

# **Straffeprosessloven § 199 a – ransaking av datasystem**

*Bestemmelsens innhold og  
rettssikkerhetsmessige betenkeligheter*

**En juridisk oppgave**

**BACHELOROPPGAVE (BOPPG30)  
Politihøgskolen  
2019**

Kand.nr: 4 og 3  
Antall ord: 8 001

# INNHOLDSFORTEGNELSE

<b>1.0</b>	<b>INNLEDNING.....</b>	<b>2</b>
1.1	PRESENTASJON AV TEMA OG PROBLEMSTILLING.....	3
1.2	BAKGRUNN FOR TEMA.....	4
1.3	TELEFONENS BETYDNING SOM BEVIS I ETTERFORSKNINGEN .....	6
1.4	RETTSKILDEBILDE OG METODE.....	7
1.5	VIDERE FREMSTILLING .....	8
<b>2.0</b>	<b>STRAFFEPROSESSLOVEN § 199 A .....</b>	<b>9</b>
2.1	STRAFFEPROSESSLOVEN § 199 A FØRSTE LEDD.....	9
2.2	STRAFFEPROSESSLOVEN § 199 A ANNET LEDD .....	12
2.3	STRAFFEPROSESSLOVEN § 199 A TREDJE LEDD .....	14
2.4	STRAFFEPROSESSLOVEN § 199 A FJERDE LEDD .....	15
<b>3.0</b>	<b>POLITIETS BRUK AV MAKT .....</b>	<b>16</b>
3.1	POLITILOVEN § 6 .....	16
3.2	STRAFFEPROSESSLOVEN § 170 A .....	18
<b>4.0</b>	<b>RETTSSIKKERHETSMESSIGE BETENKELIGHETER .....</b>	<b>19</b>
4.1	LEGALITETSPRINSIPPET .....	19
4.2	PERSONVERNHENSYN .....	20
4.3	SELVINKRIMINERINGSPRINSIPPET .....	21
<b>5.0</b>	<b>AVSLUTNING.....</b>	<b>24</b>
<b>6.0</b>	<b>KILDELISTE.....</b>	<b>25</b>

## 1.0 INNLEDNING

Temaet for denne oppgaven er straffeprosessloven<sup>1</sup> § 199 a, som er politiets hjemmel for å få tilgang til et datasystem i forbindelse med ransaking. I vår oppgave vil vi særlig legge vekt på bestemmelsens annet ledd, som hjemler politiets bruk av tvang ved ransaking av et datasystem som er låst med biometrisk autentisering, og redegjøre for om denne adgangen kan være i konflikt med sentrale rettsstatsprinsipper. Bestemmelsen gjelder datasystemer generelt, men vi vil i denne oppgaven i all hovedsak ta for oss mobiltelefoner siden det er mest aktuelt i arbeidet som generalist i politiet. Biometrisk autentisering blir stadig mer utbredt som tilgangskontroll på mobiltelefonen og har i stor grad erstattet bruken av låsekode. Dette, i kombinasjon med våre erfaringer fra praksisåret under politiutdanningen, gjør at oppgaven vil ha fokus på mobiltelefoner som er låst med biometrisk autentisering, og hjemmelen til å kunne åpne disse med tvang.

Biometrisk autentisering er bruk av bestemte personlige kjennetegn for å bekrefte identitet. I følge datatilsynet<sup>2</sup> er biometriske kjennetegn unike for hver enkelt person, og de er stabile over tid. De mest kjente formene for biometriske kjennetegn er fingeravtrykk, håndavtrykk og ansiktsform, samt øyeteleknologiene netthinne- og irisavlesning.

Oppgaven vil bestå av tre deler, hvor det legges størst vekt på den første delen. I oppgavens første del vil vi gjøre rede for innholdet i straffeprosessloven § 199 a. Etter redegjørelsen av bestemmelsen vil vi ta for oss politiets generelle adgang til å bruke makt. Her vil vi se nærmere på politiloven<sup>3</sup> § 6, med hovedvekt på fjerde ledd, som på generelt grunnlag gir politiet lov til å bruke makt i tjenesteutførelsen. Vi vil også komme inn på straffeprosessloven § 170 a, som stiller et krav om forholdsmessighet og nødvendighet, og som er en bestemmelse som alltid kommer til anvendelse ved bruk av straffeprosessuelle tvangsmidler.

I oppgavens tredje del vil vi gjøre rede for legalitetsprinsippet, vernet mot selvinkriminering, samt personvern hensyn. Oppgaven vil reise spørsmål om det kan være slik at bestemmelsen utfordrer, er i strid med, eller krenker disse viktige rettsstatsprinsippene.

---

<sup>1</sup> Lov av 22. Mai 1981, nr. 25 om rettergangsmåten i straffesaker (Straffeprosessloven)

<sup>2</sup> <https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/>

<sup>3</sup> Lov av 04. August 1995 nr. 53 Lov om politiet (politiloven)

## 1.1 PRESENTASJON AV TEMA OG PROBLEMSTILLING

Straffeprosessloven § 199 a, slik den fremstod før lovendringen den 1.juli 2017, ga politiet adgang til å pålegge enhver som hadde befatning med et datasystem om å gi nødvendige opplysninger for å gi tilgang til datasystemet. Lovendringen fra 2017 gir nå politiet hjemmel til å bruke biometrisk autentisering for å få nevnte tilgang, og den gir påtalemyndigheten, eller politiet når det er fare ved opphold, anledning til å bruke tvang dersom det ovennevnte pålegget ikke blir etterkommet. I forarbeidene<sup>4</sup> til lovendringen fremkommer det at bakgrunnen for behovet for en lovendring er Høyesteretts kjennelse<sup>5</sup> avsagt 30. august 2016 hvor det ble slått fast at straffeprosessloven § 157, som hjemler kroppslig undersøkelse, ikke ga hjemmel til å bruke tvang ovenfor mistenkte for å få tilgang til innholdet på datasystem (i den aktuelle sak en mobiltelefon) ved bruk av biometrisk autentisering (fingertrykksautentisering).

Interessen vår for å skrive om denne bestemmelsen handler om egne erfaringer fra praksisåret og problemstillinger som dukket opp der. Vi opplevde begge situasjoner hvor en mobiltelefon ble tatt i beslag, og hvor det var mye usikkerhet rundt muligheten til å åpne en låst mobiltelefon med biometrisk autentisering. Siden lovendringen er så ny opplevde vi at flere av de mer erfarne polititjenestemennene også var usikre på hvordan vi kunne håndtere dette, og om det i det hele tatt fantes en lovhjemmel for et slikt inngrep. En annen grunn til at vi har fattet interesse for denne bestemmelsen er at lovendringen før ikrafttreddelsen fikk en del kritikk under høringsrunden. Det har blant annet blitt påstått at endringen er forhastet, og at den er problematisk i forhold til sentrale prinsipper i rettsstaten. Lovendringen fikk også oppmerksomhet i media, hvor blant annet leder av forsvarergruppen i Advokatforeningen, Marius Oscar Dietrichson, sa til NRK at «*vi (Advokatforeningen) er kritiske til omfanget av hjemmelen og at det retter seg mot en enhver person. Nå må de som ikke har gjort noe galt finne seg i at politiet kan tvinge dem til å åpne enheten*»<sup>6</sup>. Jusprofessor, Hans Fredrik Marthinussen, sa i samme artikkel at «*det er snakk om ganske inngripende tiltak som går på den grunnleggende beskyttelsen mot å bidra til egen domfellelse for straffbare forhold*». Marthinussen sa at bestemmelsen kan være et brudd på menneskerettighetene.

---

<sup>4</sup> Prop. 106 L (2016-2017), s. 2

<sup>5</sup> Rt. 2016, s. 1833

<sup>6</sup> <https://www.nrk.no/norge/na-kan-politiet-tvinge-deg-til-a-lase-opp-telefonen-din-1.13572392>

Straffeprosessloven § 199 a første ledd gir politiet adgang til å pålegge enhver som har befattning med et datasystem å gi nødvendige opplysninger for å gi tilgang til datasystemet eller å åpne det ved bruk av biometrisk autentisering. Det interessante med bestemmelsen er annet ledd som gir politiet adgang til å tvinge fram nevnte autentisering dersom vedkommende nekter å etterkomme pålegget etter første ledd.

Bestemmelsen reiser rettssikkerhetsmessige spørsmål. Særlig gjelder det vernet mot selvinkriminering. Man kan nekte å si noe som kan bidra til egen domfellelse, men politiet kan ved bruk av makt åpne og ransake en telefon for å sikre viktige bevis. En telefon i dagens høyteknologiske samfunn kan inneholde enorme mengder digital informasjon, og politiet vil ved gjennomgang av en telefon dykke dypt i en persons privatliv. For mange vil ransaking av ens telefon føles som mer integritetskrenkende enn en husransaking på grunn av de enorme mengdene med personlig data som ligger lagret der. Politiet vil ved en slik ransaking kunne finne informasjon om flere straffbare forhold enn hva mistanken i utgangspunktet dreide seg om. Dette vil politiet også kunne gjøre ved andre former for ransaking, men i medhold av straffeprosessloven § 199 a kan den mistenkte/siktede aktivt medvirke med egen kropp for å gjøre denne informasjonen tilgjengelig. Bestemmelsen omfatter ikke bare mistenkte/siktede, men også enhver annen som har befattning med datasystemet. Dette hjemmelsgrunnlaget fremstår som unikt i norsk straffeprosess, noe som også var en medvirkende årsak til at denne bestemmelsen ble valgt som tema for vår oppgave.

## 1.2 BAKGRUNN FOR TEMA

I en sak fra 2016 var det uenighet om hvorvidt politiet kunne tvinge siktede til å låse opp en mobiltelefon med hjemmel i straffeprosessloven § 157. Vedkommende var siktet for overtredelse av straffeloven § 272, jf. § 271 (grov kroppskrenkelse) og politiet begjærte Jæren tingrett om kjennelse for at siktedes finger kunne brukes til å låse opp vedkommende sin mobiltelefon. Bakgrunnen for begjæringen var en mistanke om at telefonen kunne ha vært brukt til å filme eller fotografere de voldshandlinger som vedkommende nå var siktet for. Ved Jæren tingretts kjennelse av 29.03.2016<sup>7</sup> ble begjæringen tatt til følge. Siktedes anke ble av Gulating lagmannsrett den 26.04.2016<sup>8</sup> forkastet. Høyesteretts ankeutvalg bestemte at ankesaken i sin helhet skulle avgjøres av Høyesterett.

---

<sup>7</sup> TJARE-2016-43883

<sup>8</sup> LG-2016-62717

Høyesteretts førstvoterende uttalte følgende i behandlingen av saken<sup>9</sup>; «I dette tilfellet finner jeg det klart at lovkravet ikke er oppfylt. Jeg ser derfor ikke grunn til å gå nærmere inn på kravets innhold ved det straffeprosessuelle tvangsmiddel som er tema i saken, men går over til å vurdere lagmannsrettens tolkning av straffeprosessloven § 157. Bestemmelsen åpner etter ordlyden adgang til "kroppslig undersøkelse". Lovteksten konkretiserer ikke hva slags kroppslige undersøkelser som omfattes, ut over at det i første ledd andre punktum fremgår at det kan "tas blodprøve og foretas andre undersøkelser som kan skje uten fare eller betydelig smerte". Førstvoterende fant på bakgrunn av en naturlig forståelse av bestemmelsens ordlyd at de undersøkelsene som straffeprosessloven § 157 ga hjemmel til, gjaldt undersøkelser av siktedes kropp, både utvendig og i kroppens hulrom. Formålet med denne typen undersøkelse ville være å bruke kroppen, eller det som befant seg i kroppen, som et bevis i seg selv. Høyesterett viste også til at straffeprosessloven § 157 var plassert i straffeprosesslovens kapittel 12 som omhandler gransking, og at det ikke var en form for ransaking. Høyesterett kom dermed til at bruken av siktedes finger til å få tilgang til bevismidler utenfor kroppen språklig sett var noe annet enn en kroppslig undersøkelse, og at ordlyden i straffeprosessloven § 157 med ikke ga hjemmel for det inngrep som var tema i saken.

Kjennelsen fra Høyesterett var enstemmig, og det ble påpekt at straffeprosessloven § 199 a, slik den fremstod i 2016, ikke ga hjemmel for det inngrep saken gjaldt, fordi bestemmelsen ikke åpnet for bruk av tvang.

Kort tid etter at Høyesterett avsa kjennelsen sendte Justis- og beredskapsdepartementet et lovforslag til Stortinget<sup>10</sup> om endringer i straffeprosessloven. Lovforslaget ville gi politiet adgang til å bruke tvang til å gjennomføre biometrisk autentisering dersom pålegg om å gi opplysninger eller å frivillig åpne datasystemet ved bruk av biometrisk autentisering ikke ble fulgt. Lovforslaget ble vedtatt, og bestemmelsen, slik den fremstår i dag, trådte i kraft 1.juli 2017.

---

<sup>9</sup> HR-2016-1833-A, avsnitt 19.

<sup>10</sup> Prop. 106 L (2016-2017), s. 5.

### 1.3 TELEFONENS BETYDNING SOM BEVIS I ETTERFORSKNINGEN

Det fremkommer av straffeprosessloven § 226 at «*formålet med etterforskningen er å skaffe til veie de nødvendige opplysninger*» for å, blant annet, «*avgjøre spørsmålet om tiltale og å tjene som forberedelse for rettens behandling av spørsmålet om straffeskyld*». Hva som er de *nødvendige opplysningene* vil variere fra sak til sak, men det vil være ulike bevis som har blitt skaffet til veie både gjennom taktisk og teknisk etterforskning. Eksempler på dette kan være forklaringene til de involverte partene, data fra basestasjoner, videoovervåkning, våpen som har blitt brukt, biologisk materiale fra åstedet, og innhold på en mobiltelefon.

I etterforskningen av straffesaker, og som et ledd i å skaffe til veie de nødvendige opplysningene, vil det i mange tilfeller være aktuelt å ta beslag i, og ransake, en telefon for å sikre bevis. Digitale spor har blitt en viktig del av etterforskningen i takt med at stadig mer informasjon blir lagret digitalt. Når det gjelder mobilens betydning som bevis i en straffesak kan man skille mellom *traffikkdata* og *innholdsdata*. Trafikkdata er informasjon som ofte lagres av tjenesteleverandøren og som kan ha stor betydning for politiet. Trafikkdata kan gi informasjon om hvem som har ringt hvem, når det er ringt og varighet av samtalen<sup>11</sup>. Man kan også få vite om en bestemt telefon har vært tilkoblet en basestasjon på et bestemt tidspunkt, noe som kan være med på å knytte en person til et geografisk avgrenset område i et bestemt tidsrom. Slik informasjon trenger politiet ikke selve mobilen for å få tilgang til da informasjonen vil kunne utleveres av tjenesteleverandøren etter anmodning fra politiet. Informasjonen man vil få tilgang til ved ransaking av en mobiltelefon kalles gjerne *innholdsdata*. Meldinger lagret på en mobil er et eksempel på en slik form for data<sup>12</sup>. Innholdsdataene vil ofte være gode bevis i seg selv, eller de kan være med på å styrke eller svekke eksisterende bevis, f.eks. mistenkte/siktedes forklaring. Bilde- og videomateriale lagret på en mobil vil også kunne være sterke bevis i etterforskningen av en straffesak.

En mobiltelefon vil altså kunne være en viktig brikke i arbeidet med å skaffe til veie de nødvendige opplysningene i etterforskningen, og innholdet som avdekkes kan danne gode bevis i en straffesak. I mange tilfeller kan mobilen være en gullgrube for politiet i forbindelse med etterforskningen, da det kan oppdages mye rettsrelevant informasjon på den. Informasjon som vil kunne være viktige bevis både for påtalemyndigheten og retten.

---

<sup>11</sup> Bjercknes og Fahsing, *Etterforskning-Prinsipper, metoder og praksis*, Bergen 2018, s. 245.

<sup>12</sup> Bjercknes og Fahsing, s. 245.

## 1.4 RETTSKILDEBILDE OG METODE

I dette kapitlet vil vi redegjøre for rettskildebildet og presentere metoden vi har valgt å bruke til å løse vår problemstilling.

I behandlingen av oppgavens hovedproblemstilling vil vi redegjøre for innholdet i straffeprosessloven § 199 a. Siden oppgaven er en redegjørelse av en lovbestemmelse vil rettskildelæren og rettskildeprinsippene være sentrale og viktige, og man vil dermed anvende juridisk metode ved besvarelsen av oppgaven.

Juridisk metode, eller rettskildelære, er læren om hva man bygger på og hvordan man resonnerer når man skal ta standpunkt til et rettsspørsmål de lege lata<sup>13</sup>. Den juridiske metoden baserer seg på en rekke prinsipper. Prinsippene handler mye om hvilke kilder man kan innhente argumentasjon fra, og hvilke vekt disse kildene skal ha. Torstein Eckhoff<sup>14</sup> omtaler kildene lovtekst, forarbeider, rettspraksis, andre myndigheters praksis, privates praksis, rettsoppfatninger og reelle hensyn som rettskildefaktorer, og det er disse faktorene vi vil ta utgangspunkt i ved besvarelsen av oppgaven. Vi vil imidlertid avgrense til de rettskildefaktorene som er sentrale og relevante ved besvarelsen av problemstillingene.

Politiets hjemmel for å få tilgang til et datasystem i forbindelse med ransaking er omhandlet i straffeprosessloven § 199 a. Lovteksten er, som nevnt over, en rettskildefaktor, og lovtekst og ordlyd vil være sentrale ved besvarelsen. Eckhoff<sup>15</sup> har uttalt at; «*Finnes det en relevant lovbestemmelse, er den det naturlige utgangspunktet for de videre resonnementer*».

Lovforarbeidene til endringen i straffeprosessloven § 199 a vil også være en sentral og viktig rettskildefaktor i arbeidet med å besvare oppgaven. Proposisjonen fra Justis- og beredskapsdepartementet er et forslag til Stortinget om endringen i straffeprosessloven innenfor ransaking av et datasystem. Lovforarbeidene vil kunne gi viktig kunnskap om bakgrunnen for lovendringen, og dermed hva som har vært lovgivers formål med lovendringen. Et lovforarbeid er derfor en viktig rettskildefaktor fordi domstolen som skal

---

<sup>13</sup> Torstein Eckhoff, *Rettskildelære*, 2007, s. 15

<sup>14</sup> Torstein Eckhoff, s. 19 og 23

<sup>15</sup> Torstein Eckhoff, s. 39



behandle saker og anvende lovbestemmelsene føler seg forpliktet til å være lojal ovenfor lovgiver da dette er retningsgivende for hvordan bestemmelsen skal forstås og tolkes<sup>16</sup>.

Lovendringen er som nevnt tidligere i oppgaven av nyere tid, og i skrivende stund foreligger det lite rettspraksis på dette området. Vi har også forsøkt å se om det foreligger relevant rettspraksis blant de andre nordiske landene, uten funn. Rettspraksis, særlig fra Høyesterett, skal vektes som en rettskildefaktor med stor betydning. Dette på grunn av at de kan avgjøre hvordan et rettsspørsmål skal tolkes, vektlegges og forstås. Slik legger dette føringene for hvordan andre rettsadvokere skal behandle lignende rettsspørsmål<sup>17</sup>. Vi har funnet noe lagmannsrettspraksis, men denne rettskilden vil måtte tillegges noe begrenset vekt sammenlignet med en høyesterettsavgjørelse.

Vi har i vår besvarelse valgt å trekke inn flere sentrale rettsstatsprinsipper, slik som legalitetsprinsippet, personvern hensynet og selvinkrimineringsprinsippet. Den europeiske menneskerettskonvensjonen (EMK) er av stor betydning som rettskildefaktor i Norge. Dette har Stortinget gjennom lov forpliktet seg til å følge jf. menneskerettsloven<sup>18</sup> § 2. Konvensjonen skal vektes på lik linje med lovtekst og i de tilfeller der disse kommer i konflikt skal konvensjonsbestemmelsene gå foran annen lovgivning<sup>19</sup>.

## 1.5 VIDERE FREMSTILLING

I denne oppgaven vil vi starte med å tolke straffeprosessloven § 199 a. Vi vil ta for oss bestemmelsens ulike ledd suksessivt, med hovedvekt på første og annet ledd. Deretter vil vi ta for oss politiets adgang til å bruke makt i tjenesteutførelsen, hvor politiloven § 6 og straffeprosessloven § 170 a vil være sentrale bestemmelser i redegjørelsen av dette tema. Vi vil etter dette reise noen rettssikkerhetsmessige spørsmål hvor vi vurderer straffeprosessloven § 199 a, opp mot sentrale rettssikkerhetsmessige prinsipper som legalitetsprinsippet, personvern hensynet og selvinkrimineringsprinsippet.

---

<sup>16</sup> Steinar Fredriksen, *Innføring i straffeprosess*, 3. utgave, Gyldendal juridisk, Oslo 2015, s. 50

<sup>17</sup> Steinar Fredriksen, 2015, s. 51

<sup>18</sup> Lov av 21. mai 1999 nr. 30 Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)

<sup>19</sup> Steinar Fredriksen, 2015, s. 51

## 2.0 STRAFFEPROSESSLOVEN § 199 A

Straffeprosessloven § 199 a lyder som følger;

*«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.»*

Vi vil i den videre besvarelsen redegjøre for de de ulike leddene i bestemmelsen suksessivt, hvor hovedvekten vil være på bestemmelsens første og annet ledd.

### 2.1 STRAFFEPROSESSLOVEN § 199 A FØRSTE LEDD

Straffeprosessloven § 199 a første ledd sier at politiet, ved ransaking, kan pålegge enhver som har befatning med et datasystem å gi nødvendige opplysninger for å gi tilgang til datasystemet, eller å åpne det ved bruk av biometrisk autentisering. Første ledd angir dermed en medvirkningsplikt for den som pålegget retter seg mot.

Bestemmelsen angir ingen krav til bevisbyrde før en ransaking kan finne sted. Bestemmelsen ligger imidlertid inn under straffeprosesslovens kapittel 15 (ransaking), slik at de generelle vilkårene for ransaking må være oppfylt før straffeprosessloven § 199 a kan anvendes. Dette fremkommer av forarbeidene<sup>20</sup>, hvor det blant annet heter at «*straffeprosessloven kapittel 15 gir politiet adgang til å ransake datasystem dersom de grunnleggende vilkårene for*

---

<sup>20</sup> Prop.106 L (2016-2017), s. 3.

*tvangsmiddelbruk er oppfylt, herunder kravet om skjellig grunn til mistanke og forholdsmessighet». Høyesterett har også slått fast dette i kjennelse av 28.03.2019<sup>21</sup>.*

Det følger av straffeprosessloven § 192 og § 195 at ransaking kan skje når noen med «*skjellig grunn*» mistenkes for en handling som etter loven kan medføre frihetsstraff (fengsel). Det følger av rettspraksis<sup>22</sup> at det med «*skjellig grunn*» menes at det må være en sannsynlighetsovervekt, altså mer enn 50 % sannsynlig at en person er skyldig i å ha begått det angitte lovbruddet. Dette omtales gjerne som de materielle generelle vilkårene i bestemmelsene om ransaking. Videre er det noen materielle spesielle vilkår i begge bestemmelsene som må være oppfylt for at politiet kan gjennomføre ransakingen. I straffeprosessloven § 192, ofte omtalt som «*husransaking*», kan det foretas ransaking av «*bolig, rom eller oppbevaringssted for å sette i verk pågripelse eller for å søke etter ting eller bevis som kan beslaglegges eller som det kan tas heftelse i*». I straffeprosessloven § 195, ofte omtalt som «*personransaking*», er disse vilkårene at det kan «*foretas ransaking av hans person dersom det er grunn til å anta at det kan føre til oppdagelse av bevis eller av ting som kan beslaglegges eller som det kan tas heftelse i*». Det fremkommer av straffeprosessloven § 195 tredje ledd at det stilles strengere krav, både til de generelle og spesielle vilkårene, til ransaking av andre enn mistenkte. Her er vilkårene at «*av andre enn mistenkte kan det foretas ransaking når mistanken gjelder en handling som etter loven kan medføre straff av fengsel i mer enn 6 måneder, og særlige omstendigheter taler for å foreta slik ransaking*».

Straffeprosessloven § 199 a første ledd angir at enhver som er i befatning med datasystemet, kan bli ilagt et pålegg av politiet. Politiets adgang til å gi pålegg finner man flere eksempler av i både straffeprosessloven og i politiloven (se eksempelvis straffeprosessloven § 216 a og politiloven § 7). Med pålegg menes en type beordring eller en befaling fra politiet om å opptre på en bestemt måte. Det er bestemmelsens andre ledd som angir konsekvensen og reaksjonen fra politiet dersom vedkommende nekter å etterkomme pålegget som er gitt.

En tolkning av begrepet «*enhver*» innebærer at ransakingen kan skje både overfor den mistenkte, samt overfor en tredjeperson som ikke er mistenkt for å ha begått et straffbart forhold. Det kreves kun at de har en eller annen form for befatning med datasystemet som politiet ønsker adgang til. Med befatning forstås både den som eier datasystemet, men også

---

<sup>21</sup> HR-2019-610-A, avsnitt 28

<sup>22</sup> Rt. 1993 s. 1302

den som av andre årsaker har (tilgang til) datasystemet på tidspunktet når pålegget gis. Dette kan eksempelvis være IT-personell eller systemoperatører<sup>23</sup>.

Begrepet «*datasystem*» defineres ikke videre i bestemmelsen, men det følger av forarbeidene til bestemmelsen<sup>24</sup> at det med «*datasystem*» menes «*enhver innretning, bestående av maskinvare og programvare, som foretar behandling av data ved hjelp av dataprogrammer. For eksempel omfattes datamaskiner, nettbrett og smarttelefoner.*». Siden ordlyden i bestemmelsen er formulert på ovennevnte måte vil den dermed fange opp framtidens teknologi uten at det vil måtte kreves en lovendring. Dette fremstår som fornuftig med tanke på den stadige teknologiske utviklingen.

Pålegget som gis i medhold av straffeprosessloven § 199 a første ledd gjelder enten å gi politiet de nødvendige opplysninger som kreves for å gi tilgang til datasystemet, eller å åpne det ved bruk av biometrisk autentisering. Bestemmelsens forarbeider angir ingen videre forståelse av hva som menes med «*nødvendige opplysninger*», men etter en naturlig språklig forståelse forstås dette som eksempelvis pin-kode på en mobiltelefon eller passordet for å logge på en datamaskin eller nettbrett. «*Biometrisk autentisering*» har i større og større grad erstattet bruk av passord ved at man for eksempel bruker fingeravtrykket eller irisgjenkjenning til å låse opp datasystemet.

Ransaking og anvendelsen av straffeprosessloven § 199 a utenfor Norges grenser ble klarlagt da Høyesterett i kjennelse av 28.03.2019<sup>25</sup> behandlet Tidal Music AS sin anke over Borgarting lagmannsretts kjennelse av 18.01.2019. Økokrim begjærte ransaking av Tidal Music AS på bakgrunn av en siktelse som gjaldt databedrageri ved manipulasjon av avspillingstall. Tingretten besluttet at ransaking kunne finne sted. Tidal Music AS anket kjennelsen og anførte at økokrim ikke kunne gjøre beslag på servere i andre lands territorium. Lagmannsretten kom til at vilkårene for tredjemannsransaking, jf. straffeprosessloven § 192 tredje ledd var oppfylt, og at det kunne gis pålegg om å gi tilgang til datasystemet med hjemmel i straffeprosessloven § 199 a. En ansatt på Tidal Music sitt avdelingskontor i Norge, som hadde tilgang til de aktuelle serverne i utlandet, kunne dermed pålegges å gi økokrims tjenestemenn nødvendige opplysninger for å gi tilgang til datasystemet.

---

<sup>23</sup> Prop.106 L (2016-2017) s. 3

<sup>24</sup> Prop.106 L (2016-2017) s. 11

<sup>25</sup> HR-2019-610-A

Høyesterett kom til samme resultat som tingretten og lagmannsretten. Ransaking etter straffeprosessloven § 192 tredje ledd, og bruk av straffeprosessloven § 199 a, hjemler dermed at politiet kan sikre og få tilgang til materiale som fysisk ligger lagret på et lagringsmedium i utlandet. Høyesterett la i sin begrunnelse vekt på følgende momenter; beslutningen om ransaking og pålegg ble satt i verk på norsk territorium, norske domstoler traff beslutningen om ransaking, materialet ble gjort tilgjengelig gjennom bruk av tvangsmidler overfor et norsk selskap med kontor i Norge, ransakingen ville bare gi tilgang til materiale som selskapet selv hadde lagret, og materialet ville fortsatt være i behold på den utenlandske serveren<sup>26</sup>.

## 2.2 STRAFFEPROSESSLOVEN § 199 A ANNET LEDD

Straffeprosessloven § 199 a annet ledd angir som tidligere nevnt reaksjonen dersom den som pålegget retter seg mot nekter å etterkomme dette. Bestemmelsens annet ledd angir at politiet i disse tilfellene kan gjennomføre den biometriske autentiseringen ved bruk av makt.

Siden bestemmelsens første ledd angir at politiet kan gi pålegget til «*enhver*», så innebærer dette at også bruken av tvang etter bestemmelsens annet ledd også kan utøves overfor «*enhver*». Tvangsbruken gjelder kun den biometriske autentiseringen, den gir ikke anledning til å tvinge fram nødvendige opplysninger som eksempelvis pin-kode eller passord. Dette fremkommer i forarbeidene<sup>27</sup> til lovendringen hvor det står at «*man kan for eksempel ikke tvinge noen til å uttale noe*».

Bestemmelsens annet ledd må leses i sammenheng med straffeprosessloven § 170 a og politiloven § 6 fjerde ledd. Etter straffeprosessloven § 170 a kan et tvangsmiddel bare brukes når det er tilstrekkelig grunn til det, samt at det ikke kan brukes når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep. I medhold av politiloven § 6 fjerde ledd kan politiet anvende makt under tjenesteutførelsen i den utstrekning det er nødvendig og forsvarlig. En ransaking og bruk av straffeprosessloven § 199 a er å betrakte som tvangsmiddel og prinsippene som følger av straffeprosessloven § 170 a vil gjelde i de tilfeller hvor bestemmelsen skal anvendes. Redegjørelsen av politiloven § 6 og straffeprosessloven § 170 vil vi komme tilbake til i henholdsvis punkt 3.1 og 3.2 i besvarelsen.

---

<sup>26</sup> HR-2019-610-A, avsnitt 65-70

<sup>27</sup> Prop.106 L (2016-2017), s. 12.

Det som imidlertid er spesielt med straffeprosessloven § 199 a er, som vi også tidligere har påpekt, at ransakingen og tvangsmidlet kan utøves overfor en tredjeperson som ikke er mistenkt for å ha begått et straffbart forhold. Rimelighetshensyn tilsier at det bør stilles et strengere krav til forholdsmessighet når det er tale om tredjepersoner, og at terskelen for å utøve makt med hjemmel i straffeprosessloven § 199 a annet ledd må være høyere når den som ransakingen utøves mot er en tredjeperson. Dette fremkommer også av straffeprosessloven § 195 tredje ledd hvor det er strengere vilkår som må oppfylles for å kunne foreta personransaking av andre enn mistenkte. Det kan dermed tenkes tilfeller hvor det ikke er i strid med forholdsmessighetsprinsippet som følger av straffeprosessloven § 170 a å tvinge mistenkte til å gi tilgang til datasystemet, mens det vil være i strid med prinsippet å utøve samme form for tvang overfor en tredjeperson.

Videre må det påpekes at den aktuelle formen for tvang, og det inngrepet som tvangen representerer, også vil kunne medføre at vurderingen av forholdsmessighetsprinsippet etter straffeprosessloven § 170 a vil stille seg ulikt. Justis- og beredskapsdepartementet<sup>28</sup> bemerket i sin høringsrunde at *«hvert tilfelle av bruk av tvang må vurderes opp mot det alminnelige forholdsmessighetsprinsippet i straffeprosessloven § 170 a»*. Dette vil si at tvangen må være egnet til å gi den ønskede virkningen, altså lette gjennomføringen av ransakingen, og at det ikke finnes mindre inngripende alternativer som er like egnede<sup>29</sup>. Justis- og beredskapsdepartementet uttalte videre at *«tvangsgjennomføring av de to autentiseringsmetodene som ser ut til å være de mest aktuelle i dag, fingeravtrykksautentisering og irisgjenkjenning, normalt vil innebære nokså beskjeden maktbruk slik at det ikke kan anses uforholdsmessig. Departementet utelukker likevel ikke at irisgjenkjenning vil kunne innebære et noe større inngrep enn fingeravtrykksautentisering og dermed stille noe større krav til «sakens art og forholdene ellers», jf. straffeprosessloven § 170 a<sup>30</sup>»*.

En tvangsgjennomføring av en fingeravtrykksautentisering vil normalt representere en forholdsvis beskjeden form for tvang hvor faren for alvorlig skade vil være liten. En tvangsgjennomføring av en irisgjenkjenning kan imidlertid tenkes brutal og med et stort skadepotensial da dette gjelder et så sårbart organ som øyet. Dersom man sammenligner tvangsutøvelsen etter straffeprosessloven § 199 a annet ledd med eksempelvis undersøkelse

---

<sup>28</sup> Prop.106 L (2016-2017) s. 12

<sup>29</sup> Prop.106 L (2016-2017) s. 12

<sup>30</sup> Prop.106 L (2016-2017) s. 12

av kroppens hulrom, jf. straffeprosessloven § 157, vil bruken av tvang etter førstnevnte bestemmelse fremstå som mindre inngripende. Det må imidlertid bemerkes at gransking etter straffeprosessloven § 157 ikke kan anvendes overfor en tredjeperson. I straffeprosessloven § 157 første ledd fremkommer det også et krav om at undersøkelsen kun kan gjennomføres uten fare eller betydelig smerte. En slik presisering fremkommer ikke av straffeprosessloven § 199 a annet ledd.

Vilkåret for å kunne utøve tvang etter straffeprosessloven § 199 a må anses å være tilstede i den perioden ransakingen varer, og tvangsbruken må avsluttes med en gang politiet har fått adgang til datasystemet.

### 2.3 STRAFFEPROSESSLOVEN § 199 A TREDJE LEDD

Bestemmelsens tredje ledd angir hvem som kan beslutte bruk av tvang etter annet ledd. Dette kalles gjerne for det formelle vilkåret i bestemmelsen. Bestemmelsen oppstiller en hovedregel som sier at beslutningen treffes av påtalemyndigheten, men at politiet på stedet kan treffe denne beslutningen dersom det er fare ved opphold. Dersom politiet på stedet treffer beslutningen, så skal dette straks meldes til påtalemyndigheten.

Hva som menes med «fare ved opphold» defineres ikke videre i bestemmelsen, men det er rimelig å anta at det med dette menes at det må være en fare for at formålet med bruken av tvangsmiddelet vil forspilles dersom man må vente på en beslutning fra påtalemyndigheten. Det kan være seg at viktige bevis på datasystemet vil kunne gå tapt, ved at det eksempelvis slettes eller på andre måter fjernes i løpet av den tiden som går før politiet får en beslutning fra påtalemyndigheten. Dette fremstår også som naturlig når man vet hvor raskt man med dagens teknologi kan slette og fjerne eksempelvis bilder og filmer fra en mobiltelefon. Denne forståelsen av hva som ligger i formuleringen «fare ved opphold» samsvarer også med forarbeidene<sup>31</sup>.

Under høringsrunden kom det inn mange synspunkter på hvem som burde ha kompetanse til å beslutte tvangsgjennomføring etter straffeprosessloven § 199 a annet ledd. Datatilsynet uttalte<sup>32</sup> at ved å legge beslutningen til andre enn politiet på stedet så kunne det være med på å «hindre overilte beslutninger i en opphetet ransakingssituasjon». Flere av høringsinstansene

---

<sup>31</sup> Prop.106 L (2016-2017) s. 12

<sup>32</sup> Prop.106 L (2016-2017) s. 8

delte datatilsynets syn på saken, og mente at kompetansen til å treffe beslutning om bruk av tvang burde bli lagt til påtalemyndigheten.

Kompetansen til å treffe beslutning om bruk av tvangsmidler ligger i dag hos både retten, påtalemyndigheten og politiet på stedet. Retten har beslutningsmyndighet i saker som omhandler varetektsfengsling i medhold av straffeprosessloven § 184, ransaking etter straffeprosessloven § 200 a, kommunikasjonsavlytting etter straffeprosessloven § 216 a og kroppslig undersøkelse etter straffeprosessloven § 157 (påtale ved fare ved opphold). Påtalemyndigheten på sin side, fatter beslutning i saker som omhandler pågrep i medhold av straffeprosessloven § 175, teknisk sporing jf. § 202 b, og beslag etter straffeprosessloven § 205. Politiet har eksempelvis kompetanse til å fatte beslutning om ransaking og beslag dersom vilkårene etter straffeprosessloven §§ 198 og 206 er til stede. Beslutningskompetansen som er gitt til å fatte beslutninger etter straffeprosessloven § 199 a annet ledd kan derfor sies å harmonisere med straffeprosesslovens øvrige bestemmelser.

#### 2.4 STRAFFEPROSESSLOVEN § 199 A FJERDE LEDD

Bestemmelsens fjerde ledd sier at straffeprosessloven § 199 a gjelder tilsvarende så langt den passer for gransking av datasystem som er tatt i beslag etter kapittel 16.

I medhold av straffeprosessloven kapittel 16 kan politiet ta beslag i ting som antas å ha betydning som bevis (se straffeprosessloven § 203). Det er ingen bestemmelse i straffeprosessloven kapittel 16 om beslag som uttrykkelig gir politiet adgang til å anvende tvang for å få åpnet et datasystem som er beslaglagt. Ved å ta inn denne formuleringen i straffeprosessloven § 199 a fjerde ledd så innebærer dette at medvirkningsplikten og tvangshjemmelen som følger av bestemmelsens første og annet ledd også vil gjelde i de tilfellene hvor datasystemet er beslaglagt. Dette er også naturlig da en ransaking vil kunne gå over til beslag, og dermed unngår man at tvangshjemmelen opphører.

Departementet uttalte i høringsrunden<sup>33</sup> at *«det er ingen grunn til at politiet ikke skal ha samme virkemidler ved gransking av et beslaglagt datasystem, som ved ransaking av det.»*

---

<sup>33</sup> Prop.106 L (2016-2017) s. 12



### 3.0 POLITIETS BRUK AV MAKT

I straffeprosessloven § 199 a annet ledd fremkommer det som nevnt tidligere at politiet kan bruke tvang for å gjennomføre den biometriske autentiseringen. Begrepet tvang er ikke definert i lovteksten, men en naturlig forståelse av ordet vil være at man, om nødvendig, tvinger noen ved bruk av fysisk makt for å få gjennomført en handling, i dette tilfellet en biometrisk autentisering. I dette avsnittet ønsker vi å se nærmere på politiloven § 6, som hjemler politiets bruk av makt i tjenesteutførelsen, samt straffeprosessloven § 170 a som oppstiller krav om nødvendighet og forholdsmessighet for at et tvangsmiddel kan benyttes.

#### 3.1 POLITILOVEN § 6

Politoloven § 6 angir noen alminnelige regler om hvordan polititjenesten skal utføres. Av bestemmelsens fjerde ledd følger det at *«politiet kan anvende makt under tjenesteutførelsen i den utstrekning det er nødvendig og forsvarlig»*. Politiloven § 6 inneholder grunnprinsippene for all utøvelse av politimyndighet, både den som er hjemlet i politiloven og straffeprosessloven, og den som har et annet hjemmelsgrunnlag.

I utgangspunktet skal ikke politiloven § 6 brukes som en generell hjemmel for politiets adgang til å bruke makt under et tjenesteoppdrag. Bestemmelsen skal mer forstås og fungere som en retningslinje for hvordan polititjenesten skal utføres, og stiller opp rettslige rammer for valg og bruk av virkemiddel. Ettersom det er politiloven § 6 fjerde ledd som gir politiet hjemmel til å anvende makt ved iverksettelsen av blant annet straffeprosessuelle tiltak, er det naturlig å gå nærmere inn på denne bestemmelsen.

Det følger av Høyesteretts dom<sup>34</sup> av 23.08.2007 at politiloven § 6 fjerde ledd *må* sees i sammenheng med ordlyden i annet ledd som sier at *«politiet ikke skal ta i bruk sterkere midler uten at svakere midler på antas utilstrekkelig eller uhensiktsmessige, eller uten at slikt forgjeves har vært forsøkt»*. Det er også et krav etter annet ledd annet punktum at middelet må være forholdsmessig og nødvendig. Politiinstruksen<sup>35</sup> § 3-2 beskriver også politiets bruk av makt, og det fremkommer av bestemmelsens første ledd at *«politiet kan bruke makt under iverksettelse og gjennomføring av en tjenestehandling når dette følger av lov eller sedvane, og det ellers finnes klart nødvendig og forsvarlig i betraktning av situasjonens alvor, følgene for*

---

<sup>34</sup> Rt. 2007 s. 1172

<sup>35</sup> F.28.06.1985 nr. 1679. Forskrift om ordningen av påtalemyndigheten (Påtaleinstruksen)

*den maktanvendelsen rettes mot og forholdene for øvrig». Det er altså et krav om at politiets bruk av makt må være nødvendig og forsvarlig.*

Makt defineres ikke videre i politiloven, men det fremkommer av forarbeidene<sup>36</sup> til politiloven, og av politiinstruksen § 3-2 annet ledd, at det med makt menes tvangsmessige fysiske inngrep mot person eller eiendom. Det fremkommer av forarbeidene<sup>37</sup> til endringene av straffeprosessloven § 199 a at *«det er en forutsetning at den bestemmelsen som hjemler selve beslutningen eller pålegget som politiet skal gjennomføre, direkte eller indirekte forutsetter at det kan gjennomføres ved bruk av fysisk makt»*. Dette har lovgiver sikret i straffeprosessloven § 199 a annet ledd hvor det fremkommer at politiet kan gjennomføre autentisering ved bruk av tvang. I de samme forarbeidene stilles det et spørsmål om tvangsgjennomføring av biometrisk autentisering ved ransaking av et datasystem *«kan anses omfattet av politiets rett og plikt til å benytte makt ved utøvelsen av tjenestemessige oppgaver?»*.

I forarbeidene<sup>38</sup> blir dette inngrepet sammenlignet med å tvangsflytte en person som fysisk sperrer for inngangsdøren til et hus som skal ransakes, og det fremkommer at det *«i begge tilfeller er tale om å overkomme en faktisk hindring for å skaffe tilgang til informasjon som i prinsippet er rettslig tilgjengelig»*. Videre fremkommer det at den tvangsmessige gjennomføringen av biometrisk autentisering må anses som *«et aksessorium til det opprinnelige tvangsmiddelet»*. Hvor langt dette synspunktet rekker er usikkert og vil avgjøres når domstolene i fremtiden behandler saker hvor et slikt inngrep er brukt. Forskjellen på å tvangsflytte en person som fysisk hindrer politiet fra å gjennomføre en ransaking, og det å tvinge frem en biometrisk autentisering, vil være at det ved sistnevnte inngrep *«tvangsmessig gjøres bruk av mistenktes personopplysninger»*. Det særegne ved straffeprosessloven § 199 a er at bruken av slike personopplysninger ikke bare kan ramme mistenkte, men også enhver som er i befatning med et datasystem som er gjenstand for ransaking.

---

<sup>36</sup> Ot.prp. nr. 22 (1994-1995), avsnitt 2.5 Politiets maktbruk

<sup>37</sup> Prop.106 L (2016-2017), s. 4.

<sup>38</sup> Prop.106 L (2016-2017), s. 4.

### 3.2 STRAFFEPROSESSLOVEN § 170 A

Straffeprosessloven § 170 a lyder som følger; «*Et tvangsmiddel kan brukes bare når det er tilstrekkelig grunn til det. Tvangsmidlet kan ikke brukes når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep*». Det følger av bestemmelsens forarbeider<sup>39</sup> at straffeprosessloven § 170 a skal gjelde for alle bestemmelsene som ligger under straffeprosesslovens del fire (tvangsmidler). Regelen vil dermed gjelde ved politiets anvendelse av straffeprosessloven § 199 a.

Straffeprosessloven § 170 a oppstiller to prinsipper. Det ene er kravet om «*tilstrekkelig grunn*», gjerne omtalt som «*behovsprinsippet*» eller «*nødvendighetskravet*». Det andre er kravet om at «*tvangsmidlet ikke kan brukes når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep*». Dette omtales gjerne som «*proporsjonalitetsprinsippet*» eller «*forholdsmessighetsprinsippet*». Dette innebærer at selv om forutsetningene og adgangen til å anvende et tvangsmiddel er tilstede, så er det dermed ikke alltid slik at tvangsmidlet bør brukes. Høyesterett<sup>40</sup> har uttalt at bestemmelsens første punktum har sin selvstendige betydning ved siden av annet punktum, slik at selv om tvangsmidlet ikke vil være å betrakte som et uforholdsmessig inngrep, så er det ikke gitt at det er tilstrekkelig grunn til å bruke det. Johs Andenæs skriver<sup>41</sup> at «*det er til dels tale om alvorlige inngrep overfor den som rammes, og loven forutsetter at det skal vurderes om det alt i alt er rimelig å gå til et slikt inngrep*». Andenæs<sup>42</sup> skriver videre at det i forholdsmessighetsvurderingen må legges vekt på hvor alvorlig saken er, hvor sterk mistanke som foreligger, hvor stor skade eller påkjenning bruken av tvangsmidlet vil ha, og hvor påkrevd bruken av tvangsmidlet vil være for at saken skal oppklares.

Når det gjelder forholdsmessighetsvurderingen følger det av forarbeidene<sup>43</sup> til straffeprosessloven § 170 a at prinsippet har betydning både «*for spørsmålet om et tvangsmiddel kan brukes og for spørsmålet om hvor lenge et tvangsmiddel skal brukes, eventuelt om det skal opphøre før lengstefristen har løpt ut*». Dette innebærer at man hele tiden må vurdere nødvendigheten samt om kravet til tilstrekkelig grunn er tilstede.

---

<sup>39</sup> Ot.prp.nr.64 (1998-1999) s. 163

<sup>40</sup> Rt. 1988 s. 358

<sup>41</sup> Johs Andenæs, *Norsk straffeprosess*, 4.utgave, Universitetsforlaget 2009, s. 280

<sup>42</sup> Johs Andenæs, 2009, s. 280

<sup>43</sup> Ot.prp.nr.64 (1998-1999) s. 147

## 4.0 RETTSSIKKERHETSMESSIGE BETENKELIGHETER

En av årsakene til at vi fattet interesse for denne bestemmelsen var at lovgiver åpnet opp for bruk av makt overfor en «uskyldig» tredjeperson. Hva slags problemer skaper dette? Utfordrer dette noen av rettsstatens sentrale prinsipper?

### 4.1 LEGALITETSPRINSIPPET

For at myndighetene skal kunne gjøre inngrep ovenfor borgere oppstilles det i norsk rett et krav om at dette inngrepet har et hjemmelsgrunnlag. Dette prinsippet omtales som legalitetsprinsippet. Legalitetsprinsippet kalles gjerne lovskravet, hvor det med dette menes at et hvert inngrep fra myndighetene må ha hjemmel i lov. Prinsippet innebærer også at domstolene kan føre kontroll med at myndighetene har hjemmel til å foreta de inngrep som gjøres.

Hensikten med legalitetsprinsippet er å sikre borgernes rettsikkerhet og frihet, slik at maktøvelsen fra myndighetene ikke blir gjort vilkårlig<sup>44</sup>. Det sentrale i legalitetsprinsippet er at inngrep fra myndighetene skal være forutberegning for borgerne. Tidligere var ikke legalitetsprinsippet nedfelt i grunnloven, men prinsippet var likevel å betrakte som konstitusjonell sedvanerett, noe som betød at prinsippet ble ansett for å ha samme trinnhøyde som Grunnloven. I 2014 ble legalitetsprinsippet kodifisert i Grunnloven § 113 som sier at *"Myndighetenes inngrep overfor den enkelte må ha grunnlag i lov"*.

Legalitetsprinsippet kommer til uttrykk i flere av bestemmelsene i Grunnloven. Etter Grunnloven § 96 følger det at ingen kan dømmes uten etter lov, eller straffes uten etter dom, etter Grunnloven § 97 kan ingen lov gis tilbakevirkende kraft, og etter Grunnloven § 98 er alle like for loven.

Begrepet «inngrep» omfatter mange av de handlingene som politiet kan foreta seg ovenfor borgere. Politiet utøver mange verbale/bestemmende inngrep i form av pålegg og advarsler, videre gjør politiet fysiske inngrep ved eksempelvis bruk av maktmidler som pepperspray, batong, slag/spark, og i ytterste konsekvens skytevåpen. I etterforskningsøyemed kan politiet gjøre inngrep mot borgere i form av ransaking, ta beslag, gransking og pågripelse.

---

<sup>44</sup> Fredriksen, 2015, s.161

Rimelige hensyn taler for at desto mer inngripende inngrepet er, desto større krav bør stilles til hjemmelsgrunnlaget. Det bør kunne stilles et strengere krav til hjemmelsgrunnlagets klarhet (klarhetskravet), tilgjengelighet og rimelighetshensyn når det er tale om bruk av makt. Maktutøvelsen som følger av straffeprosessloven § 199 a er hjemlet i norsk lov. Bestemmelsens ordlyd er moderne, og den gir lite rom for tvil om politiets adgang til å bruke makt.

Legalitetsprinsippet var bakgrunnen til behovet for endringen av straffeprosessloven § 199 a. Høyesterett i kjennelse<sup>45</sup> datert 30.08.2016 kom til at hverken straffeprosessloven § 157 eller straffeprosessloven § 199 a, slik den fremstod i 2016, ga hjemmel til at politiet kunne foreta et slikt inngrep som var tema i den aktuelle saken.

## 4.2 PERSONVERNHEMSYN

Enhver har rett til et vern om sitt eget privatliv. Dette er grunnlovfestet i Grunnloven<sup>46</sup> § 102 hvor det står at *«enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.»*. Den europeiske menneskerettskonvensjonen<sup>47</sup> angir i artikkel 8 at *«enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.»*. Vernet om privatlivets fred er således både grunnlovfestet og en menneskerettighet som alle har i kraft av å være mennesker.

Grunnloven angir i § 102 at et unntak fra privatlivets fred vil være i kriminelle tilfeller. I disse tilfellene vil det være adgang til å foreta (hus)ransakelse. I dette kan det tenkes at lovgiver her har tenkt på de tilfellene hvor det er den som mistenkes for å ha begått den straffbare handlingen, at inngrepet i vernet om privatlivets fred foretas.

I medhold av straffeprosessloven § 199 a kan politiet foreta ransaking av et datasystem. Siden bestemmelsen angir at pålegget etter første ledd og tvangsutøvelsen etter annet ledd kan rettes

---

<sup>45</sup> HR-2016-1833-A

<sup>46</sup> Lov av 17. mai 1814, Kongeriket Norges Grunnlov

<sup>47</sup> Lov av 4. november 1950, Den europeiske menneskerettskonvensjonen

mot «enhver», vil dette som tidligere nevnt innebære at politiet vil kunne få tilgang til et datasystem som tilhører personer som ikke er mistenkt eller siktet i en straffesak.

Med dagens teknologi kan mobiltelefoner og bærbare PCer på mange måter sies å være en stor og viktig del av mange personers privatliv, hvor eksempler på dette kan være bank-ID på mobil (innlogging i nettbank ved bruk av mobiltelefon), apple-pay (betaling med bruk av mobiltelefon) og helseapper med privat informasjon om egen helse. De fleste har også store «fotoalbum» på sin mobil. I de tilfellene politiet får tilgang til en mobiltelefon etter at eieren har åpnet denne ved bruk av biometrisk autentisering så vil det være tilgjengelig en stor mengde med informasjon. Det kan reises spørsmål om hvorvidt et inngrep som nevnt ovenfor kan være i strid med vernet om privatlivets fred.

Siden begrepet «datasystem» i straffeprosessloven § 199 a utformet på en slik måte at den også vil inkludere den type teknologi som vi vil bruke i framtiden, er det nærliggende å tenke at det vil kunne tas i bruk systemer hvor vernet om privatlivets fred i enda større grad vil kunne utfordres ved anvendelsen av straffeprosessloven § 199 a.

### 4.3 SELVINKRIMINERINGSPRINSIPPET

*«Siktedes rett til å forholde seg taus er ansett som et grunnleggende krav til en god straffeprosess».*<sup>48</sup> Denne retten kommer blant annet til uttrykk i straffeprosessloven § 90 og i § 232, hvor det står at henholdsvis siktede og mistenkte ikke har en plikt til å forklare seg. Høyesterett<sup>49</sup> har poengtert at *«det er et grunnleggende rettsstatsprinsipp at den som er mistenkt for en straffbar handling, har rett til å forholde seg taus, og ikke har noen plikt til å bidra til egen straffelse.»* Denne saken handlet om en fengselsbetjent som hadde blitt domfelt for å ha hjulpet en innsatt med å rømme fra fengselet som betjenten arbeidet ved. Som bevis hadde påtalemyndigheten benyttet en forklaring som var tatt opp med skjult mikrofon og båndopptaker. Dette beviset ble ansett for å være ulovlig ervervet da den fremgangsmåten som hadde blitt benyttet, ikke i tilstrekkelig grad respektert mistenktes rett til å forholde seg taus.

Selvinkrimineringsprinsippet fremkommer ikke direkte av den europeiske menneskerettskonvensjonen (EMK), men den europeiske menneskerettsdomstolen (EMD) har

---

<sup>48</sup> Johs Andenæs, 2009 s. 56

<sup>49</sup> Rt.1999 s.1269

innfortolket dette prinsippet i EMK artikkel 6 nr. 1<sup>50</sup>. FN-konvensjonen av 16. desember 1966 om sivile og politiske rettigheter gir også uttrykk for prinsippet i artikkel 14 nr. 3 bokstav g hvor det fremkommer at enhver som er siktet for en straffbar handling har rett til «*ikke å bli tvunget til å vitne mot seg selv eller erkjenne seg skyldig*».

Norge har gjennom menneskerettsloven<sup>51</sup> § 2 gjort den europeiske menneskerettskonvensjonen og FN-konvensjonen av 16. desember 1966 om sivile og politiske rettigheter til norsk rett. Dersom det oppstår uenighet mellom noen bestemmelser i straffeprosessloven og menneskerettighetskonvensjonene skal konvensjonene gis forrang.

Det ovennevnte gir et godt bilde av hvor sterkt vernet mot selvinkriminering står i norsk rett. Med hjemmel i straffeprosessloven § 199 a vil politiet kunne få tilgang til innholdet i et datasystem ved ransaking. Formålet med denne ransakingen er for å undersøke datasystemet for viktige bevis i en straffesak.

Politiet har mange hjemmelsgrunnlag for å få tilgang til og sikre bevis i en pågående etterforskning. Med hjemmel i straffeprosessloven § 192 kan politiet ransake mistenktes bolig, rom eller oppbevaringssted når noen med skjellig grunn mistenkes for en handling som etter loven kan medføre frihetsstraff. Det er klart at en ransaking etter straffeprosessloven § 192 ikke innebærer noe brudd på vernet mot selvinkriminering. I disse tilfellene vil politiet ta seg til stedet, og uten noen form for bistand fra mistenkte, foreta ransakingen. Dersom mistenkte ikke slipper politiet inn eller gir politiet nøkler, vil politiet kunne finne andre muligheter for å ta seg inn i på stedet hvor ransakingen skal finne sted. Ransaking etter straffeprosessloven § 192 vil i mange tilfeller ikke kreve mistenktes innblanding.

Det som er interessant med den type ransaking som følger av straffeprosessloven § 199 a, ransaking av et datasystem, er at politiet med hjemmel i bestemmelsens annet ledd ved bruk av makt kan tvinge fram tilgangen. Maktutøvelsen vil i disse tilfellene rette seg direkte mot mistenkte, eller «*enhver som har befatning med datasystemet*», og tilgangen til datasystemet vil da skje som et resultat av at politiet tvinger mistenkte/siktede, eller «*enhver*», til å aktivt bruke sin egen kropp til å gi politiet adgang til datasystemet. Selvinkrimineringen vil således ikke være å gi tilgang på informasjonen i seg selv, men den aktive handlingen ved å bruke

---

<sup>50</sup> *Funke mot Frankrike*, EMD-dom av 25. februar 1993

<sup>51</sup> Lov av 21. mai 1999 nr. 30 Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)

kroppen (biometri) som et redskap for å gjøre informasjonen tilgjengelig.

I forarbeidene til lovforslaget sammenlignet justis- og beredskapsdepartementet det å tvinge mistenkte til å gi fra seg en nøkkel til en lås, med det å utnytte kjennetegn som utgår fra kroppen. Departementet uttalte at *«kjennetegnet eksisterer uavhengig av mistenktes vilje og stiller ikke mistenkte overfor et valg om å lyve eller angi seg selv. Det er tale om en faktisk hindring som står i veien for tilgang til informasjon som allerede er rettslig tilgjengelig ved at det er gjenstand for ransaking eller tatt i beslag. Det kan imidlertid ikke utelukkes at det kan oppstå situasjoner der selvinkrimineringsvernet setter en skranke for tvangsgjennomføring av biometrisk autentisering<sup>52</sup>»*. Som et eksempel på dette viste departementet<sup>53</sup> til tvangsgjennomføring av stemmegjenkjenning, og at det i disse tilfellene ville kunne gå en grense for når tvangsutøvelsen var i strid med vernet mot selvinkriminering.

Dette innebærer dermed at enkelte former for tvangsutøvelse i medhold av straffeprosessloven § 199 a kan være i strid med selvinkrimineringsvernet, og at dette vernet også må vurderes opp mot andre former for biometrisk autentisering etter hvert som den teknologiske utviklingen fortsetter. Jusprofessor Hans Fredrik Marthinussen uttalte, i forbindelse med at lovendringen trådte i kraft 1. juli 2017, til NRK at *«de fleste oppegående advokater vil utprøve dette så snart virkemidlet tas i bruk av politiet, og det er ikke gitt at dette står seg i fremtiden<sup>54</sup>»*.

---

<sup>52</sup> Prop.106 L (2016-2017) s.11

<sup>53</sup> Prop.106 L (2016-2017) s.12

<sup>54</sup> <https://www.nrk.no/norge/na-kan-politiet-tvinge-deg-til-a-lase-opp-telefonen-din-1.13572392>



## 5.0 AVSLUTNING

Den teknologiske utviklingen som finner sted skaper uten tvil et behov for at det også skjer en utvikling i norsk straffeprosess når det gjelder anvendelsen av tvangsmidler. Politiet skal i medhold av politiloven § 2 avdekke og stanse kriminell virksomhet og forfølge straffbare forhold, og det er klart at et oppdatert og moderne regelverk må ligge til grunn for at politiet skal løse sitt samfunnsoppdrag.

Endringen i straffeprosessloven § 199 a som kom i 2017 skjedde svært raskt, og man anså at det ikke var et alternativ til å vente til en ny straffeprosesslov kom på plass. Sett hen til at både tingretten og lagmannsretten i 2016 vurderte at politiet med hjemmel i straffeprosessloven § 157 kunne tvinge noen til å åpne et datasystem ved bruk av biometrisk autentisering, så kan dette tyde på at politiet, fram til dette tidspunktet, kan ha handlet i strid med loven. At et enstemmig Høyesterett i 2016 kom til det motsatte resultat, og at lovgiver dermed måtte gjøre en lovendring, er et godt eksempel på hvordan Norge som en rettsstat fungerer.

Det fremstår som noe unikt i norsk straffeprosess at politiet, i en ransakingssituasjon, kan bruke tvang overfor en tredjeperson. Som nevnt under kapittel 4.3 så vil selvinkrimineringsvernet fungere som en skranke for rekkevidden av tvangsutøvelsen og maktutøvelsen som bruken av straffeprosessloven § 199 a gir, det samme vil politiloven § 6 og straffeprosessloven § 170 a. Dette gir grunn til å tro at Høyesterett i framtiden vil måtte definere anvendelsesområdet og den lovlige bruken av straffeprosessloven § 199 a etter hvert som den teknologiske utviklingen fortsetter.

## 6.0 KILDELISTE

### **Lover:**

Lov av 17. mai 1814, Kongeriket Norges Grunnlov

Lov av 4. november 1950, Den europeiske menneskerettskonvensjonen

Lov av 22. Mai 1981, nr. 25 om rettergangsmåten i straffesaker (Straffeprosessloven)

Lov av 04. August 1995 nr. 53 Lov om politiet (politiloven)

Lov av 21. mai 1999 nr. 30 Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)

### **Domsregister:**

Rt. 1988 s. 358

Rt. 1993 s. 1302

Rt. 1999 s. 1269

Rt. 2007 s. 1172

Rt. 2016 s. 1833

HR-2016-1833-A

HR-2019-610-A

LG-2016-62717

TJARE-2016-43883

### **Forarbeider:**

Prop. 106 L (2016-2017) Endringer i straffeprosessloven (biometrisk autentisering)

Ot.prp. nr. 22 (1994-1995) Om lov om politiet (politiloven)

Ot.prp.nr.64 (1998-1999) Om lov om endringer i straffeprosessloven og straffeloven m v (etterforskningsmetoder m v)

### **Forskrift:**

Forskrift om ordningen av påtalemyndigheten (Påtaleinstruksen) av 28.06.1985 nr. 1679.

### **Avgjørelser fra den europeiske menneskerettighetsdomstol:**

Dom av 25. februar 1993, *Funke mot Frankrike*.

### **Litteratur:**

Andenæs, Johs. *Norsk straffeprosess*, 4.utgave, Universitetsforlaget, 2009

Bjerknes, Ole Thomas og Fahsing, Ivar A. *Etterforskning – Prinsipper, metoder og praksis*, 2. opplag, Fagbokforlaget (Bergen 2018)

Eckhoff, Torstein. *Rettskildelære*, 2007

Fredriksen, Steinar. *Innføring i straffeprosess*, 3. utgave, Gyldendal juridisk (Oslo 2015)

**Nettsider:**

<https://www.nrk.no/norge/na-kan-politiet-tvinge-deg-til-a-lase-opp-telefonen-din-1.13572392>

(februar 2019)

<https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/> (februar

2019)