette følger av Grl. §§ 113 og 102 samt EMK art. 8, som er gjort rede for i redegjørelsene for privatlivet og legalitetsprinsippets krav til klarhet. Det er strpl. § 199 a som hjemler nettopp dette. Bestemmelsen sikrer at politiet kan åpne opp datasystemer for å kunne ransake dem for bevis.

Etter sin ordlyd gir strpl. § 199 a første ledd politiet hjemmel til å kunne pålegge alle som har «befatning» med «datasystemet» å gi tilgang til det, enten med «nødvendige opplysninger» eller «biometrisk autentisering». Pålegget må være forholdsmessig, og mindre inngripende tiltak skal alltid benyttes dersom dette er mulig, jf. strpl. § 170 a, EMK art. 8 nr. 2 og politiloven § 6.[103] Se også avhandlingens redegjørelse for forholdsmessighet.

Kapitlet vil i det videre tolke begrepene befatning, datasystem, nødvendige opplysninger og biometrisk autentisering. Så vil det i 3.5 bli drøftet konsekvensen av at et pålegg nektes etterkommet. I 3.6 vil avhandlingen belyse hvem som innehar kompetanse til å utøve tvang. Til sist vil det i 3.7 bli drøftet jurisdiksjon.

3.1 Befatning

Etter naturlig språklig forståelse må «personkretsen»[104] som innehar befatning omfatte alle som har tilgang til datasystemet. Det betyr at eieren av datasystemet, den siktede som er bruker av det og andre personer som måtte inneha tilgang, inngår i denne personkretsen. Arbeidsgiver, IT-ansvarlige på jobb og andre brukere av datasystemet (enten på jobb eller i hjemmet) er, etter en ordlydstolkning, del av personkretsen.

Forarbeidene støtter opp om en slik forståelse av begrepet:

> «Det følger at utkastet til *første ledd* at opplysningsplikt kan pålegges enhver som har befatning med datasystemet. Ved ransaking av datasystemer til virksomheter med eget IT-personale vil det være naturlig å rette pålegget mot

[103] Lov 4. august 1995 nr. 53 om politiet (politiloven).
[104] Avhandlingen vil benytte dette begrepet slik det gjøres i Ingvild Bruce og Geir Sunde Haugland, *Skjulte tvangsmidler*, 2. utgave Oslo 2018 (Bruce og Haugland 2018) s. 187 flg.

> disse personene. Personkretsen som kan pålegges opplysningsplikt er imidlertid ikke begrenset til bestemte profesjonsgrupper.»[105]

Etter forarbeidene ser man altså at dersom det finnes «IT-personale» bør pålegget helst rettes mot slike, istedenfor andre personer som måtte ha befatning.

Implikasjonen av at IT-personale er del av personkretsen, er at tilgang ikke nødvendigvis må innehas, men også kan skaffes. Det tolkes derfor slik at alle som kan lovlig skaffe tilgang på datasystemet er del av personkretsen med befatning og kan gis pålegg om å gi politiet tilgang.

Et relevant spørsmål er om hvorvidt politiet kan gi pålegg til en person om å skaffe tilgangen *ulovlig*. Etter bestemmelsens ordlyd, kan imidlertid ikke utenforstående «hackere»[106] ta del i personkretsen som har befatning. Dette spørsmål er ikke vurdert verken i rettspraksis eller forarbeider. Ettersom en utenforstående ikke har befatning med datasystemet må slike hackere være utelukket å benytte i ransakingen til tross for at de har nok kunnskap til å skaffe seg befatning. Subsidiært vil ikke dette la seg gjøre all den tid strpl.§ 199 a ikke er tilstrekkelig presis for å hjemle dette, jf. klarhetskravet. Dessuten kan politiet ved hjelp av de generelle ransakings- og beslagshjemmelene benytte seg av Kripos` eller Økokrims datateam for å bryte seg inn i systemer som ikke kan åpnes ved andre midler.

Det finnes ingen rettspraksis der spørsmålet om hvem som har befatning har kommet på spissen. Imidlertid finnes det rettspraksis som kan gi en *indirekte* innsikt i hvordan Høyesterett tolker begrepet i kjennelsen inntatt i HR-2019-610-A, heretter Tidalkjennelsen. Her ønsket Økokrim tilgang til å ransake Tidal Music AS sine dataterminaler. Firmaet var ikke siktet. Den siktede var ansatt i firmaet og det var ønskelig å lete etter bevis for etterforskningen av ham. Lagmannsretten dømte i favør Økokrim, og Høyesterett forkastet anken enstemmig. Av Høyesterett var det ikke uttrykt noe *obiter dictum* om hvem som er å anse som å inneha befatning. Det *kan* derfor tolkes slik at, Høyesterett ikke anser det som

[105] Ot. prp. nr. 40 (2004-2005) s. 34.
[106] Det finnes mange definisjoner på begrepet «hacker», for avhandlingens del holder det med å benytte seg av Sundes definisjon. Se Sunde (2006) s. 19 fotnote 9. Lik Sunde vil ikke avhandlingen sondre forskjellen mellom hacker og cracker, de går begge under ett.

problematisk at et firma kan gis pålegg om å låse opp utstyr som en av deres ansatte bruker. En slik tolkning støttes av juridisk teori.[107]

Sammenlignet med bestemmelsens parallell i forslag til ny straffeprosesslov er det en forskjell i rekkevidden av hvem som innehar befatning. Etter § 14-6 første ledd i forslag til ny straffeprosesslov kan et pålegg rettes mot enhver som har «vitneplikt i saken» for å utlevere nøkler, koder, passord og lignende.[108] Dette kan i noen tilfeller være videre enn personkretsen som innehar «befatning», og i andre tilfeller kan det være en snevrere personkrets. Eksempelvis har ikke en siktedes nære familie vitneplikt i en sak.[109] Slike personer vil dermed ikke kunne rettes et pålegg mot, noe de kan i dag. På den andre siden kan det tenkes tilfeller der en person ikke innehar befatning med et datasystem men innehar vitneplikt. Det er imidlertid nærliggende å tro at slike personer ikke vil ha tilgang til datasystemet uansett.

Etter forslag til ny straffeprosesslov § 14-6 annet ledd kan enhver pålegges eller tvinges til å medvirke til biometrisk autentisering. Dette er en betydelig utvidelse av personkretsen som kan pålegges og benyttes tvang mot. Imidlertid er det vanskelig å se for seg tilfeller der en person som ikke innehar befatning skulle ha tilgang til et system ved hjelp av biometrisk autentisering. Det eneste tilfelle som kan tenkes er at en tvilling til en siktet kan bli tvunget til å «lure» ansikts-id på sitt søskens datasystem. Dette er noe som ikke er hjemlet i strpl. § 199 a.

3.2 Datasystem

Begrepet «datasystem» er ganske vidt og må etter en ordlydstolkning forstås som ethvert system der data behandles eller lagres. Dette kan være alt fra enheter som pc, mobil og nettbrett, til eksterne harddisker, rutere, biler og kjøleskap.

Bakgrunnen for et slikt vidt begrep ligger i at lovgiver har gitt uttrykk for at bestemmelsen skal være teknologinøytral.[110] I NOU 2003:27 side 10 gjøres det rede for utvalgets forståelse

---

[107] Bruce og Haugland (2018) s. 187 og Hans Kristian Bjerke, Erik Keiserud og Knut Erik Sæther, *Straffeprosessloven kommentarutgave*, Bekreftet à jour per 1. juli 2019 (Bjerke, Keiserud og Sæther 2019) kommentar til § 199 a 1. avsnitt punkt 3 lest 15. desember 2019 kl. 22.00 på juridika.no.
[108] NOU 2016:24 s. 47.
[109] Strpl. § 122.
[110] Ot. prp. nr. 40 (2004-2005) s. 34 og NOU 2003:27 s. 10.

av datasystem, jf. ordlyden i konvensjon om datakriminalitet art. 1 bokstav a. Utvalgets drøftelse om forståelsen av begrepet datasystem, er utførlig gjort og har høy presisjon. Utvalget legger til grunn at et nettverk av datasystemer også ligger innenfor bestemmelsens ordlyd. Dette medfører at enheter som knytter sammen andre enheter også faller innenfor, som for eksempel rutere og lignende. Det medfører dessuten at enheter som kommuniserer med andre enheter også faller innenfor selv om de ikke nødvendigvis lagrer data. Slike enheter kan for eksempel være smart tv-er, overvåkingskameraer, trådløse hodetelefoner, nyere kjøleskap og biler.

Det er imidlertid ikke alt som er problematisert eller tatt høyde for i forarbeidene. Flere brukere per enhet, i hjemmet eller på jobben, og andre personvernhensyn har medført at man i dag har teknologi for flere lag med sikkerhet. Der ett lag trengs for å låse opp selve datasystemet, kan ett annet lag beskytte innholdsdata. Det kan derfor problematiseres om ordlyden «datasystemet» strekker seg til også å gjelde innholdsdata, eller om det kun gjelder tilgangen til å komme seg inn i hovedsystemet.

3.2.1 Om ordlyden datasystem også omfatter innholdsdata

Med ordlyden «datasystemet», kan det etter en naturlig språklig forståelse bare være tilgangen for å åpne selve systemet, og ikke innholdsdata som kan pålegges åpnet. Dette begrunnes med bestemmelsens utforming i bestemt form.

I Ot. prp. nr. 40 (2004-2005) s. 34 henvises det til det tidligere utvalgets forståelse av begrepet.[111] Dette går frem i proposisjonens første avsnitt i kommentar til § 199 a. Imidlertid presiseres det at: «[m]ed tilgang til datasystemet menes også tilgang til data som er lagret i systemet. Slik tilgang kan for eksempel kreve at politiet gis opplysninger om tilgangskoder.»[112]

En slik utvidende tolkning av ordlyden støttes i konvensjon om datakriminalitet. Norge forpliktet seg til å innføre hjemmel for at «competent authorities»[113] (her: påtalemyndigheten, og politibetjenter) skal kunne gi pålegg til enhver som har befatning med et «(...) computer

[111] NOU 2003:27 s. 10.
[112] Ot. prp. nr. 40 (2004-2005) s. 34.
[113] Konvensjon om datakriminalitet art. 19 nr. 1.

system or measures applied to protect the computer data therein (...).»[114] Med en slik ordlyd og ordlyden til art. 19 nr. 1 bokstav a, tolkes det slik at intensjonen bak konvensjonens artikkel var at politiet og påtalemyndigheten også kunne gi pålegg om å gi tilgang til innholdsdata. Det er imidlertid ikke nødvendigvis slik at dette er gjeldende rett.

I norsk rett er det slik at der det ikke er direkte motstrid mellom en internasjonal forpliktelse og norsk rett, presumeres norsk rett å harmonisere med den internasjonale forpliktelsen (presumsjonsprinsippet). Hverken strpl. § 199 a eller andre bestemmelser i straffeprosessloven utrykker noe eksplisitt om denne problemstillingen angående innholdsdata. Det *kan* derfor tolkes slik at etter presumsjonsprinsippet er det harmoni mellom den norske retten og konvensjonen.

På den andre side er det tale om et tvangsmiddel og klarhetskravet gjør seg gjeldende. Her må med andre ord den tolkning som følger av konvensjon mot datakriminalitet holdes opp mot klarhetskravet. Når klarhetskravet er Grunnlovfestet må det tas til inntekt for at dette må tillegges vekt. Problemstillingen er imidlertid drøftet i juridisk teori.

Bjerke, Keiserud og Sæther mener at forarbeidene kan tas til inntekt for at datasystem skal tolkes utvidende.[115] Som støtteargument viser Bjerke, Keiserud og Sæther til at, «En slik tolking er i tråd med den folkerettslige forpliktelsen bestemmelsen gjennomfører.»[116] Med dette siktes det altså til konvensjon om datakriminalitet art. 19 nr. 4, og argumentasjonen blir dermed at presumsjonsprinsippet er styrende. Bjerke, Keiserud og Sæther har imidlertid ikke drøftet klarhetskravet. Det er dermed uvisst hvordan de vurderer avveiningen mot dette kravet og presumsjonsprinsippet. Et slikt syn støttes av Georg Fredrik Rieber-Mohn og Haugland.[117] Imidlertid konstaterer både Rieber-Mohn og Haugland at hjemmelen strekker seg til å gjelde innholdsata uten noen argumentasjon eller redegjørelse.

Sunde er uenig med Bjerke, Keiserud og Sæther når det kommer til om hvorvidt forarbeidene taler for å tolke bestemmelsen utvidende.[118] Her må jeg si meg enig med Bjerke, Keiserud og

---

[114] Konvensjon om datakriminalitet art. 19. nr. 4.
[115] Bjerke, Keiserud og Sæther (2019) kommentar til § 199 a, punkt 2 avsnitt 2 lest 13. september 2019 på juridika.no. med videre henvisning til Ot. prp. nr. 40 (2004-2005) s. 34.
[116] Bjerke, Keiserud og Sæther (2019) kommentar til § 199 a, punkt 2 avsnitt 2.
[117] Peter Lødrup, Knut Kaasen og Steinar Tjomsland, *Norsk Lovkommentar*, bind 1, Oslo 2008 s. 1364 note 1252 og Geir Sunde Haugland, kommentar til straffeprosessloven, Gyldendals norsk lovkommentar, kommentar til § 199 a, note 1309, sist revidert 21.09.2016, lest 15. desember 2019 kl. 22.00.
[118] Sunde (2006) s. 272.

Sæther. Det går tydelig frem av forarbeidene at «Med tilgang til datasystemet menes også tilgang til data som er lagret i systemet.»[119]

Sunde gir imidlertid uttrykk for at «(...) den norske bestemmelsen er straffesanksjonert (...)» og at legalitetsprinsippet derfor oppstiller et særlig krav til hjemmelens klarhet.[120] Tidligere inneholdt strpl. § 199 a annet ledd en straffebestemmelse for andre enn siktede med henvisning til straffeloven 1902 § 339 nr. 1, der det var straffbart å nekte å oppgi informasjon som de var pålagt å oppgi til politiet.[121]

Lovgiver har imidlertid valgt å ikke følge opp strl. 1902 § 339 nr. 1 i ny straffelov. Sundes bok var skrevet i 2011, altså før den nye straffeloven hadde ikrafttredelse og før tidligere annet ledd i strpl. § 199 a ble fjernet 1. oktober 2015.[122] Straffbarheten ved å nekte å oppgi informasjon som var pålagt av politiet er med andre ord ikke gjeldende rett per i dag.

Imidlertid gjelder som nevnt det generelle legalitetsprinsippet og derfor klarhetskravet, jf. Grl. § 113 og EMK art. 8 nr. 2.[123] Sundes argumentasjon er med andre ord like gyldig i dag som det var i 2011. Kanskje er det omså et enda sterkere argument i dag enn da Sunde skrev boken, siden legalitetsprinsippet er grunnlovfestet i Grl. § 113 etter Grunnlovsendringen i 2014, og det har skjedd en innstramming av klarhetskravet.

Sunde kommer imidlertid med motargumenter, og uttrykker at hjemmelen ble vedtatt samtidig med strl. 1902 § 145b. Sunde legger til grunn at strl. 1902 § 145 b omfatter også spredning av koder som kan dekode innhold, og at sammenhengen i regelverket tilsier at strl. § 199 a må tolkes på samme måte.[124] Sunde kommer ikke med noen konklusjon med sin drøftelse, slik at hennes vektlegging mellom presumsjonsprinsippet og legalitetsprinsippet er uvisst. Hennes drøftelse fremstår imidlertid som mer nyansert og gjennomtenkt enn øvrige kilder gjengitt i dette kapittel.

Situasjonen er altså at lovteksten ikke er presis. Forarbeidene og konvensjonens ordlyd taler i retning utvidende tolkning. Det samme gjør lovens system. Imidlertid taler Grunnloven, EMK og rettskildeprinsipper for at hjemmelen ikke er tilstrekkelig presis, mens det i juridisk teori

---

[119] Ot. prp. nr. 40 (2004-2005) s. 34.
[120] Sunde (2006) s. 272.
[121] Lov 22. mai 1902 nr. 10 Almindelig borgerlig straffelov (strl. 1902).
[122] Lov 19. juni 2015 nr. 65 om ikraftsetting av straffeloven 2005 § 5, jf. strl. § 411.
[123] Se 2.3 om klarhetskravet.
[124] Sunde (2006) s. 273.

tas høyde for tolkning i begge retninger. Det finnes ingen rettspraksis der dette spørsmålet er satt på spissen. Imidlertid legger avhandlingen til grunn at ordlyden etter strpl. § 199 a ikke er tilstrekkelig presis, og at kravet til en presis og klar lovhjemmel må tillegges avgjørende vekt all den tid klarhetskravet er forankret i Grunnloven.

For å oppsummere hvordan begrepet «datasystem» skal tolkes: Det er en vid og teknologinøytral term. Begrepet inkluderer alle redskaper som lagrer og behandler data også i nettverk. Begrepet begrenses imidlertid kun til å gjelde tilgang til systemet, ikke underliggende innholdsdata. Dette medfører for eksempel at ny teknologi som kryptovaluta eller «blockchain» (transaksjonskjede på norsk) ikke kan hjemles åpnet dersom dette også er låst.[125]

I forslag til ny straffeprosesslov er strpl. § 199 a speilet i § 14-6:

> «Påtalemyndigheten kan pålegge enhver som har vitneplikt i saken, å utlevere nøkler, koder, passord og lignende for å få *tilgang til* sted eller *datasystem* når det er nødvendig for å gjennomføre et tvangstiltak.»[126]

Ved å bruke ordlyden «tilgang til (...) datasystem» legger avhandlingen til grunn at den nye bestemmelsen noe mer klar. Det benyttes ikke bestemt form om datasystem (altså «et datasystem» og «datasystemet») som det skal gis tilgang til.[127] Dette er en svært liten nyanse, men en viktig en. Imidlertid har ikke lovgiver reflektert over verken problemstillingen eller nyanseforskjellen på noe vis i forarbeidet.

Det er også foreslått en bestemmelse § 15-8. Bestemmelsens tredje ledd lyder:

> «Nekter en person å etterkomme rettskraftig pålegg om å gi forklaring, kan det besluttes fengslig forvaring til plikten oppfylles. Det samme gjelder dersom pålegg etter §§ 14-6 første ledd, 19-6 eller 19-7 ikke etterkommes. Vedkommende kan likevel ikke holdes fengslet i mer enn 3 måneder i samme sak eller i annen sak om samme forhold.»[128]

---

[125] Avhandlingen legger til grunn Store norske leksikon forståelse av begrepet transaksjonskjede. Se Svein Johan Knapskog, "Transaksjonskjede", Store norske leksikon (2018), https://snl.no/transaksjonskjede.
[126] NOU 2016:24 s. 47, § 14-6 første ledd første setning, min kursivering.
[127] Sammenlign ordlyden i strpl. § 199 a første ledd og NOU 2016:24 s. 47 sitt forslag til § 14-6.
[128] NOU 2016:24 s. 49, § 15-8 tredje ledd .

Forslag til ny bestemmelse åpner altså for en slags straffesanksjon der en person nekter å etterkomme et pålegg. Dersom lovgiver gjør det slik at det kan sanksjoneres med fengsel å ikke etterkomme et pålegg, må det stilles svært høye krav til hjemmelens klarhet.

3.3 Nødvendige opplysninger

Bestemmelsens ordlyd gir tilgang til å ransake datasystemer. Slike systemer kan være låst. Det er vil derfor være nødvendig for politiet å få tilstrekkelig med opplysninger for hvordan systemet skal åpnes. Med ordlyden «nødvendige opplysninger» ser vi igjen at lovgiver har valgt å benytte begrep som favner vidt. Lovgiver kunne ha valgt begrepet «passord», men har da tilsynelatende ønsket å gå for en videre begrepsbruk.

Etter ordlyden vil da for eksempel svar på «sikkerhetsspørsmål» ved glemt passord også rammes.[129] Å informere om systemets svakheter for å utnytte dem, kan også tenkes å rammes av ordlyden, dersom eksempelvis IT-personell ikke sitter med passord. Systemets svakheter kan ligge i å utnytte dem for hacking eller omgåelse av sikkerhetsbeskyttelsen. Dette er tross alt informasjon som kan være nødvendig for å få låst opp et gitt datasystem. Imidlertid begrenses bestemmelsen etter sin ordlyd til kun å gjelde det som er *nødvendig*.

I forarbeidene til bestemmelsen er begrensingen av nødvendig informasjon uttrykkelig nevnt. Det fremgår at «[e]n person kan bare pålegges å gi 'nødvendige' opplysninger, dvs. opplysninger som er påkrevd for at politiet skal få tilgang til datasystemet.»[130] Med andre ord kan alle typer opplysninger som tjener til å åpne opp et gitt datasystem pålegges utlevert, forutsatt at de er nødvendig for å få det åpnet.

Imidlertid kan datasystemer være beskyttet med et adgangskort i tillegg til passord eller biometrisk autentisering. Det kan derfor problematiseres om det kan innfortolkes noen utleverings- eller aksjonsplikt for den som har befatning om å utlevere adgangskortet til politiet eller å bruke det.

---

[129] Et sikkerhetsspørsmål er en funksjon som tillater personer som har glemt sitt passord for en tjeneste eller system å kunne sette passordet til side eller tilbakestille det ved å svare på et spørsmål som bare personen kjenner til, oftest lages dette i kombinasjon med første gang man lager et passord.
[130] Ot. prp. nr. 40 (2004-2005) s. 34.

Etter bestemmelsens ordlyd må det i det minste være slik at politiet kan kreve informasjon om hvordan prosedyren er for å låse opp datasystemet. Altså hvor og hvordan kortet skal brukes for å låse opp systemet.

For en som er siktet stiller det seg slik at det ikke kan være noen utleveringsplikt av adgangskort, dette følger av selvinkrimineringsvernet, jf. Funke v. Frankrike.[131] Imidlertid kan politiet uansett ransake etter og ta beslag av slike adgangskort, jf. strpl. § 192.

For andre som ikke er siktet men innehar befatning stiller det seg noe annerledes, selvinkrimineringsvernet kan gjøre seg gjeldende her slik som hos siktede. Dette kan for eksempel være at det finnes noe på datasystemet som er inkriminerende, eller det kan virke inkriminerende bare det at vedkommende har et slikt adgangskort. I de tilfeller det ikke vil virke inkriminerende, er det ikke gitt i seg selv etter ordlyden til strpl. § 199 a at det finnes en slik utleveringsplikt. Forarbeidene til bestemmelsen har ikke problematisert dette i noen grad og spørsmålet er ikke kommet på spissen i noen rettsavgjørelser. Imidlertid kan det argumenteres med at et slikt adgangskort vil være satt i nettverk med datasystemet og kan kommunisere med det. Som allerede konkludert med i avhandlingens redegjørelse for begrepet datasystem er slike enheter også å anse som et datasystem. Det kan dermed ledes ut en utleveringsplikt for et adgangskort i slike tilfeller som nevnt over. Politiet kan også her ransake etter og ta beslag etter strpl. § 192 tredje ledd nr. 3.

Det er konkretisert i forslag til ny straffeprosesslov § 14-6 første ledd slik utleveringsplikt.[132] Her er det foreslått en ordlyd som eksplisitt nevner utlevering av «(...) nøkler, koder, passord og lignende (...)». Det er imidlertid ikke drøftet denne utleveringen i noen nevneverdig grad forholdet mellom gjeldende rett og det nye forslaget i forhold til adgangskort.

3.4 Biometrisk autentisering

Et datasystem trenger ikke nødvendigvis være låst med passord eller lignende. Datasystemer kan være låst ved biometrisk autentisering. Fingeravtrykk-kjennelsen gjorde det synlig at dersom politiet skal kunne tvinge noen til å medvirke til å åpne et system med biometrisk

[131] Se redegjørelse i 2.4.
[132] NOU 2016:24 s. 47.

autentisering må det være en tilstrekkelig klar hjemmel for dette. Som allerede nevnt i innlendingen implementerte lovgiver en endring i første ledd for også å gjelde *biometrisk autentisering*.[133] Biometrisk autentisering er gjenkjenning og godkjenning av biometriske markører, i motsetning til et objekt (nøkkelkort) eller kunnskapsbasert godkjenning (passord). En biometrisk markør er et samlebegrep på egenskaper ved ens egen kropp som er helt unik for deg som individ. Eksempler på biometriske markører kan være DNA, fingeravtrykk, ansiktsgeometri, handgeometri eller ganglag.

Lovgiver *kunne* begrenset seg til å benytte begrepet «fingeravtrykk» ettersom det var i utgangspunktet dette som var avdekt mangel ved og nødvendighet for å endre i lovverket. Igjen ønsket lovgiver en videre begrepsbruk enn det som var nødvendig på lovendringstidspunktet. Teknologinøytralitet har med andre ord vært viktig for lovgiver i forhold til hvilke typer biometrisk autentisering som er aktuelle også i fremtiden. Det er uttrykt eksplisitt i forarbeidene at «[b]estemmelsen er teknologinøytral og omfatter ethvert datasystem og enhver form for biometrisk autentisering.»[134] Det er ikke uttrykt noe ytterligere om teknologinøytralitet i forarbeidets drøftelse av hvilke biometriske kjennetegn som skulle rammes av bestemmelsen hva gjelder pålegget. Ved tvang vil det være hensyn som gjør seg gjeldende for å skille mellom typer biometriske markører. Dette er tatt høyde for i forarbeidene: «Imidlertid kan noen former for biometrisk autentifisering etter sin art være utelukket fra gjennomføring ved tvang.»[135]

Til nå har det ikke vært spesielt aktuelt å benytte tvang etter strpl. § 199 a for andre biometriske markører enn fingeravtrykk og ansiktsgjenkjenning. Slike markører byr ikke på særlige problemer knyttet til bestemmelsens skranker da det ikke kan problematiseres om en eventuell behandling vil være umenneskelig eller nedverdigende. Innhenting av fingeravtrykk og ansiktsgjenkjenning vil klart utgjøre ett inngrep i privatlivet.[136] Imidlertid fremstår et slikt inngrep som forholdsmessig: Det er egnet til å vareta kriminalitetsbekjempelse, det vil sannsynligvis være nødvendig for å låse opp systemet og det fremstår proporsjonalt i forhold til en situasjon ved ransakelse. Det legges til grunn den samme vurderingen hva gjelder DNA-innsamling, det er verken smertefullt eller vanskelig å samle inn DNA ved tvang, for

[133] Prop.106 L (2016-2017) s. 10.
[134] Prop.106 L (2016-2017) s. 10.
[135] Prop.106 L (2016-2017) s. 11.
[136] Se avhandlingens redegjørelse i 2.2.

eksempel med spytt eller hårstrå. Forarbeidene har kun vurdert om DNA-innsamling strider mot selvinkrimineringsvernet, og har ikke vurdert dette opp mot forholdsmessighetsvurderingen etter EMK. art. 8.[137] Det utrykkes imidlertid at i et fremtidsrettet perspektiv kan være aktuelt å benytte tvang for å innhente DNA, dette var intensjonen til departementet.[138]

Et personvernhensyn som kan problematiseres er om hvorvidt norske myndigheter har adgang til å lagre den biometriske autentiseringen i en database for senere bruk.

Etter strpl. § 199 a sin ordlyd er det ingenting som tilsier at myndighetene har adgang til å lagre de data de samler inn ved bruk av biometrisk autentisering. Etter forarbeidene er myndighetene avskåret fra å lagre slikt materiale per i dag.[139]

Til motsetning er det i forslag til ny straffeprosesslov ikke drøftet et slikt forbud.[140] Imidlertid vil klarhetskravet sette en skranke for å kunne tillate slik lagring. Verken nåværende strpl. § 199 a eller den parallelle bestemmelsen i forslaget til ny straffeprosesslov inneholder noe konkret om dette etter sine ordlyder, det kan heller ikke hjemles ved politiets alminnelige handlefrihet, all den tid det utgjør et inngrep i privatlivet.

Visse typer biometriske markører kan problematiseres, med hvordan de skal kunne inndrives med tvang. I det følgende vil det drøftes tre slike biometriske markører; irisgjenkjenning, ganglagsgjenkjenning og stemmegjenkjenning. De er aktuelle eksempler fordi de kan komme til å bli implementert innen rimelig nær fremtid.[141] De representerer også problemstillinger som vil være ganske lik øvrige biometriske markører. For eksempel er irisgjenkjenning teknologisk forskjellig fra retinaskanning, men i forhold til skrankene er problemstillingen identisk.

[137] Prop.106 L (2016-2017) s. 3.
[138] Prop.106 L (2016-2017) s. 4 med videre henvisning til departementets høringsnotat.
[139] Prop. 106 L (2016-2017) s. 11.
[140] NOU 2016:24.
[141] Irisgjenkjenning er allerede i bruk på telefoner i dag, se uttalelse i prop.106 L (2016-2017) s. 8 og 9. Ganglagsanalyse er allerede tatt i bruk av kinesiske myndigheter for kriminalitetsbekjempelse se Giordano (2019). Stemmegjenkjenning har som nevnt også allerede vært i bruk, se Rossen (2019).

3.4.1 Irisgjenkjenning

Ved irisgjenkjenning benyttes en persons unike mønster på iris for å skille den autoriserte personen fra andre personer. Forarbeidene har i svært liten grad problematisert irisgjenkjenning. Tvert imot finnes uttalelser som tilsynelatende finner irisgjenkjenning som lite problematisk:

> «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.»[142]

Imidlertid nyanseres dette noe med etterfølgende setning:

> «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»[143]

Irisgjenkjenning må nødvendigvis gjøres med at personens øyne er åpne. Dersom en person ikke ønsker å åpne opp sine øyne må det benyttes tvang for å få øynene åpnet. Å tvinge opp noens øyne mot sin vilje, bør gjøres med medisinsk utstyr for å sikre at den som blir tvunget ikke tar skade av fingre eller negler som kan fysisk skade eller forårsake infeksjon på øyet. Slik medisinsk utstyr tar heller ikke høyde for at personen ser opp slik at iris ikke vises til tross for at øyelokkene holdes åpne.

Det er her ikke vanskelig å se hvor lett man kan ende i en situasjon der en person blir utsatt for både nedverdigende og umenneskelig behandling for å få låst opp et datasystem ved irisgjenkjenning. I motsetning til narkotikaposer i kroppens hulrom, som i Jalloh v. Tyskland, er det vanskelig å tenke seg tilfeller der en slik tvang kan gjøres for å redde en persons liv eller helse. Den primære årsaken for å tvinge noens øyne opp vil derfor være for å samle inn bevis. Som konkludert med i avhandlingens delkapittel 2.1 kan det derfor ikke unnskyldes noen form for tvangsmessig medisinsk inngrep, jf. EMD praksis.

---

[142] Prop.106 L (2016-2017) s. 11.
[143] Prop.106 L (2016-2017) s. 11.

Uansett om personen ikke blir utsatt for nedverdigende eller umenneskelig behandling vil innhenting av denne formen for biometrisk autentisering utgjøre et inngrep den fysiske integritet. EMK art. 8 vil derfor også sette en skranke. Det legges til grunn at inngrepet er egnet til å ivareta kriminalitetsbekjempelse som et legitimt formål og at det vil være nødvendig etter omstendighetene forutsatt at ikke andre mindre inngripende tiltak kan utføres. Imidlertid vil proporsjonalitetsvurderingen fortsatt være nødvendig. Denne proporsjonalitetsvurderingen vil bero på en konkret helhetsvurdering i den gitte situasjon.

3.4.2 Ganglagsgjenkjenning

Ganglagsgjenkjenning er en annen type biometrisk markør som benytter en persons unike måte å gå på og skiller denne fra andres ganglag. En person kan filmes mens han går, og bevegelsesmønsteret hans analyseres. Personen må med andre ord gå slik han pleier under kontrollerte forhold for at man skal kunne få identifisert biometrien.

Hvis noen nekter å gå, er det vanskelig å se for seg et tilfelle der personen tvinges til å gå, ikke skulle være umenneskelig behandling eller i verste fall tortur. For hvordan skal man påtvinge noen å gå? Dette kan sikkert gjøres med forskjellige metoder, men slike metoder vil bære preg av å ha tilsvarende alvorlighetsgrad som «de fem teknikker» som var benyttet i Irland v. Storbritannia. Det er derfor vanskelig å se for seg at forbudet mot tortur, umenneskelig og nedverdigende behandling ikke skulle være en skranke overfor ganglagsgjenkjenning ved tvang.

Subsidiært vil en slik tvangsmessig innhenting av biometrisk data neppe gi adekvate resultater heller fordi det er rimelig lett å gå på en slik måte at det ikke samsvarer med hvordan man går til vanlig. Et slikt inngrep vil av den grunn ikke kunne være egnet å ivareta kriminalitetsbekjempelse heller, slik at det vil uansett være en ikke forholdsmessig behandling og vernet av den fysiske integritet vil også sette en skranke overfor denne typen tvangsmessig innhenting av biometrisk data.

3.4.3 Stemmegjenkjenning

Ved stemmegjenkjenning analyseres en persons stemme og sammenligner det med allerede lagret informasjon om kjennetegn ved personens stemme. Personen kan enten snakke fritt eller det kan være nødvendig med en forhåndsbestemt passfrase avhengig av teknologien.

Naturlig nok må en person dermed ytre seg for å aktivere stemmegjenkjenningen. Det å tvinge en person til å snakke eller ytre seg er problematisk i forhold til både selvinkrimineringsvernet og torturforbudet. Som allerede nevnt i avhandlingens drøftelse av selvinkrimineringsvernet, har lovgiver gitt uttrykk for at tvangsgjennomføring av stemmegjenkjenning ikke praktisk lar seg gjøre.[144] Nyutviklet teknologi kan imidlertid gjøre slik at dette kan problematiseres ytterligere. I den senere tid har man etterhvert kunnet samle på lydklipp av en person og syntetisere stemmen ved hjelp av datautstyr, også kaldt «deepfake».[145] Spørsmålet som kan oppstilles her er om politiet har adgang til å benytte lydklipp som er fritt tilgjengelig for å gjennomføre stemmegjenkjenning, enten direkte eller ved hjelp av deepfake. En slik benyttelse av lydklipp eller deepfake er ikke hjemlet i strpl. § 199 a eller straffeprosessloven forøvrig.

Ved direkte bruk av lydklipp som siktede for eksempel har på en åpen Facebook-profil kan muligens en stemme-autentisering åpnes direkte. Dersom lydklipp kan samles inn på åpne plattformer der siktede selv har delt det, må dette sees på som at det er bevis som eksisterer uavhengig av siktedes vilje og fører dermed ikke til budd av selvinkrimineringsvernet, jf. Saunders v. Storbritannia.[146] Problemstillingen er ikke drøftet verken i forarbeid, juridisk teori eller i EMD-praksis. Det er klart at politiet ikke har noen hjemmel for dette. Imidlertid kan dette bygges på den alminnelige handlefrihet som gjør det mulig for politiet å spane, observere, infiltrere og drive med bevisprovokasjon. Politiet har også mulighet til å samle inn søppel eller andre abandonerte gjenstander for eksempel for å innhente fingeravtrykk eller DNA.

---

[144] Prop.106 L (2016-2017) s. 11.
[145] Anders Brekke, «Utfordres av 'deepfakes': - vi er våre egne fiender», NRK, 24. februar 2019, https://www.nrk.no/norge/utfordres-av-_deepfakes__-_-vi-er-vare-egne-fiender_-1.14421262 infoboks om «deepfake», se for øvrig hele artikkelen for en forståelse av hva innholdet i begrepet er og hva det kan benyttes til. Siden det er en rykende fersk teknologi er det svært vanskelig å finne konkrete definisjoner og gode kilder. Teknologien er i sin startfase kan man si.
[146] Se 2.4 og Saunders v. Storbritannia avsnitt 69.

Det legges til grunn at en slik bruk ikke vil stride mot lov, på bakgrunn av informasjonens eksistens uavhengig av den siktedes vilje, politiets handlefrihet og at det ikke utføres noen slags tvang mot siktede.

Spørsmålet blir da om politiet kan benytte seg av deepfake dersom et lydklipp i seg selv ikke direkte er tilstrekkelig for å åpne datasystemet. Denne problemstilling er heller ikke drøftet i noen rettskilder. I et slikt tilfelle foretar politiet seg noe aktivt, til forskjell fra å passivt innhente informasjon som ligger åpent tilgjengelig. Informasjonen eksisterer dermed *ikke* uavhengig av siktedes vilje. Noen form for fysisk tvang eksisterer imidlertid ikke. Det avgjørende her må være at det ikke kan hjemles i verken den alminnelige handlefriheten eller noen eksplisitt hjemmel. Det legges dermed til grunn at det ikke er adgang for politiet å benytte deepfake for å syntetisere en persons stemme med formål å åpne et datautstyr som er beskyttet av biometrisk autentisering.

3.5 Konsekvensen av at pålegg nektes etterkommet

Som allerede nevnt, inneholdt straffeloven fra 1902 en straffebestemmelse dersom noen nektet å følge pålegget om å utlevere nødvendig informasjon til politiet.[147] Imidlertid ble ikke denne videreført i ny straffelov. Det naturlige spørsmålet blir derfor hvordan skal politiet kunne håndheve bestemmelsen for noen som nekter?

Til tross for at det i dag ikke kan straffes eller sanksjoneres på noen måte, kan det begjæres rettslig avhør etter strpl. § 108, jf. påtaleinstruksen §§ 15-1 og 15-2.[148]

Ut over dette kan man benytte tvang etter strpl. § 199 a annet ledd for biometrisk autentisering. Etter annet ledd er det imidlertid kun biometrisk autentisering som kan tvinges.

Annet ledd må tolkes i sammenheng med første ledds ordlyd. Dette går tydelig frem siden annet ledd henviser til første ledd. Dette gir forarbeidene også støtte for:

> «Tvangshjemmelen 'speiler' påleggshjemmelen. Tvangen kan benyttes overfor 'enhver som har befatning med datasystemet', jf. første ledd. Det omfatter

[147] Strl. 1902 § 339, se 3.2.1.
[148] Forskrift 28. juni 1985 nr. 1679 om ordningen av påtalemyndigheten (påtaleinstruksen). Se også Øyen (2019) s. 170 og 420.

> mistenkte og enhver tredjemann, uavhengig av om personen eier datasystemet.»[149]

Selv om lovgiver har gitt uttrykk for slik «speiling» av første ledd må dette modifiseres med hvilke biometriske autentiseringer som lar seg gjøre å utføre med tvang.[150] Her vil skrankene gjengitt i avhandlingens andre kapittel gjøre seg gjeldende. Dette er tilsynelatende også noe lovgiver har tenkt på: «I utgangspunktet gjelder bestemmelsen enhver form for biometrisk autentisering, herunder fingeravtrykk, annen avtrykksautentisering og irisgjenkjenning (...). Imidlertid kan noen former for biometrisk autentifisering etter sin art være utelukket fra gjennomføring ved tvang.»[151]

3.6 Om hvem som innehar kompetanse til tvangsbruk

Spørsmålet om hvem som har kompetansen til å bestemme tvang er regulert i strpl. § 199 a tredje ledd. Det er i utgangspunktet påtalemyndigheten som har kompetansen etter ordlyden, jf. første setning. Hvem som inngår i begrepet påtalemyndigheten er definert etter strpl. § 55 første og annet ledd.

Etter strpl. § 199 a tredje ledd andre setning har «politiet på stedet» kompetanse dersom det er «fare ved opphold». Med politiet på stedet må det forstås politibetjent.[152] I forarbeidene er det uttrykt at det opprinnelig var vurdert slik at det var politiet som hadde primærkompetansen, men etter uttalelser fra høringsinstansene ble det vurdert slik at primærkompetansen ble løftet til påtalemyndigheten i politiet, kombinert med hastekompetanse til politiet.[153]

Med ordlyden «fare ved opphold» forstås det fra konteksten og ordlyden forøvrig at det menes dersom det er fare for bevisforspillelse i påvente av avgjørelse fra påtalemyndigheten. Forarbeidene gir støtte til en slik tolkning.[154] Her uttrykkes at «[d]ersom det er fare for at bevismaterialet kan gå tapt i påvente av beslutning fra påtalemyndigheten, kan politiet på

[149] Prop.106 L (2016-2017) s. 10.
[150] Se 2.1 og 2.2.
[151] Prop.106 L (2016-2017) s. 10 og 11.
[152] Prop.106 L (2016-2017) s. 9.
[153] Prop.106 L (2016-2017) s. 9.
[154] Prop.106 L (2016-2017) s. 11.

stedet treffe beslutningen.»[155] Dersom politiet på stedet ser seg nødt til å bruke tvang, skal det straks meldes til påtalemyndigheten, jf. tredje ledd tredje punktum.

3.7 Jurisdiksjon

Den digitale verden kan som kjent strekke seg over landegrenser, det kan derfor problematiseres om hvorvidt norske myndigheter har adgang for å ransake eller granske data som ligger lagret i utlandet. Faktum i Tidalkjennelsen inneholdt en slik problemstilling og kjennelsen tjener derfor til å belyse temaet.

I Tidalkjennelsen var det konkrete spørsmålet om hvorvidt norsk politi kunne laste ned data som lå lagret på konsernets servere i utlandet ved hjelp av Tidal Music AS sine dataterminaler. Tidal Music AS er den norske avdelingen til Tidalgruppen. Tidalgruppen er en rekke selskaper med tilknytning til blant annet både USA og Norge.[156] Det var med andre ord et spørsmål om det var adgang til å benytte hjemmelen i strpl. § 199 a, eller om dette lå utenfor norske myndigheters jurisdiksjon.

Høyesterett kom frem til at det ikke fantes noen folkerettslig sedvane som begrenset norske myndigheters jurisdiksjon i slike tilfeller som faktum i saken.[157] Høyesterett gav videre uttrykk for at det fantes praksis fra utlandet som tilsa at slik ransaking var akseptert.[158] Høyesterett konkluderte med at slike spørsmål måtte vurderes selvstendig av norske rettsanvendere og under en helhetsvurdering av den konkrete sak.[159] Ved den konkrete vurderingen om norske myndigheter hadde anledning å ransake Tidals databaser i utlandet kom Høyesterett frem til at det var norske myndigheter som hadde besluttet ransaking, ransakingen var satt i verk på norsk territorium overfor en norsk firma.[160] Det medførte heller ikke at materialet i utlandet ble påvirket på noen måte siden det ble kun foretatt en kopi og derfor at ransakingen ikke på noen måte berørte suverenitetsprinsippet.[161] Konklusjonen ble derfor at politiet hadde anledning til å ransake.

---

[155] Prop.106 L (2016-2017) s. 11.
[156] Tidalkjennelsen avsnitt 2.
[157] Tidalkjennelsen avsnitt 58.
[158] Tidalkjennelsen avsnitt 59.
[159] Tidalkjennelsen avsnitt 61 og 62.
[160] Tidalkjennelsen avsnitt 65 – 68.
[161] Tidalkjennelsen avsnitt 70 og 71.

Det må derfor legges til grunn at dersom en ransaking ikke på noen måte sletter, sperrer eller på noen måte endrer data vil det være anledning å ransake og granske data som ligger i utlandet. Det må imidlertid være forutsatt at ransakingen utøves av norske myndigheter på norsk jord overfor et norsk rettssubjekt.

4 Avsluttende konklusjoner og vurderinger

4.1 Avhandlingens funn og konklusjoner

Det har vært lovgivers intensjon å gjøre bestemmelsen teknologinøytral. Både ved at den ikke skulle skille mellom ulike former for datasystemer og den skulle heller ikke lages noe skille mellom biometriske autentiseringer.

Ordlyden til strpl. § 199 a annet ledd opprettholder intensjonen om teknologinøytralitet med tanke på biometrisk autentisering. Imidlertid vil som nevnt skrankene etter Grl. §§ 93 og 102, strpl. § 90 og EMK art. 3, 8 og 6 nr. 1 sette grenser for hvor langt tvangen skal gå. Rent praktisk må det derfor gjøres et skille mellom ulike typer biometrisk autentisering når det er tale om tvang. Skrankene medfører imidlertid ikke at bestemmelsen *i seg selv* ikke er teknologinøytral når det gjelder biometrisk autentisering. Hjemmelen er ikke vag med tanke på hva som ligger i begrepet biometrisk autentisering. Når det er sagt er det ikke utelukket at det i et lengre fremtidsrettet perspektiv som kan medføre en viss vaghet. Dette kan komme i form av datasystemer som for eksempel tar i bruk hjernen. Hvor går da skillet mellom et datasystem og en kropp eller tanke? Men dette er nok ikke teknologi som kan komme i overskuelig fremtid, hvis i det hele tatt.

Avhandlingen har også funnet at bestemmelsen ikke skiller mellom ulike datasystemer som sådan. Etter mitt syn vil teknologi som kommer i all overskuelig fremtid dekkes under ordlyden datasystem. Den er ikke vag slik at det skal kunne misforstås hvilke systemer som kan tenkes rammet. Imidlertid skiller strpl. § 199 a mellom forskjellige lag av beskyttelse all den tid bestemmelsen ikke er tilstrekkelig presis i sin ordlyd for å kunne ramme andre lag enn det som gir tilgang til selve systemet. Det er klart etter bestemmelsens forarbeider at lovgiver ønsket å ramme alle lag med beskyttelse, avhandlingen har imidlertid funnet at hjemmelen ikke er tilstrekkelig presis for å kunne hjemle dette.

På bakgrunn av det foregående vil jeg komme med følgende konklusjoner: 1) Hjemmelen oppfyller intensjonen om teknologinøytralitet og 2) Hjemmelen er tilstrekkelig presis for det den er satt til å regulere, med unntak i å hjemle åpning av innholdsdata.

4.2 Vurderinger av gjeldende rett

Etter avhandlingens gjennomgang av strpl. § 199 a er følgende svakheter avdekt: For det første inneholder den ingen eksplisitt ordlyd hva gjelder skranker for bruk av tvang. For det andre inneholder ikke ordlyden noen presisering av at den er teknologinøytral og hvilke teknologier som skal anses nøytrale. For det tredje, er ikke ordlyden tilstrekkelig klar på at den er ment til å ramme flere lag av beskyttelse.

Noen endringer i ordlyden med tanke på skranker eller biometrisk autentisering er lite hensiktsmessig all den tid bestemmelsen må tolkes i lys av de overordnede skranker uansett hvilke biometriske autentiseringer som måtte komme i fremtiden.

Det kan være hensiktsmessig å konkret spesifisere at bestemmelsen er teknologinøytral. Dette kan gjøres i bestemmelsens ordlyd. Det kan også være hensiktsmessig også å spesifisere hvor den er teknologinøytral. Slik det foreligger i dag ønskes det å ikke skille mellom ulike former for datasystem, samtidig som det ikke ønskes å skilles mellom ulike teknologier for biometrisk autentisering. Det forekommer altså to former av teknologinøytralitet, og av den grunn kan det konkret nevnes i bestemmelsens ordlyd, da det kan tenkes tilfeller der rettsanvendere ikke er oppmerksom på at den skal fremstå som å være teknologinøytral på to punkter.

For at innholdsdata også skal kunne pålegges åpnet, eller åpnet ved tvang med biometrisk autentisering må dette presiseres i lovtekst. Hensynet til etterforskningens effektivitet og kriminalitetsbekjempelse taler for at en slik regel burde eksistere. Det er derfor ønskelig med en slik regel og det er ikke tvil om at dette har vært lovgivers intensjon etter forarbeidene å dømme.

Den nåværende strpl. § 199 a speiles i forslag til ny straffeprosesslov § 14-6, jf. § 14-5. Bestemmelsene som er foreslått fremstår som mer gjennomtenkt og mer presist utformet enn dagens bestemmelse. Imidlertid har forslag til ny bestemmelse også forbedringspotensial hva

gjelder tilgang til innholdsdata, all den tid det åpnes for inntil 3 måneders fengsling dersom en person nekter å medvirke til åpning av et datasystem.

Det fremstår for meg som at det kan være hensiktsmessig å vurdere om det burde være anledning til å benytte deepfake syntetisering til bruk for etterforskning. Denne typen teknologi gjør at man ikke trenger å utøve tvang som krenker den fysiske integritet. Det kan være et nyttig verktøy for etterforskningen både med tanke på ransaking og beslag. På linje med at politiet har adgang til å bryte seg inn i fysiske lokasjoner med å ødelegge låser eller forfalske nøkler burde dette kunne gjøres digitalt også. Denne typen teknologi kan også være nyttig for andre skritt i etterforskningen, for eksempel infiltrering i lukkede digitale medier som kamuflasje. En åpning for slik bruk av teknologi må nødvendigvis redegjøres for nøye og hensyn for og imot må veies. Det vil være hensiktsmessig for lovgiver å ta opp dette til vurdering all den tid dette er en ny teknologi som bare i løpet av de siste årene har sett store fremskritt.

Referanseliste

Norske lover

Grunnloven	Lov 17. mai 1814 Kongeriket Norges Grunnlov
Straffeloven 1902	Lov 22. mai 1902 nr. 10 almindelig borgerlig straffelov
Straffeprosessloven	Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker
Politiloven	Lov 4. august 1995 nr. 53 om politiet
Menneskerettsloven	Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett
Straffeloven	Lov 20. mai 2005 nr. 28 om straff
Straffelovens ikraftsettingslov	Lov 19. juni 2015 nr. 65 om ikraftsetting av straffeloven 2005

Forskrifter

Påtaleinstruksen	Forskrift 28. juni 1985 nr. 1679 om ordningen av påtalemyndigheten

Konvensjoner

EMK	Europarådets konvensjon av 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter
Konvensjon om datakriminalitet	Europarådets konvensjon av 23. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi

Lovforarbeider

NOU 2003:27	NOU 2003:27 Lovtiltak mot datakriminalitet Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi
Ot. prp. nr. 40 (2004-2005)	Ot. prp. nr. 40 (2004-2005) om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet)
Dok. 16 (2011-2012)	Dok. nr. 16 (2011-2012) Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven
NOU 2016:24	NOU 2016:24 Ny straffeprosesslov
Prop. 6 L (2016-2017)	Prop. 6 L (2016-2017) Endringer i tinglysingsloven, inkassoloven og tvangsfullbyrdelsesloven mv. (teknologinøytralitet)
Prop. 106 L (2016-2017)	Prop. 106 L (2016-2017) Endringer i straffeprosessloven (biometrisk autentisering)

Rettspraksis

Norges Høyesterett

Rt. 1952 s. 1217 (to mistenkelige personer)

Rt. 1999 s. 1269 (fengselsbetjentdommen)

Rt. 2007 s. 932

Rt. 2011 s. 800

Rt. 2014 s. 1105 (acta)

Rt. 2014 s. 1292

Rt. 2015 s. 93 (Maria-dommen)

Rt. 2015 s. 155 (Rwanda)

HR-2016-1833-A (Fingeravtrykk-kjennelsen)

HR-2016-2554-P (Holship)

HR-2018-104-A (Mirmotahari)

HR-2019-610-A (Tidalkjennelsen)

Underrettspraksis

TJARE-2016-43883

LG-2016-62717

Den europeiske menneskerettsdomstolen

EMDs dom av 18. januar 1978, *Ireland v. The United Kingdom*, 5310/71
(Irland v. Storbritannia)

EMDs dom av 26. mars 1985, *X and Y v. The Netherlands*, 8978/80
(X og Y v. Nederland)

EMDs dom av 25. februar 1993, *Funke v. France*, 10828/84
(Funke v. Frankrike)

EMDs avvisningskjennelse av 6. april 1994, *Peters v. The Netherlands*, 21132/93
(Peters v. Nederland)

EMDs dom av 17. desember 1996, *Saunders v. The United Kingdom*, 19187/91
(Saunders v. Storbritannia)

EMDs dom av 22. juli 2003, *Y.F v. Turkey*, 24209/94
(Y.F. v. Tyrkia)

EMDs storkammerdom av 11. juli 2006, *Jalloh v. Germany*, 54810/00
(Jalloh v. Tyskland)

EMDs dom av 7. oktober 2008, *Bogumil v. Portugal*, 35228/03
(Bogumil v. Portugal)

EMDs storkammerdom av 4. desember 2008, *S. and Marper v. The United Kingdom*, 30562/04 and 30556/04
(S. og Marper v. Storbritannia)

EMDs storkammerdom av 1. juni 2010, *Gäfgen v. Germany*, 22978/05
(Gäfgen v. Tyskland)

EMDs storkammerdom av 28. september 2015, *Bouyid v. Belgium*, 23380/09
(Bouyid v. Belgia)

Bøker og artikler

Aall (2018)	Aall, Jørgen, *Rettsstat og menneskerettigheter*, 5. utgave (Bergen 2018)
Bernt og Doublet (2008)	Bernt, Jan Fridthjof og David R. Doublet, *Vitenskapsfilosofi for jurister*, 6. opplag (Bergen 2008)
Bruce og Haugland (2018)	Bruce, Ingvild og Geir Sunde Haugland, *Skjulte tvangsmidler*, 2. utgave (Oslo 2018).
Frøberg (2015)	Frøberg, Thomas, «Nyere praksis om det strafferettslige legalitetsprinsippet», *Jussens venner*, 01-02/2015 (volum 50) s. 46 - 71
Harris m.fl. (2018)	Harris, David m.fl., *Law of the European convention on Human Rights*, 4. utgave (Oxford 2018)
Hovlid (2017)	Hovlid, Ellen Lexerød, «Betydningen av teknologiutvalg for grensen mellom lovlige og ulovlige ytringer», *Lov og rett*, 10/2017 (volum 56) s. 609 - 626
Jacobs, White og Ovey (2017)	Jacobs, Francis, Robin White og Clare Ovey, *The European Convention on Human Rights*, 7. utgave av Bernadette Rainey, Elizaabeth Wicks og Clare Ovey (Oxford 2017)
Kaltenborn (2019)	Kaltenborn, Jul Fredrik, «Teknologinøytralitet og datakriminalitet – Særlig om klassifiseringen av begrepet datasystem», *Tidsskrift for strafferett*, 02/2019 (volum 19) s. 148 - 167

Lødrup, Kaasen og Tjomsland (2008) Lødrup, Peter, Knut Kaasen og Steinar Tjomsland, *Norsk Lovkommentar*, bind 1 (Oslo 2008)

Rui (2009) Rui, Jon Petter, «Om retten til å forholde seg taus og retten til ikke å måtte bidra til egen domfellelse», *Tidsskrift for rettsvitenskap*, 01/2009 (volum 122) s. 47 - 68

Rui (2018) Rui, Jon Petter, «Grunnlovens krav om forholdsmessighet ved inngrep i grunnlovfestede menneskerettigheter», *Lov og rett*, 03/2018 (volum 57), s. 129 - 130

Smith (2017) Smith, Eivind, *Konstitusjonelt demokrati: Statsforfatningsretten i prinsipielt og komparativt lys*, 4. utgave (Bergen 2017)

Sunde (2006) Sunde, Inger Marie, *Lov og rett cyberspace* (Bergen 2006).

Øyen (2019) Øyen, Ørnulf, *Straffeprosess*, 2. utgave (Oslo 2019).

Digitale kommentarutgaver

Bjerke, Keiserud og Sæther (2019) Bjerke, Hans Kristian, Erik Keiserud og Knut Erik Sæther, *Straffeprosessloven kommentarutgave*, bekreftet à jour per 1. juli 2019 på juridika.no. (sist lest 15. desember 2019 kl 18.00)

Haugland (2016) Haugland, Geir Sunde, kommentar til straffeprosessloven, *Gyldendals norsk lovkommentar*, kommentar til § 199 a, note 1309,

sist revidert 21.09.2016 (sist lest 15. desember kl. 18.00)

Nettbaserte kilder

Giordano (2019) — Giordano, Chiara, «Chinese police use surveillance technology to identify people by their walking style», *The Independent*, 26. februar 2019, https://www.independent.co.uk/news/world/asia/china-police-walking-gait-technology-surveillance-ai-suspect-a8797836.html (sist lest 14. desember 2019 kl. 16.00)

Knapskog (2018) — Knapskog, Svein Johan "Transaksjonskjede", *Store norske leksikon*, 2018, https://snl.no/transaksjonskjede (sist lest 14. desember 2019 kl. 16.00)

Rossen (2019) — Rossen, Eirik, «Biometrisk gjenkjenning», *Store norske leksikon*, 2019, https://snl.no/biometrisk_gjenkjenning (sist lest 14. desember 2019 kl. 16.00)

Brekke (2019) — Brekke, Anders, «Utfordres av 'deepfakes': - Vi er våre egne fiender», *NRK*, 24. februar 2019, https://www.nrk.no/norge/utfordres-av-_deepfakes__-_-vi-er-vare-egne-fiender_-1.14421262 (sist lest 14. desember 2019 kl. 16.00)