UiT Norges arktiske universitet

Det juridiske fakultet

En analyse av reguleringen av biometriske personopplysninger i personvernforordningen og personopplysningsloven

Frida Åberg Mokkelbost

Masteroppgave i JUR-3902 høsten 2021

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling for avhandlingen

Temaet for denne avhandlingen er personvern. Problemstilling for oppgaven er hvordan regelverket rundt biometriske personopplysninger fungerer. Nærmere bestemt skal det foretas en redegjørelse og analyse av personvernregelverket rundt biometriske personopplysninger. Avhandlingen avgrenses således mot det generelle reguleringene av personopplysninger, selv om det også da regulerer biometriske personopplysninger.[1] Etter gjeldende rett er biometriske personopplysninger regulert i personvernforordningen art. 4 nr. 14[2], samt med en nasjonal regulering i pol. § 12[3].

Formålet med oppgaven er å foreta en rettsdogmatisk og rettspolitisk analyse av hvordan personvernregelverket fungerer i dag opp mot hvordan det muligens bør reguleres. Ettersom det finnes en tilleggsregulering i pol. § 12, kommer jeg til å ha et særlig fokus på hvordan den nasjonale reguleringen samsvarer med reguleringen i personvernforordningen, samt samfunnet ellers.

Det jeg ønsker å oppnå med avhandlingen er å kunne besvare spørsmålet om biometriske personopplysninger har gode og hensiktsmessige reguleringer, som fungerer i dagens samfunn. Hvis dette ikke kan bekreftes, ønsker jeg å se på hvordan reguleringen av biometriske personopplysninger bør være. Eventuelle endringer i regelverket vil i så fall forekomme i den nasjonale reguleringen av biometriske personopplysninger, ettersom Stortinget kun har myndighet til å vedta lover som binder innenfor Norges grenser.[4]

1.2 Bakgrunn og aktualitet

Det er relativt vanlig i vårt samfunn å knytte rettigheter opp mot identitet, i den forstand man får tilgang til rettigheter knyttet opp mot individets identitet gjennom å identifisere vedkommende. Med ordet biometri sikter man til «automatiserte systemer for gjenkjenning

[1] Se redegjørelsen for den rettslige reguleringen av biometriske personopplysninger i pkt. 3.2.
[2] Europaparlamentet og Rådets forordning 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (heretter personvernforordningen).
[3] Lov 15 juni 2018 nr. 38 om behandling av personopplysninger (heretter pol.).
[4] Jfr. lov 17 mai 1814 kongeriket Norges Grunnlov § 75 bokstav a.

ved å ta i bruk unike målbare biologiske kjennetegn».[5] Biometri egner seg særlig godt til slik identifisering og autentisering av tre grunner. For det første fordi det er universelt, i den forstand at alle mennesker har en biometrisk kode. På den måten kan biometriske personopplysninger brukes til identifisering og autentisering på tvers av landegrenser. For det andre er biometri konstant, det kan ikke endres og ikke ødelegges. Biometri er, for det tredje, entydig. Din biometriske kode peker kun tilbake til deg, slik at man ved identifisering eller autentisering i liten grad risikerer at feil person får tilgang til det som identifiseringen skulle åpne for.[6]

Det foreligger en økende trend ved bruk av biometri i hverdagen. Praksis fra Personvernnemnda, som avhandlingen skal ta for seg senere, viser en variert bruk av fingeravtrykk som en biometrisk personopplysning, innen flere forskjellige bransjer. I Kina har de innført bruk av kameraovervåkning for å identifisere enkeltindividet, og på bakgrunn av dette bygge opp en sosial profil på hvert individ for å regulere borgernes atferd.[7] Og Amazon har nylig åpnet sin første matvarebutikk, uten noen ansatte, der de blant annet bruker kameraovervåking for å vite hva kundene legger ned i handlekurven sin.[8] Dette er eksempler som skaper et bilde av en omfattende bruk av biometri, over hele kloden.

Norge er gjennom EØS-avtalen bundet av EUs forordning om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.[9] [10] Personvernforordningen er innholdsmessig langt mer omfattende enn personopplysningsloven, og er sånn sett å anse som hovedregelverket.[11] Personopplysningsloven er dermed et lovverk som supplerer personvernforordningen. Biometriske personopplysninger er på nasjonalt nivå regulert under pol. § 12. Dette er en bestemmelse som ikke har blitt oppdatert siden 2000, ettersom den ble videreført fra den tidligere personopplysningsloven ved ny lov i 2018. I tillegg foreligger det begrenset med

---

[5] Jfr. Nasjonalt ID-senter, *Biometri og identitet: utfordringer og nye muligheter for utlendingsforvaltningen,* nidsenter.no fotnote 7. Se også pkt. 3.1 i avhandlingen.
[6] Artikkel 29 – Gruppen vedrørende datasikkerhet, *Arbejdsdokument om biometri,* (2003) s. 3.
[7] Gry Blekstad Almås, *Digitalt diktatur: Kina planlegger sosialt poengsystem,* nrk.no.
[8] Maggie Tillman, *Amazon Go and Amazon Fresh: How the 'Just walk out' tech works,* pocket-lint.com.
[9] Se redegjørelsen for forordningen, og forholdet mellom forordningen og personopplysningsloven i pkt. 2.3 og 5.1.
[10] Jfr. pol. § 1.
[11] Schartum (2020) s. 31.

rettsavgjørelser og praksis som utdyper, tolker og utvikler loven videre. De siste avgjørelsene er fra Personvernnemnda, avsagt i 2011, altså syv år før den nye loven trådte i kraft.

Ved vedtakelsen av den nye personopplysningsloven i 2018 ga Justis- og beredskapsdepartementet uttrykk for å være i en avventende situasjon, og der man må se an hvordan regelverket blir anvendt før man foretar noen flere endringer i bestemmelsen. Dette kommer blant annet til uttrykk gjennom at departementet for vurderingen av om biometriske personopplysninger bør reguleres under samme bestemmelse som identifikasjonsnummer sier at «behandlingen [bør] etter departementets oppfatning *inntil videre* reguleres i samme bestemmelse» (mine kursiveringer).[12] Til nå, i 2021, er det ikke foretatt noen videre vurdering av hvordan regelverket fungerer. Det dette sier oss er at foreligger lite rettsavklaring rundt et tema som bare blir brukt mer og mer.

Lover og regler må utvikle seg i takt med samfunnsutviklingen, slik at gjeldende rett best mulig samsvarer med fungerende rett. For behandling av biometriske personopplysninger er dette særlig viktig fordi det er en form behandling av personopplysninger som er sterkt inngripende overfor enkeltindividet.[13]

Jeg har valgt å se særlig på biometriske personopplysninger fordi jeg tror det kommer til å skje en betydelig utvikling ved bruken av dette, som vi kun har sett begynnelsen av. Ser man dette opp mot den risikoen som kan foreligge ved behandling av biometriske personopplysninger, og at lovene allerede kan være utdatert, mener jeg det er nødvendig og hensiktsmessig å stille seg spørsmålet om regelverket fungerer bra nok slik det er i dag, eller om det bør oppdateres. For en ting er helt sikkert; teknologi er kommet for å bli, og det eneste vi kan søke og gjøre er å opprette en balansert regulering som beskytter enkeltindividet, men likevel stimulerer til en videre utvikling av teknologi i takt med samfunnsutviklingen.

1.3 Videre fremstilling for avhandlingen

I kapittel 2 skal jeg kort gjøre rede for hvordan rettskildebildet i avhandlingen er, og hvilke rettskilder jeg har anvendt for å besvare problemstillingen min.

[12] Jfr. Prop. 56 LS (2017-2018) s. 56.
[13] Se mer pkt. 3.3 for utfordringer med behandling av biometriske personopplysninger.

I kapittel 3 skal jeg gjøre rede for hva biometriske personopplysninger er og hvordan de reguleres i personvernforordningen.

I kapittel 4 skal jeg se nærmere på hva som er å anse som behandling av personopplysninger[14], og da særlig hva som ligger i kravet til en «særskilt teknisk behandling».[15]

I kapittel 5 skal jeg se nærmere på den nasjonale reguleringen av biometriske personopplysninger i pol. § 12. Jeg skal se nærmere inn i ordlyden «entydige identifikasjonsmidler», og vurdere forholdet mellom identifikasjonsnummer og biometriske personopplysninger.

Til sist skal jeg i kapittel 6 oppsummere hva jeg har sett på i avhandlingen, før jeg prøver å besvare spørsmålet om trengs det en ny regulering av biometriske personopplysninger, og, i så fall, hvordan ordlyden til en slik bestemmelse bør være.

2 Metode og rettskilder

2.1 Generelt om rettskildebildet i avhandlingen

Det er særlig to tendenser som preger det nasjonale rettskildebildet når det kommer til personvernregelverket.

For det første at det foreligger lite rettsavklaring fra tingrett, lagmannsrett og Høyesterett for tolkning av personopplysningsloven. Dette ser man blant i Høyesterett, der det de siste tjue årene kun er avsagt seks avgjørelser som tolker personverndirektivet/personvernforordningen og/eller personopplysningsloven.[16] Og ingen av disse avgjørelsene tolker eller anvender regelverket rundt biometriske personopplysninger.

Det er vanskelig å si noe om hvorfor det foreligger lite rettsavklaring nasjonalt, men det kan blant annet ha sammenheng med at klager på vedtak fra Datatilsynet først behandles i klageinstans, Personvernnemnda, før det eventuelt klages inn til tingretten. Man har altså et

[14] Personopplysningsregelverket trer først i kraft ved behandling av personopplysninger, se personvernforordningen art. 2 nr. 1.
[15] Jfr. personvernforordningen art. 4 nr. 14.
[16] Rt. 2001 s. 428, Rt. 2002 s. 1500, Rt. 2004 s. 878, Rt. 2012 s. 1669, Rt. 2013 s. 143, HR-2021-966-A, og HR-2021-2403-A.

organ til, før retten, der tvisten kan søkes løst, uten at partene må betale sakskostnader for dette. Under dette argumentet kan det sikkert også trekkes frem at det er kan være en kostnadsfull affære å ta en sak til retten.

Problemet med manglende praksis fra, særlig Høyesterett, er at det er et rettsområde der det foreligger et særlig behov for en dynamisk tolkning og utvikling av regelverket. Således vil Høyesteretts rolle som en rettsavklarende og rettsutviklende institusjon, kunne ha kommet med viktige bidrag til denne utviklingen.[17]

For det andre er personvernregelverket[18] er også preget av at store deler av lovgivningen er gitt gjennom en forordning som Norge, gjennom EØS-avtalen, er bundet av.[19] Personvernforordningen er et stort, og tidvis tungt regelverk, slik at det finnes et stort utvalg av kilder fra EU og organer under EU, som kommer med rådgivende uttalelser om hvordan regelverket skal forstås. Det foreligger således betraktelig mer med rettskilder når det kommer til personvernforordningen, og ettersom Norge er bundet av forordningen, oppstår det da et spørsmål om i hvilken grad vi kan være bundet av de øvrige rettskildene fra et internasjonalt plan.

2.2 Personopplysningsloven

Personopplysningsloven trådte i kraft i 2018, og erstattet med dette den tidligere lov 14 mars 2000 nr. 31 om behandling av personopplysninger. Det fremkommer av forarbeidene til loven, Prop. 56 LS (2017-2018), at hovedformålet med loven er å gjennomføre personvernforordningen i norsk rett.[20] Mange av bestemmelsene i personopplysningsloven vil således bare være en videreføring av den tilsvarende ordlyd i personvernforordningen.

Forholdet mellom personvernforordningen og personopplysningsloven er slik at personvernforordningen er hovedregelverket.[21] Personopplysningsloven supplerer personvernforordningen med nasjonale bestemmelser, der personvernforordningen åpner for

[17] Begrepet rettsavklarende og rettsutviklende institusjon er hentet fra Ot.prp. nr. 51 (2004-2005) s. 302.
[18] Til orientering vil jeg i denne avhandlingen henvise til personvernforordningen og personopplysningsloven ved «personvernregelverket». Dersom det kun er meningen å henvise til en av de to, vil dette blir presisert i fortløpende.
[19] Se pol. § 1.
[20] Jfr. Prop. 56 LS (2017-2018) s. 8.
[21] Schartum (2020) s. 31.

det.[22] I de tilfeller der personopplysningsloven viderefører personvernforordningen, kommer jeg videre i avhandlingen kun å vise til personvernforordningens regulering.

2.3 Personvernforordningen

Personvernforordning ble vedtatt av EU i 2016. Forordningen erstattet med dette det tidligere personverndirektivet av 1995.[23] I motsetning til direktiv, som kun er bindende utfra sitt formål, får en forordning direkte virkning ved de konkrete bestemmelser.[24]

Det norske rettssystemet er bygget opp rundt en dualistisk tankegang. Det vil si at nasjonal og internasjonal rett blir sett på som to forskjellige rettssystemer.[25] Som en konsekvens av dette må all internasjonal rett gjennomføres internt i norsk rett, for å få anvendelse i Norge, enten gjennom inkorporasjon eller transformasjon.[26] [27] Personvernforordningen er gjennomført i norsk lov ved inkorporering gjennom personopplysningsloven.[28] Forordningen gjelder således som norsk lov, og det fremkommer også av §2 i loven at den har forrang for annen formell lov: «bestemmelsene i personvernforordningen går i tilfelle konflikt foran bestemmelser i annen lov som regulerer samme forhold».[29]

Forordningen er delt opp i to deler; fortalen til forordningen og de påfølgende artiklene.

2.3.1 Fortalen til personvernforordningen

Fortalen er en del av forordningen, og således en del av den helhet som medlemslandene har bundet seg til å gjennomføre. Før fortalen blir presentert foreligger det følgende ordlyd: «Europarlamentet og Rådet for den europeiske union har … ut fra følgende betraktninger …», hvor så fortalen følger. Etter fortalen kommer så følgende ordlyd: «vedtatt følgende forordning», hvorpå de konkreten artiklene i forordningen følger. Det er altså kun artiklene som er selve forordningen. Ut fra denne ordlyden fremstår det som klart at det kun er

[22] Se avhandlingens pkt. 3.2.
[23] Jfr. personvernforordningen art. 94
[24] Jfr. Traktat om den europeiske unions virkemåte (heretter TEUV) art. 288 nr.2 og nr.3.
[25] Jfr. Knut Einar Skodvin, *Dualisme,* snl.no 1 avsnitt.
[26] Jfr. Knut Einar Skodvin, *Dualisme,* snl.no 1 avsnitt.
[27] Ved inkorporasjon vedtas det ved lov eller forskrift at relevant internasjonal konvensjon, traktat eller forordning skal få direkte virkning som norsk rett. Transformasjon innebærer at internasjonal rett blir gjennomført ved vedtakelsen av en norsk lov som gjengir bestemmelsene i norsk språkdrakt jfr. Skoghøy (2018) s. 39.
[28] Se pol. § 1.
[29] Jfr. pol. § 2 fjerde ledd.

artiklene som er vedtatt, og således rettslig bindende. Fortalen er således ikke rettslig bindende.

I personvernforordningen blir altså ordlyden «betraktninger» brukt om fortalen. En naturlig språklig forståelse av «betraktninger» kan være forhold som er tatt hensyn ved utarbeidelsen av forordningen. På mange måter har slike betraktninger mange likhetstrekk med de betraktninger og formålsvurderinger man finner i forarbeider til norsk lov, og også formålsbestemmelser som man ofte finner i norske lover, dog betraktelig mer omfattende enn de.[30] Wien-konvensjonen regulerer hvordan internasjonale avtaler skal tolkes.[31] Norge har ikke ratifisert avtalen, men er likevel bundet av ordlyden da konvensjonens er å anse som folkerettslige sedvane.[32] Det følger av art. 31 blant annet at traktater skal tolkes «in the light of its object and purpose», noe som henviser til formålet med traktaten. Betraktningene i fortalen viser, som nevnt, til formålet med forordningen, og på bakgrunn av uttalelsen i art. 31 av Wien-konvensjonen, bør den dermed tillegges vekt ved tolkning av avtalen.

I samme retning trekker rettspraksis. I E-9/97, Erla María Sveinbjörnsdóttir mot Island, måtte EFTA-domstolen, blant annet, komme med en rådgivende uttalelse om hvorvidt staten var erstatningsansvarlig overfor Sveinbjørnsdottir.[33] For dette spørsmålet la domstolen vekt på fortalen til EØS-avtalen, som en viktig kilde.[34] At fortalen er en viktig rettskilde for tolkning av EU-retten er også bekreftet i juridisk teori.[35]

2.4 Ot.prp.nr.92 (1998–1999) om lov om behandling av personopplysninger (personopplysningsloven)

Dette forarbeidet er knyttet til den tidligere personopplysningsloven av 2000. Denne loven er nå opphevet og erstattet av personopplysningsloven av 2018. Forarbeider vil i utgangspunktet være en sentral rettskilde, fordi det kan gi uttrykk for lovgivers vilje og formål med loven. Det er på bakgrunn av dette at Prop. 56 LS (2017-2018), som forarbeidene til

[30] Se for eksempel lov 17 juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven) § 1-1.
[31] Vienna Convention on the Law of Treaties, Wien, 23 mai 1969.
[32] Utenriksdepartementet, *Folkerett,* regjeringen.no.
[33] E-9/97 Sveinbjørnsdottir avsnitt 7.
[34] E-9/97 Sveinbjørnsdottir avsnitt 49–52.
[35] Jfr. Sejersted, Arnesen, Rognstad og Kolstad (2011) s. 57.

personopplysningsloven av 2018, er en relevant rettskilde. Når loven er opphevet, vil dette dog i utgangspunktet medføre at forarbeidene til nevnte lov i stor grad mister sin relevans.

Selv om vedtakelsen av nye personopplysningslov i 2018 medførte en del endringer fra den tidligere loven fra 2000, er også flere deler av den tidligere loven videreført. For eksempel er bestemmelsen som regulerer biometriske personopplysninger videreført.[36] Når bestemmelser og ordlyd er videreført, tilsier dette gjerne at også lovgivers vilje og formål med loven i stor grad videreføres også. Noe som kan resultere i at forarbeidene fra tidligere lov også vil være relevant for tolkning av den nye loven.

Dette er tilfellet for Ot.prp.nr. 92 (1998-1999). I forarbeidet til personopplysningsloven av 2018, Prop. 56 LS (2017-2018), vises det flere steder til det tidligere forarbeidet. For eksempel gjennom ordlyden «…se Ot.prp.nr.92 (1998–1999) side 114 om bakgrunnen for bestemmelsen».[37] På bakgrunn av dette vil forarbeidene til personopplysningsloven av 2000 fortsatt være relevant for tolkning og vurdering av ordlyden i personopplysningsloven av 2018.

2.5 Forvaltningspraksis fra Datatilsynet og Personvernnemnda

Datatilsynet er et uavhengig forvaltningsorgan, og fungerer som tilsynsmyndighet for etterlevelse av personvernregelverket.[38] En uttømmende liste over tilsynsmyndighetens myndighet følger av personvernforordningen art. 58.[39] Personvernnemnda er et uavhengig forvaltningsorgan opprettet med hjemmel i pol. §22. Nemndas oppgave er å avgjøre klager over Datatilsynets vedtak.[40]

I avhandlingen har jeg brukt forvaltningspraksis fra Personvernnemnda og Datatilsynet som empirisk materiale, for å se hvordan ordlyden er forstått i praksis, og hvordan denne forståelsen har utviklet seg over tid. Det avsies flere avgjørelser i forvaltningsinstansene enn rettsinstansene. Det medfører at forvaltningsinstansene hyppigere kan vurdere ordlyden, og på den måten har et bedre grunnlag for å tolke loven både utfra hvordan den fungerer, men også

[36] Se redegjørelsen for bestemmelsens historiske bakgrunn i pkt. 5.2.
[37] Se blant annet Prop. 56 LS (2017-2018) s. 215.
[38] Se pol. §20 første og tredje ledd.
[39] Se personvernforordningen art. 58 nr. 1, nr. 2 og nr. 3.
[40] Jfr. pol. § 22 andre ledd.

hvordan den bør fungere i samfunnet. Det egner seg således godt til bruk som slikt empirisk materiale.

2.6 Retningslinjer og uttalelser fra EUs underinstanser

En utfordring med at det skal innføres et likt regelverk i flere forskjellige land, er at regelverket kan tolkes, forstås og gjennomføres på forskjellige måter. Det kan oppstå tvil om hvordan EU-retten skal forstås. Denne utfordringen kan blant annet søkes løst gjennom at EU-domstolen kan komme med uttalelser om hvordan EU-retten skal forstås.[41] En annen måte å søke dette løst på er at det kan komme utredninger og rådgivende uttalelser fra EUs underinstanser, som kan gi retningslinjer på hvordan EU-retten bør forstås. Et eksempel på et slikt rådgivende organ er Personvernrådet (på engelsk: European Data Protection Board), som er et uavhengig organ opprettet av EU.[42] Rådet skal «sikre en ensartet anvendelse» av personvernsforordningen, jfr. personvernforordningen art. 70 nr. 1, og består av representanter fra datatilsynsmyndighetene i EØS, samt det europeiske datatilsynet (på engelsk: European Data Protection Supervisor, som er datatilsynsmyndigheten for EU-organene.

Det ligger i ordlyden «retningslinjer» at man ikke er bundet av uttalelsene. Når det er sagt, er et av hovedformålet med å innføre en forordning, at regelverket skal være likt på tvers av landegrensene, og at man skal kunne sikre en ensartet tolkning. Da må uttalelser fra slike instanser fra EU kunne og burde tillegges vekt ved tolkning av personvernforordningen.

De nasjonale bestemmelsene i personopplysningsloven er gitt med hjemmel i personvernforordningen, og man ønsker en samsvarende behandling av personopplysninger på tvers av landegrensene. På bakgrunn av dette bør det kunne argumenteres for at man også i tolkning og anvendelse av de nasjonale bestemmelsene i personopplysningsloven kan illegge praksis og rådgivende uttalelser fra EUs underinstanser vekt. I samme retning trekker presumsjonsprinsippet, som medfører at man, så langt det er mulig, skal tolke norsk rett i samsvar med våre internasjonale forpliktelser, selv om disse reglene ikke har formell status som norsk lov.[43]

---

[41] Jfr. TEUV art. 260 nr. 1.
[42] Jfr. personvernforordningen art. 69 nr. 1.
[43] Jfr. Skoghøy (2018) s. 39.

3 Nærmere om biometriske personopplysninger; en redegjørelse for det faktiske og rettslige grunnlaget

3.1 Definisjonen av biometriske personopplysninger

Ordet biometri er satt sammen av to; «bios» som betyr liv og «metri» som sikter til å måle verdier, ordene satt sammen sikter således til å måle liv.[44] I en rapport fra nasjonal ID-senter blir biometri definert som «automatiserte systemer for gjenkjenning ved å ta i bruk unike målbare biologiske kjennetegn».[45] Slike biologiske mønstre kan være fysiologiske karaktertrekk som for eksempel fingeravtrykk, eller atferdsmessige, som for eksempel stemmeleie eller ganglag.[46]

Definisjonen av biometriske *personopplysninger* ble inntatt i personvernforordningen, ved vedtakelsen i 2016. Det fantes før det ingen regulering av biometriske personopplysninger i det tidligere personverndirektivet. At det da i 2016 kom inn en regulering av biometriske personopplysninger medførte at biometriske personopplysninger ble satt i et større fokus. Dette må også ses i sammenheng med at bruken av biometri trolig har økt siden personverndirektivet ble innført i 1995.

Det fremkommer av personvernforordningen art. 4 nr. 14 tre vilkår for at opplysninger er å anse som biometriske personopplysninger. For det første må opplysningene være å anse som personopplysninger etter definisjonen som fremkommer i art. 4. nr. 1. For det andre må opplysningene være behandlet ved en «særskilt teknisk behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige egenskaper». Det tredje vilkåret for behandling av biometriske personopplysninger er at opplysningene «muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person». Jeg skal nå se litt nærmere på hva disse vilkårene innebærer.

---

[44] Charlotte Bagger Tranberg, *Persondata og biometri i Skandinavien,* lovdata.no pkt. 2.
[45] Nasjonalt ID-senter, *Biometri og identitet: utfordringer og nye muligheter for utlendingsforvaltningen,* nidsenter.no fotnote 7.
[46] Jfr. Dag Wiese Schartum og Lee A. Bygrave, *Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12,* regjeringen.no (2008) s. 13 (heretter Schartum og Bygrave (2008)).

3.1.1 Definisjonen av personopplysninger i art. 4 nr. 1

Det første vilkåret retter seg mot at opplysningene som blir behandlet må være å anse som personopplysninger. Personopplysninger har sin legaldefinisjon i personvernforordningen art. 4 nr. 1.[47] Der fremkommer det at personopplysninger er «enhver opplysning om en identifisert eller identifiserbar person». Når ordlyden viser til at det er «enhver opplysning» må dette forstås slik at det ikke foreligger noen begrensninger i hvilke opplysninger det er. I den tidligere personopplysningsloven §2 nr.1 ble ordlyden «opplysninger og vurdering» brukt om hva personopplysninger er. Det er ingenting som tilsier at ordlyden skal være noe snevrere nå, enn det var i loven fra 2000. Trolig må da «vurderinger» også falle innenfor den svært vide ordlyden i personvernforordningens definisjon. Det har altså ikke noe betydning for definisjonen hvorvidt opplysningene er sanne, usanne, subjektive oppfatninger eller allment kjente.[48]

Det fremkommer av ordlyden at det må være opplysninger som medfører at en person «kan direkte eller indirekte identifiseres». Med direkte identifisering sikter man til de tilfeller der personopplysningen kan identifisere vedkommende alene. Eksempelvis vil et fingeravtrykk alene identifisere eieren av fingeravtrykket. I ordlyden «indirekte» identifisering ligger det nødvendigvis da det motsatte av direkte, altså at personopplysningen ikke alene kan identifisere vedkommende. Schartum har i juridisk teori brukt to eksempler for å vise distinksjonen mellom direkte og indirekte identifisering. For det første kan indirekte tilsi at identifisering ikke kan skje alene på bakgrunn av personopplysningen, men at det trengs flere teknikker. For det andre kan distinksjonen vise til hvor mange ledd det er mellom behandling av opplysningen og identifisering; et fingeravtrykk kan identifisere et individ med en gang, mens bilde av bilskiltet til et individ vil måtte gå gjennom flere ledd, før det kan identifisere eieren av bilen.[49] Poenget med distinksjonen er å få frem at det ikke er en forutsetning med personopplysninger at de i seg selv kan identifisere et individ, regelverket trer også i kraft der det trengs mer enn bare en personopplysning for å identifisere et individ.

Kravet til indentifisering reiser også spørsmålet om hvor den nedre grense for hva som er å anse som identifiserbare personopplysninger opp mot ikke-identifiserbare opplysninger. I Breyer mot Tyskland måtte EU-domstolen ta stilling til hvorvidt en IP-adresse var å anse som

---

[47] Legaldefinisjon er en definisjon fastsatt i lov, jfr. Erik Magnus Boe, *Legaldefinisjon,* snl.no.
[48] Eva Jarbekk, *Lovkommentar til GDPR art. 4 nr. 1,* lovdata.no pkt.1.
[49] Schartum (2020) s. 44.

en personopplysning.[50] Angående tolkning av daværende art. 2. bokstav a i personverndirektivet, som hadde en tilsvarende ordlyd som personvernforordningen art. 4 nr. 1, sa domstolen at man måtte vurdere hvorvidt IP-adresse utgjorde et middel som var «*reasonably* to be used to identify the data subject» (mine kursiveringer).[51] Domstolen baserer så denne vurderingen på om identifiseringen vil være «prohibited by law or practically impossible» utfra en vurdering av om det vil være uforholdsmessig utfra «terms of time, cost and man-power», på en slik måte at risikoen for identifisering i realiteten er ubetydelig.[52] Dersom dette kan besvares bekreftende, er personen ikke identifiserbar.

Det enkeltindividet som det blir behandlet personopplysninger om, kalles den registrerte.[53] Betegnelsen behandlingsansvarlig bruker man om den fysiske eller juridiske personen som ønsker å behandle personopplysninger, og således bestemmer formålet med behandlingen.[54] Den som behandler personopplysningene på vegne av en behandlingsansvarlig er en databehandler.[55]

3.1.2 Vilkåret om «særskilt teknisk behandling»

Det andre vilkåret retter seg mot hva slags behandling som må forekomme, for at personopplysninger er å anse som biometriske personopplysninger.[56] For at en opplysning skal være å anse som biometriske personopplysninger, må personopplysninger ha blitt behandlet gjennom en særskilt teknisk behandling.

Hva det innebærer at det må foreligge en særskilt teknisk behandling skal jeg se nærmere på i pkt. 4.2 i avhandlingen.

3.1.3 Personopplysningene må identifisere vedkommende

Det siste vilkåret er at opplysningene som er innhentet «muliggjør eller bekrefter en entydig identifikasjon av nevnte fysisk person». Ordlyden «entydig identifikasjon» sikter mot at behandlingen av de biometriske personopplysningene må kunne identifisere det fysiske

---

[50] En IP-adresse er en adresse som tildeles en enhet, som en PC, basert på et datanettverk, jfr. Wikipedia, *IP-adresse,* wikipedia.no første punktum.
[51] Jfr. *Breyer* [C5] C-582/14, avsnitt 45.
[52] Jfr. *Breyer* [C5] C-582/14 avsnitt 46.
[53] Personvernforordningen inneholder ingen definisjon av «registrert», men det kommer til uttrykk flere steder i personvernforordningen, se blant annet personvernforordningen art. 3 nr. 2.
[54] Jfr. personvernforordningen art. 4 nr. 7.
[55] Jfr. personvernforordningen art. 4 nr. 8.
[56] Se mer om behandling av biometriske personopplysninger i kapittel 4.

individet. Det følger videre av art. 9, som regulerer behandling av særlige kategorier av personopplysninger, at biometriske personopplysninger faller innenfor dersom det er «med det formål å entydig identifisere en fysisk person».[57] Ut fra ordlyden kan det virke rimelig klart at det kun foreligger behandling av biometriske personopplysninger dersom opplysningene blir brukt for å identifisere et enkeltindivid.

Ved bruk av biometriske personopplysninger har det blitt vanligere de siste årene å skille mellom identifisering og *autentisering.* Biometrisk identifikasjon vil si at man ved bruk av biometrisk data innhentet om vedkommende, og ved å sammenligne den med annen biometriske data besvarer spørsmålet «hvem er du?».[58] Biometrisk *autentisering* foreligger når man ved bruk av biometrisk data innhentet om vedkommende besvarer spørsmålet «er du den du utgir deg for å være?».[59] Vi kan bruke fingeravtrykk som et eksempel for å vise skillet. Ved bruk av fingeravtrykk for å identifisere, må man søke å finne det fingeravtrykket som er en nøyaktig match med det som blir presentert ut fra flere forskjellige fingeravtrykk. Der fingeravtrykk brukes for autentisering vil man kun sammenligne et fingeravtrykk med et annet, for å bekrefte eller avkrefte at disse er like. Ut fra ordlyden og definisjonen i art. 4 nr. 14 kan det virke som biometrisk autentisering faller utenfor ordlydens virkeområde.

Det finnes ingen rettskilde som konkret tar stilling til spørsmålet om ordlyden favner om autentisering eller ikke. Man finner dog flere rettskilder som sidestiller autentisering og identifisering på en slik måte at det kan være naturlig å tolke ordlyden utvidende slik at autentisering faller innenfor. Blant annet blir det i fortalen til personvernforordningen gitt uttrykk for at fotografier kun er å anse som en særlig kategori av personopplysninger etter art. 9 «bare når de behandles ved hjelp av et særskilt teknisk middel som gjør det mulig entydig å identifisere *eller autentisere* en fysisk person» (mine kursiveringer).[60] Uttalelsen i fortalen har blitt videreført i juridisk litteratur.[61] Schartum er av samme oppfatning: «inn under

[57] Jfr. personvernforordningen art. 9 nr. 1.
[58] Jfr. Tambiama Madiega og Hendrik Mildebrath, *Regulating facial recognition in the EU,* europarl.europa.eu (2021) s. 1.
[59] Jfr. Tambiama Madiega og Hendrik Mildebrath, *Regulating facial recognition in the EU,* europarl.europa.eu (2021) s. 1.
[60] Jfr. fortalen til personvernforordningen avsnitt 51.
[61] Personvernrådet, *Guidelines 3/2019 on processing of personal data through video,* edpb.europa.eu, (2019) s. 15.

identifisering må en trolig også regne autentisering, dvs. det å vise at en person er den han eller hun utgir seg for».[62]

Det finnes gode grunner som taler for at autentisering bør falle inn under ordlyden. Flere av de samme risikoene som oppstår ved bruk av biometriske personopplysninger for identifikasjon, vil også gjøre seg gjeldende ved bruk av biometriske personopplysninger for autentisering.[63] For eksempel vil innhenting av fingeravtrykk for autentisering kunne medføre de samme risikoene for misbruk som innhenting av fingeravtrykk med den hensikt å identifisere. Dette fordi det, uavhengig av om formålet er å identifisere eller autentisere, blir brukt den samme biometriske personopplysningen. Dette må også ses i lys av at forbudsregelen i art. 9 nr. 1, som er ment å verne om særlig sensitive personopplysninger.[64] Da bør vernet i så fall verne om all behandling av slike sensitive opplysninger.

På bakgrunn av dette mener jeg man må kunne tolke ordlyden utvidende, slik at autentisering også faller innenfor.

3.1.4 Eksempler på hva som er å anse som biometriske personopplysninger

Vi har nå sett på definisjonen for biometriske personopplysninger, og her følger noen eksempler på opplysninger som kan være biometriske personopplysninger. Fingeravtrykk, ansiktsgjenkjenning, håndavtrykk og irisavlesning er eksempler på biometri som *kan* være biometriske personopplysninger.[65]

Dette er bare noen eksempler på hva som er og kan være biometriske personopplysninger. Et viktig poeng å bite seg merke i er at innhenting og anvendelse, og da også behandling, av biometriske personopplysninger i vil være avhengig av teknologi. Man bruker teknologi til å sammenligne fingeravtrykk, og lese av iris. Dette vil dermed også si at ved utvikling og oppfinnelsen av ny teknologi, kan man også finne nye metoder å anvende biometri på, som kan føre til nye biometriske personopplysninger. For eksempel kan man, ved bruk av en teknologisk enhet, gjenkjenne mennesker gjennom hastigheten de skriver på et tastatur.[66] Definisjonen biometriske personopplysninger er med andre ord ikke et begrep som har et fast

---

[62] Schartum (2020) s. 152.
[63] Se pkt. 3.3 i avhandlingen for nærmere redegjørelse for utfordringene ved anvendelse av biometriske personopplysninger.
[64] Se fortalen til personvernforordningen avsnitt 51 første punktum.
[65] Datatilsynet, *Biometri,* datatilsynet.no.
[66] Tom Heine Nätt, *Biometrisk autentisering,* snl.no, punktet «andre metoder».

innhold, men kan endre seg over tid. Dette er viktig å være klar over dette fordi det medfører potensielt at art. 4 nr. 14 i personvernforordningen kvalitativt kan endre seg over tid.

3.2 Den rettslige reguleringen av biometriske personopplysninger

Biometriske personopplysninger er å anse som en særlig kategori av personopplysninger etter personvernsforordningen. I art. 9 i personvernforordningen ramses det opp en rekke typer personopplysninger, blant annet «biometriske personopplysninger med det formål å entydig identifisere en fysisk person», som det som utgangspunkt er forbudt å behandle. Andre ledd av bestemmelsen åpner likevel for i tilfeller der behandling ikke er forbudt.[67]

Alle personopplysninger som skal behandles, må ha et lovlig grunnlag etter personvernforordningen art. 6. Dette gjelder også for de personopplysninger som er av en særlig kategori av personopplysninger etter art. 9. Det vil dermed si at selv om man har funnet et unntak i art. 9 nr. 2 som passer, vil ikke behandlingen i seg selv være lovlig dersom man ikke i tillegg har et behandlingsgrunnlag etter art. 6.

Det fremkommer av art. 9 nr. 4 at medlemsstatene «kan opprettholde eller innføre ytterligere tiltak, herunder begrensninger» for anvendelsen av blant annet biometriske personopplysninger. Det gis altså til medlemsstatene og selv vurdere om de ønsker å gjennomføre noen ytterligere regulering innad i landet. Dette er kun gjort for et fåtall av personopplysningene i personvernforordningen.[68] For biometriske personopplysninger er dette gjort i pol. § 12, som vi skal se nærmere på i kapittel 5.

3.3 Utfordringer ved behandling av biometriske personopplysninger

At biometriske personopplysninger er å anse som en særlig kategori av personopplysninger som i utgangspunktet er forbudt, må ses i sammenheng med hvor inngripende det er overfor enkeltpersonen som det blir behandlet biometriske personopplysninger om.[69] Biometriske personopplysninger er konstante. Det vil si at det i utgangspunktet ikke er mulighet å endre

[67] De øvrige kategoriene av personopplysninger som faller innenfor særlig kategori av personopplysninger etter art. 9 nr.1 er personopplysninger om etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger.
[68] Etter art. 9 nr. 4 er det kun mulig for behandling av genetiske personopplysninger, biometriske personopplysning og helseopplysninger.
[69] Jfr. personvernforordningen art. 9 nr. 1.

sin biometriske kode. Dette medfører at dersom biometriske personopplysninger er behandlet og registrert om en person, vil enhver som har tilgang til personopplysningene kunne identifisere vedkommende for så lenge de har tilgang til personopplysningene.[70] Dette medfører risiko for å bli overvåket, og i den anledning risiko for betydelige inngrep i vern av privatlivet.

Biometri er å måle biologiske, altså fysiske, ting ved individet. Ved behandling av biometriske personopplysninger gjennom en særskilt teknisk behandling, overfører man unike, fysiske kjennetegn ved en person over til data.[71] Fysiske ting ved et individ, fingeravtrykk, irisgjenkjenning o.l., blir tatt vekk fra vedkommende, på en måte som gjør det vanskelig for individet å vite når disse kjennetegnene senere blir brukt – man mister oversikten over bruken av disse sensitive personopplysninger.[72]

Til dette kan det også trekkes frem at dersom de biometriske personopplysningene som er hentet inn blir misbrukt, blant annet som en del av identitetstyveri, kan dette være vanskelig å oppdage. Her gjør risikoen seg også særdeles mer omfattende enn for øvrige personopplysninger nettopp fordi man ikke kan endre de biologiske kjennetegnene som er bakgrunnen for de biometriske personopplysningene som blir hentet inn.

Det foreligger en økende trend med å bruke biometriske personopplysninger for identifisering og autentisering.[73] Ved en økende trend av bruk vil det også forekomme en økende risiko for cyberangrep med det formål å innhente biometriske personopplysninger, for å «låse» opp den informasjon de skal beskytte. Denne risikoen gjør seg særlig gjeldende ved bruk av biometriske personopplysninger, da det ikke er mulig å endre dem, i motsetning til et passord som kan endres og byttes ut dersom det blir utlevert.[74]

---

[70] Christiane Wenderhorst og Yannic Duller, *Biometric recognition and behavioural detection: assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces,* europarl.europa.eu, (2021) s. 44 (heretter Wenderhorst og Duller (2021)).
[71] Wenderhorst og Duller (2021) s. 44.
[72] Wenderhorst og Duller (2021) s. 44.
[73] Wenderhorst og Duller (2021) s. 46
[74] Wenderhorst og Duller (2021) s. 46.

4 Behandling av biometriske personopplysninger

4.1 Hva er å anse som en behandling av personopplysninger

Personvernregelverket trer kun i kraft ved behandling av personopplysninger. Hva som er å anse som behandling av personopplysningene fremkommer av personvernforordningen art. 4 nr. 2. Det kan være naturlig å tenke at personvernregelverket først trer i kraft når det innhentes personopplysninger om et enkeltindivid, men i art. 4 nr. 2 defineres behandling som: «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger». Ordlyden «enhver operasjon» tilsier at all form for interaksjon med det som er å anse som personopplysninger vil falle innenfor ordlyden. Av ordlyden kan man altså forstå at det foreligger en lav terskel for at det foreligger behandling av personopplysninger. En slik forståelse har blitt bekreftet i Høyesterett. I HR-2021-966-A måtte Høyesterett, i en straffeprosessuell tvist, ta stilling til om et videopptak var en lovlig behandling av personopplysning etter personvernforordningen. Ved tolkning av ordlyden i personvernforordningen art. 2 nr. 1 uttaler førstvoterende at «definisjonen omfatter nærmest enhver befatning med personopplysninger».[75]

Personvernforordningen art. 2 nr. 1 regulerer det saklige virkeområdet for forordningen, og det følger av artikkelen at forordningen gjelder for «helt eller delvis automatisert behandling», i tillegg til ikke-automatiserte behandling av personopplysning der dette «inngår i eller skal inngå i et register».

Hva som ligger i ordlyden «automatisert» er ikke nærmere definert i forordningen. En naturlig språklig forståelse av «automatisert» sikter man til behandling som ikke er manuell, altså at det foregår uten medvirkning av mennesker. Hva som ligger i «delvis automatisert» fremkommer ikke av ordlyden. Ovenfor så vi at behandling var «enhver operasjon» med personopplysninger. En behandling kan også være satt sammen av flere operasjoner. For at behandlingen skal være «delvis automatisert» må det være tilstrekkelig at en av operasjonen er automatisert, for at hele behandlingen skal falle innenfor ordlyden. Slik er også ordlyden forstått i juridisk litteratur. Schartum mener at dersom blir utført en type automatisert operasjon «vil hele behandlingen være undergitt bestemmelsen …».[76]

[75] Se HR-2021-966-A avsnitt 28.
[76] Jfr. Schartum (2020) s. 50.

Bakgrunnen for at det skal så lite til for at en delvis automatisert behandling faller innenfor ordlyden må ses i sammenheng med bestemmelsen skal favne om personopplysninger som blir digitalisert, fordi det er dette som medfører risiko overfor enkeltindividet.[77] Dermed er det gjerne tilstrekkelig at en ganske liten del av behandlingen er automatisert, for at selve behandlingen er å anse som «delvis automatisert». Dette er også bakgrunnen for at ikke-automatisert behandling faller innenfor ordlyden dersom det er eller skal registreres i et register; ved å registrere opplysninger i et register gjør man personopplysningene søkbare, som medfører at de kan anvendes og behandles igjen senere.

Ser man på vilkårene samlet sett bærer de preg av å ha en vid ordlyd, der mye kan falle innenfor. Dette har mange likheter med definisjonen på personopplysninger, som jeg har redegjort for tidligere, noe som neppe er en tilfeldighet.[78] I personvernforordningen art. 4 nr. 1 brukes ordlyden «enhver» om hva slags personopplysninger som faller innenfor definisjonen. Dette kan mulig ha sammenheng med formålet er å beskytte enkeltindividet, den registrerte. Da bør ordlyden være vid, slik at man ikke risikerer at noe som bør reguleres av ordlyden ikke faller innenfor.

4.2 Et krav om særskilt teknisk behandling

Fra personvernforordningen art. 4 nr. 14 følger det at det kun foreligger biometriske personopplysninger dersom personopplysningene «stammer fra en *særskilt teknisk behandling*». Rent lovteknisk er dette ikke en innsnevring av den generelle definisjonen av behandling av personopplysninger, da kravet til en «særskilt teknisk behandling» er et vilkår for hva som er å anse som biometriske personopplysninger. I praksis vil dette skillet skli ut. Dette fordi et krav om «særskilt teknisk behandling» vil medføre at enhver behandling av biometriske personopplysninger også må være en særskilt teknisk behandling. Det vil si at enhver form for manuell behandling av personopplysninger, som for eksempel «ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register» vil medføre at det ikke kan være behandling av biometriske personopplysninger, fordi det ikke foreligger en særskilt teknisk behandling.

[77] Jfr. Schartum (2020) s. 51.
[78] Se pkt. 3.1.1 i avhandlingen.

Spørsmålet blir da videre når man har med en særskilt teknisk behandling å gjøre. Ordlyden «særskilt teknisk behandling» tilsier at ikke enhver behandling av biometriske materiale fra et individ er en biometrisk personopplysning; det må gjennom en viss prosess i forkant. I fortalen til personvernforordningen fremkommer det at for behandling av fotografier vil dette være en behandling av biometriske personopplysninger «bare når de behandles ved hjelp av et særskilt teknisk middel som *gjør det mulig* å entydig identifisere eller autentisere en fysisk person» (mine kursiveringer).[79] Uttalelsen ved at den særskilte tekniske behandlingen skal gjøre det mulig å entydig identifisere en fysisk person tilsier at poenget med vilkåret er selve identifisering skjer gjennom en særskilt teknisk behandling som identifiserer vedkommende. Dersom en teknisk gjenstand blir brukt til innhenting, men selve identifiseringen blir gjennomført av mennesker, foreligger det ikke en «særskilt teknisk behandling».

Skillet mellom behandling av personopplysninger og særskilt teknisk behandling av biometriske personopplysninger kan vises gjennom vedtak fra Datatilsynet angående kameraovervåking. I vedtaket fra mars 2021 besluttet Datatilsynet å utgi en bot for brudd på personvernsreguleringen ved kameraovervåking av offentlig plass.[80] Avgjørelsen gjaldt lovligheten av videoopptak av offentlig området. Videokameraet var festet på bygget til et selskap, og viste en offentlig gate i sentrum av Rognan, og videoopptaket ble sendt direkte på Youtube. I en redegjørelse til Datatilsynet fremgår det at videoopptaket var av en slik kvalitet at det ikke var mulig å gjenkjenne ansikter eller bilnummer som ble fanget opp av kameraet. Datatilsynet vurderte det likevel slik at kvaliteten på videoopptaket var tilstrekkelig til at man kunne gjenkjenne hårfarge, biltype og andre «personlige karakteristikker og kjennetegn», og at mennesker som hadde slike forhåndskunnskaper om de som ble fanget opp av filmen, kunne identifisere vedkommende.

I denne avgjørelsen ble det brukt teknologi for å innhente personopplysningene, men selve identifiseringen måtte skje manuelt ved at mennesker gjenkjente individer, og dermed kunne identifisere dem.[81] Det forelå altså en behandling av personopplysninger etter art. 2 nr. 1, fordi man indirekte kunne identifisere individene. Men ettersom selve identifisering skjedde

[79] Jfr. personvernforordningens fortale avsnitt 51.
[80] Se 20/01627-3 Vedtak om overtredelsesgebyr – Direktesending fra kameraovervåking fra offentlig område, datatilsynet.no pkt. 1.
[81] Se 20/01627-3 Vedtak om overtredelsesgebyr – Direktesending fra kameraovervåking fra offentlig område, datatilsynet.no pkt. 2.

manuelt, forelå det ikke en særskilt teknisk behandling som hadde medført at det ville falt innenfor definisjonen av biometriske personopplysninger etter art. 4 nr. 14.

Saken hadde stilt seg annerledes dersom kameraet hadde en form for innstilling som brukte kunstig intelligens til å gjenkjenne og samle ansikter umiddelbart.[82] Et eksempel som ville medføre at en kameraovervåking ville være å anse som behandling av biometriske personopplysninger er et flyselskap som bruker kameraovervåking med ansiktsgjenkjenning for å bekrefte identiteten til sine passasjerer.[83]

5 Biometriske personopplysninger i personopplysningsloven

5.1 Introduksjon til personopplysningsloven §12

I kapittel 3 og 4 har jeg redegjort for hvordan biometriske personopplysninger er regulert i personvernforordningen. I kapittel 5 skal jeg se nærmere på hvordan biometriske personopplysninger er regulert nasjonalt i personopplysningsloven.

Pol. § 12 regulerer muligheten for behandling av «fødselsnummer og andre entydige identifikasjonsmidler». Fødselsnummer er et identifikasjonsnummer som alle som er folkeregistrert i Norge har.[84] Formålet med fødselsnummer er ene og alene å bruke det for å identifisere den som er tildelt det fødselsnummeret. Når det gjelder ordlyden «andre entydige identifikasjonsmidler» siktes det da til øvrige midler som kan identifisere individet. Fra forarbeidende til den tidligere personopplysningsloven fremkommer det at et eksempel på et entydig identifikasjonsmiddel vil være biometriske personopplysninger, som for eksempel fingeravtrykk.[85] Et eksempel på ett entydig identifikasjonsmiddel som ikke er biometriske personopplysninger er d-nummer.[86]

Vilkåret om «behandling av fødselsnummer og andre entydige identifikasjonsmidler» er et åpningsvilkår for å anvende pol. § 12. Det fremkommer i tillegg to kumulative vilkår som må

---

[82] Les mer om ansiktsgjenkjenningsteknologi her: Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU,* (2021) s. 5.
[83] Personvernrådet, *Guidelines 3/2019 on processing of personal data through video devices,* edpb.europa.eu (2019) avsnitt 77.
[84] Datatilsynet, *Fødselsnummer,* datatilsynet.no.
[85] Ot.prp. nr. 92 (1998-1999) s. 114.
[86] Et identifikasjonsnummer tildelt utenlandske borgere som enten ikke oppfyller kravene for å få fødselsnummer, eller skal oppholde seg i Norge mindre enn seks måneder, se Skatteetaten, *D-nummer,* skatteetaten.no.

være oppfylt, for at behandlingen er lovlig etter pol. § 12. For det første må det foreligge et «saklig behov for sikker identifisering». For det andre må det foreligge et saklig behov, må også metoden være «nødvending for å oppnå slik identifisering». Ordlyden «nødvendig» tilsier at dersom man kan møte det saklige behovet på en tilfredsstillende måte, med andre metoder, er kravet til nødvendighet ikke oppfylt. En slik forståelse bekreftes av forarbeidene til personopplysningsloven av 2000, der det fremkommer at kravet til nødvendighet kun er oppfylt «dersom andre og mindre sikre identifikasjonsmidler, som for eksempel navn, adresse og kundenummer ikke er tilstrekkelig».[87] Pol. § 12 oppstiller således en skjønnsmessig vurdering for hvorvidt man kan behandle fødselsnummer eller andre entydige identifikasjonsmidler.

5.2 Bestemmelsens historiske bakgrunn og utvikling: resultatet av en EØS-rettslig forpliktelse

Paragraf 12 i personopplysningsloven ble vedtatt ved innførelsen av den tidligere personopplysningsloven av 2000, som gjennomførte direktiv 1995/46/EF om personvern internt i norsk rett.[88] Det følger av traktaten om den europeiske unions virkemåte at direktiv i stor grad gir det til medlemsstatene å bestemme innholdet i de konkrete bestemmelsene, så lenge målsettingen for direktivet blir nådd.[89] I noen tilfeller kan likevel et direktiv inneholde mer konkrete retningslinjer for innholdet i bestemmelsen. Det fremkommer av personverndirektivet art. 8 nr. 7 at statene som er bundet av direktivet «skal bestemme hvilke vilkår som må oppfylles for at et nasjonalt identifikasjonsnummer eller andre vanlige midler til identifikasjon kan behandles». Gjennom ordlyden «skal» er det klart at direktivet påla medlemsstatene å sette vilkår for behandling av «nasjonalt identifikasjonsnummer eller andre vanlige midler til identifikasjon». Det fremkommer fra forarbeidene til personopplysningsloven av 2000, at formålet med pol. § 12 er å imøtekomme denne plikten som art. 8 nr. 7 gir.[90] Bakgrunnen for bestemmelsen var således å få inn en regulering av dette.

Personverndirektivet art. 8 nr. 7 ble ikke videreført i personvernforordningen, som erstattet personverndirektivet i 2016. Det ble dog innført en lignende bestemmelse i art. 87 i

---

[87] Ot.prp. nr. 92 (1998-1999) s. 114.
[88] Jfr. Schartum (2020) s. 17
[89] Jfr. TEUV art. 288 nr. 3.
[90] Se Ot.prp. nr. 92 (1998-1999) s. 114.

personvernforordningen, men denne bestemmelsen har en viktig forskjell fra art. 8 nr. 7 i personverndirektivet. Istedenfor at medlemsstatene har en plikt til å innføre en regulering av fødselsnummer, kan de selv velge om de *ønsker* å innføre vilkår for bruk av fødselsnummer og «andre vanlige midler til identifikasjon». Justis- og beredskapsdepartementet valgte likevel å stå ved hvordan den tidligere bestemmelsen var formulert, selv om bakgrunnen og formålet med pol. § 12, som var å imøtekomme plikten etter art. 8 nr. 7, ikke lenger var til stede i personvernsforordningen av 2016. Dette vil dermed si at formålet med pol. § 12 da den ble vedtatt, ikke er det samme som det som muligens er formålet med bestemmelsen i dag.

Ved vedtakelsen av personvernforordningen gikk man fra at personvern ble regulert gjennom direktiv til forordning. Pol. § 12 ble til da det fantes et personverndirektiv. En forordning får direkte virkning, mens et direktiv kun er bindende med hensyn til sin målsetning.[91] At EU gikk fra regulering gjennom direktiv til forordning kan ses på som at man mente at behovet for en entydig og samsvarende regulering på tvers av landegrensene var så påtrengende, at man ikke kunne risikere at et direktiv ble gjennomført forskjellig innad i landene. Dette har nok mulig også sammenheng med at personopplysninger, og teknologi, er grenseoverskridende, det forholder seg ikke til landegrenser, og dermed burde lovgivningen være lik for å gi lik beskyttelse. På en slik måte er endringen fra direktiv til forordning en anerkjennelse av at behovet for personvern har økt, og fortsetter å øke i takt med den teknologiske utviklingen.

En slik forståelse kan bekreftes av fortalen til personvernsforordningen, der det fremkommer at «det bør sikres at reglene for vern av fysiske personers grunnleggende rettigheter og friheter i forbindelse med behandling av personopplysninger anvendes på en ensartet og enhetlig måte i hele Unionen».[92]

Biometriske personopplysninger fikk sin definisjon i personvernforordningen av 2018 art. 4 nr. 14. Som utgangspunkt er det forbudt å behandle biometriske personopplysninger, det fremkommer av personvernforordningen art. 9. Noen unntak følger av art. 9 nr. 2, Blant annet fremkommer det av art. 9 nr. 4 at det tillegges statene selv å komme med øvrige reguleringer av de personopplysningene som følger av art. 9 nr. 1.[93] Pol. § 12 slik den fremstår i dag, har

[91] Jfr. TEUV art. 288 nr. 2 og nr. 3.
[92] Jfr. fortalen til personvernforordningen avsnitt 10.
[93] Se pkt. 3.2 for den rettslige reguleringen av biometriske personopplysninger.

nå bakgrunn i personvernforordningen art. 9 nr. 4 samt art. 87 som delvis viderefører den tidligere art. 8 nr. 7. Dette fremkommer av forarbeidene til den nye personopplysningsloven av 2018.[94] Det er altså, slik loven står i dag, slik at biometriske identifikasjonsmidler skal falle innenfor ordlyden «andre entydige identifikasjonsmidler» i pol. § 12.

Tanken bak å redegjøre for den historiske bakgrunnen til biometriske personopplysninger er for å reflektere rundt forholdet mellom den norske pol. § 12 og personvernforordningen. Som vi kan se ble den pol. § 12 til *før* definisjonen og reguleringen av biometriske personopplysninger ble innført i personvernforordningen, uten at pol. § 12 ble endret tilsvarende. Pol. § 12 er resultatet av en utdatert og opphevet direktiv, men ble likevel stående uten at dette har blitt tatt til vurdering ved den norske bestemmelsen. Spørsmålet en kan stille seg er hvorvidt bestemmelsen fungerer som en tilstrekkelig og god regulering av biometriske personopplysninger.

5.3 Nærmere om ordlyden «entydige identifikasjonsmidler»

Pol. § 12 kommer kun til anvendelse for behandling av fødselsnummer eller «andre entydige identifikasjonsmidler». Det er ikke tvilsomt hva som faller innenfor ordlyden «fødselsnummer».[95] Dette er en klart avgrenset definisjon. Tvilen retter seg mot hva som ligger i ordlyden «entydige identifikasjonsmiddel». En naturlig språklig forståelse taler i den retning at det må forstås slik at man med «entydig» sikter man ut til at identifikasjonsmiddelet må peke ut en person. Men da dukker spørsmålet opp; peke ut en person i forhold til hva?

Én måte å forstå «entydig» på er at identifikasjonsmiddelet må være entydig i den forstand at det kan peke ut en person i flere forskjellige systemer og ikke bare innad et system. Som eksempel vil et KID-nummer, som er et identifiseringsnummer i banker, ikke være entydig fordi nummeret ikke kan identifisere vedkommende utenfor bankes systemer.

En annen måte å se på ordlyden «entydig» er at det handler om hvor presist identifikasjonsmiddelet kan peke ut vedkommende. Dersom et fingeravtrykkstemplat har en presisjon på 1:250, altså at den kan snevre ned antallet til 250 individer, vil dette for eksempel vanskelig kunne være å anse som entydig.

---

[94] Prop. 56 LS (2017-2018) s. 215.
[95] Se pkt. 5.1 i avhandlingen.

Ordlyden «identifikasjonsmiddel» tilsier at det som brukes, må være et middel som kan identifisere vedkommende. En måte å se for seg «identifikasjonsmiddel» på er at man bruker et middel for å gjenkjenne og peke ut ett individ, utfra en større mengde registrerte individer. Utfordringen med denne ordlyden retter seg særlig mot bruk av biometri for autentisering. Hvordan kan for eksempel et fingeravtrykkstemplat, et mønster med noen få punkter fra individets fingeravtrykk, være et identifikasjonsmiddel når det inneholder for få punkter til å identifisere vedkommende.

Ordlyden gir ikke noen videre veiledning på hva som menes med at identifikasjonsmiddelet må være «entydig». Verken forarbeidene fra 2018 eller forarbeidene til personopplysningsloven av 2000 gir noe videre veiledning til hva som faller innenfor ordlyden, annet enn, som vi allerede har vært inne på, at biometriske personopplysninger er et entydig identifikasjonsmiddel.[96] Ut over dette kan det således være usikkert hva som faller innenfor ordlyden.

5.3.1 Formålet og fordelene med en vid ordlyd

Bakgrunnen for at ordlyden er så vid kan være at det foreligger et behov for en dynamisk utvikling av regelverket. Med dynamisk utvikling sikter man til at gjeldende rett skal samsvare med fungerende rett i samfunnet. For at det skal være mulig må man ha en ordlyd som er vid nok til at man kan tolke den forskjellig, og dermed la retten utvikle seg dynamisk i tråd med den samfunnsutvikling som forekommer. Dette gjør seg særlig gjeldende for personvernsreguleringer. Personvernregelverket trer først i kraft ved helt eller delvis automatisert behandling, eller manuell behandling som i senere tid kan bli registrert.[97] Det ligger med dette at det må være en eller annen form for teknologi bak behandling av personopplysninger. Teknologi vil konstant være i utvikling, og det er dermed i utgangspunktet et umulig prosjekt å regulere ethvert tilfelle og alternativ til enhver tid. Som en konsekvens av dette er man avhengig av å ha et regelverk som åpner for rom for en tolkning i samsvar med utviklingen av teknologi.

For personvernforordningen er dette, i tillegg til en vid ordlyd, løst ved å unngå å beskrive de teknologiene som anvendes, men heller beskrive hvilken funksjon disse teknologiene skal ha. Dette fremkommer fra fortalen til personvernforordningen, der det fremkommer at ordlyden

[96] Prop. 56 LS (2017-2018) s. 215.
[97] Jfr. personvernforordningen art. 2 nr. 1.

bør være teknologisk nøytral «for å unngå at det oppstår en alvorlig risiko for at bestemmelsene omgås».[98] Dersom man oppretter for konkrete bestemmelser, så risikerer man at forskjellige situasjoner som burde falle innenfor reguleringene, ikke faller innenfor. En slik forståelse kan man også finne i juridisk teori.[99]

En teknologinøytral løsning kan man også se spor av i ordlyden i pol. § 12. Ordlyden «entydige identifikasjonsmidler» beskriver funksjonen teknologien skal ha, nemlig å entydig identifisere, men gir videre lite beskrivelse av i hvilke former for teknologi som kan brukes til å entydig identifisere.[100] Dette kan også være bakgrunnen for at man i forarbeidene til bestemmelsen har holdt tilbake fra å ramse opp eller på annen måte beskrive teknologiene, eller midlene som kan anvendes.

5.3.2 En rekke avgjørelser fra Personvernnemnda for bruk av fingeravtrykk

For å vise hvordan forståelsen av ordlyden i pol. §12 har endret og utviklet seg over tid skal vi se på en rekke avgjørelser fra Personvernnemnda, som klageinstans for vedtak fra Datatilsynet.[101] Alle avgjørelsene retter seg mot bruk av fingeravtrykk. Problemstillingen var om bruken av fingeravtrykket falt innenfor ordlyden i pol. § 12, og det var i hovedsak to utfordringer ved bruken som nemnda måtte ta stilling til: kan et fingeravtrykkstemplat falle innenfor ordlyden «entydig», og om det foreligger et «identifikasjonsmiddel» når fingeravtrykket brukes til autentisering, og ikke identifisering.[102] For ordens skyld ønsker jeg å bemerke at alle avgjørelsene fra Personvernnemnda er truffet før 2016, så altså før vi fikk definisjonen av biometriske personopplysninger i personvernforordningen, noe avgjørelsene bærer preg av. En annen bemerkning jeg ønsker å komme med innledningsvis er at referansekoden til avgjørelsene kan gi inntrykk av at avgjørelsene er nummerert i kronologisk rekkefølge. Denne nummerering har dog ingen sammenheng med kronologisk rekkefølge. Det fremkommer av datoen på vedtakene, at de er avsagt i en annen rekkefølge, og jeg kommer til å presentere avgjørelsene i etter den rekkefølgen de har blitt avsagt i.

---

[98] Fortalen til personvernforordningen avsnitt 15.
[99] Schartum (2020) s. 29.
[100] Formålet med personopplysningsloven av 2000 var blant annet at den skulle være teknologinøytral, se NOU 2009:1 pkt. 7.1.
[101] Jfr. pol. § 22 andre ledd.
[102] Ordet «templat» er hentet fra avgjørelsene selv. Det er et engelsk ord, som oversatt til norsk betyr «mal». Poenget er at ikke selve fingeravtrykket blir brukt, men en forenklet form for biologisk mønster hentet fra konkrete punkter på fingeravtrykket. Se, blant annet, PVN-2006-8 pkt. 6.2 for nærmere redegjørelse om hvordan teknologien fungerer.

PVN-2006-7 Tysvær kommune – fingeravtrykkspålogging

I PVN-2006-7 måtte Personvernnemnda ta stilling til Datatilsynets avgjørelse om en kommunes bruk av fingeravtrykk ved innlogging på PC. Med fingeravtrykk til de ansatte skulle det lages en template, basert på 75 punkter fra fingeravtrykket til enhver enkelt.[103]

For vurderingen av hvorvidt fingeravtrykkstemplatet faller innenfor ordlyden eller ikke er det særlig to momenter nemnda trekker frem. For det første er at det i forarbeidene til pol. § 12 pekt på at fingeravtrykk som eksempel vil være ett entydig identifikasjonsmiddel.[104] Dette blir det av nemnda lagt avgjørende vekt på. Nemnda tolker således ordlyden lojalt overfor lovgiver. For det andre mener nemnda at «identifikasjonsmiddel» sikter til «hva brukeren presenterer til systemet», og ikke hva som blir igjen etter behandlingen. Det siste argumentet underbygger nemnda med å vise til at fødselsnummer er regulert under pol. § 12, selv om også fødselsnummer kan krypteres slik at det ikke brukes til identifisering.[105] Nemnda konkluderer således med at fingeravtrykkstemplat faller innenfor ordlyden.

Når det gjelder skillet mellom autentisering og identifisering, fremstår det fra nemndas vurderinger som om de kun ser for seg at to tilfeller av identifikasjonsmidler, der begge to i en grad forutsetter en form for identifikasjon. Nemnda presenterer to forskjellige måter å forstå «identifikasjonsmidler» på. For det første må identifikasjonsmidler forstås som et «middel» som brukes som en opplysning for å finne frem til én, allerede registrert, person. Altså en form for identifisering. Den andre måten å bruke identifikasjonsmiddel på er til autentisering «etter at identifisering har funnet sted». Det spørsmålet nemnda må besvare er hvorvidt den sistnevnte faller innenfor ordlyden «identifikasjonsmiddel» i pol. § 12.[106] Den andre måten å bruke et identifikasjonsmiddel på fordrer således at den første metoden allerede er brukt. Utfra disse uttalelsene kan det fremstå som det for nemnda er klart at bruk av et slikt middel kun for å autentisere en bruker, ikke er mulig, og denne forståelsen, får innvirkning på hvordan nemnda videre vurderer bruken som er knyttet til autentisering, ettersom de mener at så lenge en del av behandlingen medfører en identifikasjon, vil behandlingen falle innenfor pol. § 12.

[103] PVN-2006-7 pkt. 3.
[104] Se Ot.prp. nr. 92 (1998-1999) s. 114.
[105] Jfr. PVN-2006-7 pkt. 7.5.1.
[106] PVN-2006-7 pkt. 7.5.1 fjerde avsnitt.

Nemnda kommer også med en klar rettspolitisk uttalelse, som blir vist til også i de senere avgjørelsene.

> Nemnda stiller seg kritisk til hvorvidt det er ønskelig å regulere de to tilfellene [fingeravtrykk og fødselsnummer] på samme måte, særlig når dette bare har grunnlag i en enkelt setning i forarbeidene uten nærmere utredning av konsekvenser. Biometriske metoder til bruk for identifikasjon eller autentisering har vært i sterk utvikling siden loven ble vedtatt. Nemnda har merket seg at Datatilsynet har fremmet forslag om særlig regulering av biometriske metoder, og stiller seg sterkt positiv til at dette blir gjort, og blir gitt prioritet i revisjonsarbeidet.[107]

Det som også er interessant med denne uttalelsen er at nemnda tidlig viser forståelse og stiller spørsmål ved om ordlyden i pol. § 12 bør være som den er. Likevel velger de å holde seg lojalt til lovgivers uttalelse. Det er særlig spesielt å se at nemnda allerede i 2006 etterspør at det utredes nærmere hvordan dette fungerer, når man i 2021 fortsatt ikke har fått en endring i ordlyden.

PVN-2006-10 Esso Norge

Esso Norge ønsket å bruke adgangskontroll gjennom bruk av fingeravtrykk, for å begrense adgangen til fire tankanlegg, slik at kun trent og autorisert personell fikk tilgang. I likhet med de andre tilfellene med bruk av fingeravtrykk ble det også her kun brukt et templat av fingeravtrykket.

Nemnda tar her utgangspunkt i det som allerede har blitt slått fast i PVN-2006-7, nemlig at fingeravtrykk som utgangspunkt faller innenfor ordlyden «entydige identifikasjonsmidler».[108]

Når det gjelder skillet mellom identifisering og autentisering tar nemnda her utgangspunkt i uttalelsen fra PVN-2006-7, nemlig at det foreligger to måter «identifikasjonsmiddel» kan brukes på. Også i denne avgjørelsen er det den sistnevnte bruken som er relevant. Nemnda peker på at selve fingeravtrykket kun blir brukt til autentisering, mens identifiseringen skjer gjennom bruk av et adgangskort. Nemnda viser til at de i den tidligere avgjørelsen under tvil kom til at bruken falt innenfor, men konkluderer med at fingeravtrykk også må falle innenfor

---

[107] Jfr. PVN-2006-7 pkt. 7.5.1 tredje avsnitt fra bunnen.
[108] Se PVN-2006-10 pkt. 6.3.

ordlyden i pol. § 12 også «til autentisering *etter at identifisering* har funnet sted, fordi autentisering er en bruk som omfattes av 'sikker identifisering'» (mine kursiveringer).[109] Selv om fingeravtrykket i seg selv kun brukes til autentisering, mener nemnda at denne autentiseringen er en del under et samlet system, der det også foreligger en identifisering, og at disse to fasene dermed ikke kan ses uavhengig av hverandre.

PVN-2006-11 Rema 1000

I denne avgjørelsen måtte nemnda ta stilling til lovligheten av bruk av fingeravtrykk for timeregistrering hos en matbutikk. Når det gjaldt bruken av fingeravtrykk til autentisering var det klart at også selve fingeravtrykket kun ble brukt til autentisering. Først måtte de ansatte taste inn et ansattnummer, som førte til at de ble identifisert.

For spørsmålet om autentisering faller innenfor, vises det til vurderingene gjort i PVN-2006-7, og videreført i PVN-2006-10. Nemnda viser så til at fingeravtrykket brukes for å lage en template som representerer individet, og at denne representasjonen er den som senere sammenlignes for å finne ut av hvorvidt individet har tilgang eller ikke. Dersom «sammenligningen ligger innenfor den forhåndsdefinerte margin for avvik, vil (1) brukeren være identifisert, og (2) brukeren være autentisert».[110] På denne måten er også autentiseringen her koblet opp mot en identifisering, slik at nemnda kommer til at det faller innenfor pol. § 12.

PVN-2006-8 Oxigeno Fitness og PVN-2006-9 Oslo trimsenter – fingeravtrykk ved adgangskontroll til treningssenter

Avgjørelsene fra PVN-2006-8 og PVN-2006-9 ligner i stor grad på hverandre, og ble avsagt samme dag, der to treningssentre brukte et templat av et fingeravtrykk som adgangskontroll til senteret. Om tolkning av ordlyden «entydige identifikasjonsmiddel» ble det i begge avgjørelsene trukket frem at «identifikasjonsmiddel» må ses i sammenheng med hva «brukeren presenterer til systemet» uavhengig av hvordan systemet så behandler dette. Når det ble presentert et fingeravtrykk i disse sakene, var dette tilstrekkelig for at det for nemnda var klart at det forelå behandling av entydige identifikasjonsmiddel etter pol. § 12.[111] Dette er

[109] Jfr. PVN-2006-10 pkt. 6.3.
[110] Jfr. PVN-2006-10 pkt. 6.3.
[111] Jfr. PVN-2006-8 pkt. 6.3 og PVN-2006-9 pkt. 6.3.

altså i tråd med den linjen Personvernnemnda har lagt seg på i avgjørelsene PVN-2006-7, PVN-2006-10 og PVN-2006-11.

5.3.2.1 En samlet vurdering av avgjørelsene fra 2006

Det man kan se fra disse avgjørelsene er at de ilegger den ene uttalelsen fra forarbeidene mye vekt ved vurderingen av hvorvidt fingeravtrykkstemplatet faller innenfor ordlyden eller ikke. Herunder er det interessant at nemnda innrømmer at et fingeravtrykkstemplat ikke er entydig, ettersom det er på det rene at et mønster trukket ut av et begrenset antall punkter på en finger ikke kan medføre nok informasjon til å identifisere en person.

Når det gjelder hvorvidt identifikasjonsmiddelet faller innenfor ordlyden også når det brukes til autentisering, ser man at nemnda har opprettet en forståelse av hvordan autentisering må brukes, og koblet dette opp mot en form for identifisering. Dette medfører at de risikerer å miste synet på, og vurderingen av, om autentisering kan skje uten noen form for identifisering. Når man heller da ikke vurderer spørsmålet opp mot den konkrete situasjonen i de videre avgjørelsene, men bare viser til hvordan spørsmålet ble vurdert i PVN-2006-7, risikerer man å opprette en praksis som ikke samsvarer med bruken. Det medførte også en endring i hvordan ordlyden blir forstått senere, da problemstillingen ble vurdert på nytt av nemnda i 2011.

Samlet sett viser avgjørelsen fra 2006 at Personvernnemnda har fulgt en lik linje hele veien. Selv om avgjørelsene til tider bærer preg av litt forskjellige vurdering, og trekker frem forskjellige momenter som ilegges vekt, er det gjennomgående de to samme spørsmålene som tas opp, som blir vurdert likt og der nemnda ender på samme resultat i alle sakene; hva faller innenfor identifikasjonsmiddel og hva har det å si at et identifikasjonsmiddel brukes til autentisering.

Tidligere har vi sett at det er et formål at ordlyden i personvernforordningen skal være teknologinøytral.[112] Nemnda legger i disse avgjørelsene avgjørende vekt på en uttalelse fra forarbeidet om hva som er å anse som «entydig identifikasjonsmiddel». Dette istedenfor å fokusere på *hva* teknologien må gjøre for å falle innenfor ordlyden, slik som en teknologinøytral tolkning skulle tilsi. Ettersom avgjørelsene ble vedtatt lenge før personvernforordningen ble vedtatt, der den teknologinøytrale tolkningen ble presentert, er

[112] Se pkt. 5.3 i avhandlingen.

det sånn sett ikke å forvente at nemnda opprettholder en slik tilnærming til ordlyden. Det er likevel interessant, særlig når man sammenligner med mindretallets vurdering.

To av personvernnemndas medlemmer var uenig i hvilken vekt som kan tillegges forarbeidene ved tolkning av pol. § 12.[113] Denne særmerknaden blir opprettholdt i samtlige av avgjørelsene. For dem fremstår det som uheldig å låse ordlyden til en enkel uttalelse i forarbeidene som ikke er begrunnet noe ytterligere i forarbeidet. Etter deres mening må det når forarbeidene gir uttrykk for at «andre entydige identifikasjonsmidler» kan være fingeravtrykk, må dette ses i sammenheng med nettopp hvordan fingeravtrykket blir brukt. Ettersom ordlyden i pol. § 12 trekker andre entydige identifikasjonsmidler sammen med fødselsnummer, må dette, ifølge mindretallet, tilsi at dette vil gjelde for der fingeravtrykk blir brukt på lik måte som fødselsnummer, altså for å identifisere vedkommende. Altså blir det feil å legge til grunn at også fingeravtrykk til bruk som autentisering, vil falle innenfor ordlyden. I tillegg peker mindretallet på at selv om man prinsipielt sier at fingeravtrykk faller innenfor ordlyden, vil ikke dette nødvendigvis også gjelde for et fingeravtrykkstemplat, som da kun er en begrenset del av fingeravtrykket. Dette har igjen sammenheng med at ordlyden knytter fødselsnummer sammen med det øvrige, og at et fingeravtrykkstemplat ikke kan brukes for å identifisere noen, til det finnes det for få punkter. Dermed vil ikke templatet medføre et «entydig» identifikasjonsmiddel.

Det ligger flere gode poenger i mindretallets vurdering. Særlig kan det fremstå som merkverdig å tillegge en uttalelse fra forarbeidene så mye vekt som det gjøres i nemndas avgjørelser. For det første er ikke denne uttalelsen begrunnet på noen måte, slik at man aldri helt sikkert kan knytte uttalelsen opp mot hva lovgiver mente med det. For det andre er nemndas avgjørelser på et rettsområde der det er særlig viktig å tolke lovene dynamisk, i takt med samfunnsutviklingen. I lys av denne samfunnsutviklingen er det noe merkelig å legge så mye vekt på en uttalelse fra forarbeidet som ble skrevet for fem/seks år tilbake i tid. Allikevel skal man være forsiktig med å gå imot en så klar uttalelse i forarbeidene, uten å ha gode grunner til det. Dette kan trolig være bakgrunnen for at nemnda tolket ordlyden i samsvar med forarbeidene.

[113] Se PVN-2006-7 pkt. 7.5.1.

I mindretallets vurdering kan man kjenne igjen en mer teknologinøytral tolkning, som jeg har trukket frem tidligere. Mindretallet setter søkelys på hva fingeravtrykket skal brukes til, opp mot ordlyden i bestemmelsen, istedenfor å legge for mye vekt hva det er. I tillegg har mindretallets vurdering av betydningen av forarbeidende og skillet mellom identifisering og autentisering flere likheter med de to neste avgjørelse som ble avsagt om fingeravtrykk, PVN-2011-11 og PVN-2011-12.

5.3.2.2 Avgjørelsene fra 2011

PVN-2011-11 Visma Retail

Bakgrunnen for avgjørelsen var lanseringen av en selvbetjent butikk i Oslo, der eierne ønsket at Datatilsynet skulle vurdere deres løsning for alderskontroll. Ordningen hadde mange likhetstrekk med fingeravtrykksautentisering i avgjørelsene fra 2006, med en viktig forskjell. I avgjørelsene fra 2006 forelå det en todelt operasjon, der man for å autentisere først måtte identifisere vedkommende. I denne avgjørelsen forelå det en ren autentiseringsprosess, *uten* at individet først ble identifisert. Det er vanskelig å si nøyaktig hva som medfører dette skillet i avgjørelsen. Men uansett ser man i denne avgjørelsen at det har skjedd en utvikling i forståelsen og bruken av fingeravtrykk til autentisering, på en slik måte at det ikke trenger å ha en sammenheng med identifisering.

For vurderingen av pol. § 12 ser Personvernnemnda på de samme spørsmålene som avgjørelsene i 2006; om fingeravtrykkstemplatet er ett entydig identifikasjonsmiddel og skillet mellom identifisering og autentisering. Nemnda pekte på at et fingeravtrykkstemplat ikke i seg selv er ett entydig identifikasjonsmiddel, fordi templatet inneholder for få punkter til å kunne identifisere en person. Dette poenget var, som nemnda også viser til, oppe i de tidligere avgjørelsene, men der fikk uttalelsen i forarbeidene mer vekt.

Når det kommer til identifisering og autentisering, bruker nemnda god tid på å se på skillet mellom de to. Nemnda peker på at dette i praksis ofte er knyttet sammen, men mener at man på denne bakgrunn ikke er tydelig nok på at det er tale om to adskilte fenomen. Etter deres mening må de betraktes adskilt. De konkluderer dermed med at et fingeravtrykk ikke brukes

som et «entydig identifikasjonsmiddel» dersom bruken begrenser seg til autentisering, altså å bekrefte eller avkrefte en påstand.[114]

PVN-2011-12 Adgangskontroll ubetjent treningssenter

Nemnda måtte ta stilling til klage på Datatilsynets vedtak om pålegg for at et treningssenter måtte avslutte bruk av fingeravtrykk i forbindelse med adgangskontroll. Avgjørelsen viderefører vurderingene som fremkommer i PVN-2011-12.[115]

5.3.2.3 Forståelsen av ordlyden og bruken har utviklet seg over tid

Det denne redegjørelsen viser er at det, over en relativt kort tidsperiode, har foregått en endring i hvordan man forstår ordlyden «entydig identifikasjonsmiddel». Fingeravtrykkstemplat kan ikke anses å være «entydig», og at «identifikasjonsmiddel» ikke foreligger der det har vært en ren autentisering, uten noen form for identifisering.

Det er usikkert om muligheten til å autentisere uten å koble det opp mot identifisering er noe som har kommet etter at avgjørelsene i 2006 ble avsagt, eller ikke. Men det som er klart etter avgjørelsen i 2011 er at Personvernnemnda her tar klar avstand fra nemndas egen praksis med å koble autentisering opp mot identifisering på en slik måte at autentisering kan betraktes som et eget system som faller utenfor ordlyden til pol. § 12.

En annen ting som er viktig å merke seg ved disse avgjørelsene, er at det er de samme problemstillingene som dukker opp, på faktum som er mer eller mindre helt like. Og selv om nemnda allerede i 2006 er inne på de samme punktene som blir avgjørende i avgjørelsene fra 2011, så ender de altså opp med helt forskjellig resultat når det gjelder tolkning av «entydige identifikasjonsmidler». På denne måten får ordlyden et helt annet omfang, og ordlyden har også endret seg betraktelig over en veldig kort tidsperiode, og dette har da også åpenbart stor konsekvens for anvendelsen av bestemmelsen. Dette mener jeg er et argument som taler for at bestemmelsen ikke fungerer godt nok, og at den må endres.

---

[114] Jfr. PVN-2011-11 pkt. 6 fjerde avsnitt fra bunnen av underkapittelet.

[115] Dette er den siste avgjørelsen fra Personvernnemnda som vurderer bruk av fingeravtrykk.

5.3.3 Hensynet til en dynamisk utvikling sett opp mot behovet for forutberegnelighet

Det løper flere risikoer ved en vid ordlyd, og disse må også tas i betraktning ved vurderingen av hvordan ordlyden fungerer.

Her kan man blant annet trekke frem at en for vid ordlyd igjen kan skape usikkerhet rundt hva som faller innenfor. Dette fordi en vid ordlyd kan medføre at man ikke klarer å feste konkrete tilfeller til den. Datatilsynet har myndighet til å treffe vedtak om sanksjoner ved lovbrudd.[116] Dersom det er for usikkert hva som faller innenfor ordlyden, kan det potensielt medføre at behandlingsansvarlig og/eller databehandlere unngår å anvende teknologi, i frykt for at dette ikke er i samsvar med loven.[117] Er det tilfellet, vil en vid ordlyd fungere imot sin hensikt, og det er man heller ikke tjent med. Herunder er det viktig å huske på at samfunnet i stor grad er tjent med anvendelse og utvikling av teknologi. Lovverket bør således ikke være bygget opp på en slik at det potensielt kan forhindre videre utvikling og bruk av teknologi.

Behovet for en dynamisk utvikling må veies og vurderes opp mot behovet for et forutsigbart lovverk. For personvernlovgivningen er behovet for en forutsigbar lov særlig viktig fordi inngrepene retter seg mot enkeltpersoner. Når det samtykke fra den registrerte er et av de viktigste behandlingsgrunnlagene i personvernforordningen er det helt grunnleggende at den registrerte forstår regelverket som anvendes.[118] Til dette punktet kan det også trekkes frem at de som er forpliktet etter lovverket, behandlingsansvarlig og databehandlere, i stor grad vil være bedrifter som ikke har tid eller kompetanse til omfattende tolkning av loven.[119] Da er det en forutsetning at lovverket er enkelt å forstå, slik at de vet hva de er forpliktet til. Det er, blant annet, på bakgrunn av dette at det er knesatt et prinsipp om åpenhet i personvernforordningen.[120] I juridisk teori er prinsippet om åpenhet beskrevet som at det gjelder all informasjon som er relevant for å forstå hva som innebærer en behandling av personopplysninger, hvilke regler som gjelder, og hvordan praksis rundt behandlingen er.[121]

---

[116] Jfr. pol. § 26 andre ledd.
[117] Bergen kommune mottok en bot på svimlende 3 millioner kroner i mars 2020, se 20/02181-3 vedtak om overtredelsesgebyr – Direktesending fra kameraovervåking fra offentlig område, datatilsynet.no pkt. 2. Og Trumf fikk, i desember 2021, varsel om bot på 5 millioner kr, se 20/03046-11 varsel om vedtak om overtredelsesgebyr – TRUMF AS, datatilsynet.no pkt. 2.
[118] Jfr. personvernforordningen art. 6 nr. bokstav a og personvernforordningen art. 9 nr. 2 bokstav a.
[119] Se definisjon av behandlingsansvarlig og databehandler i pkt. 3.1.
[120] Jfr. personvernforordningen art. 5 nr. 1 bokstav a.
[121] Jfr. Schartum (2020) s. 90.

For biometriske personopplysninger må dette ses i sammenheng med den store risikoen som foreligger ved behandling, og at samtykke er et rettsgrunnlag for behandling av særlige kategori av personopplysninger etter art. 9.[122]

For tilfellet «entydige identifikasjonsmidler» og behovet for en dynamisk utvikling er det også et poeng å trekke frem at det per dags dato ikke finnes noen øvrige identifikasjonsmidler som faller innenfor ordlyden enn biometriske personopplysninger og d-nummer. På den måten kan man argumentere for at behovet for en vid ordlyd ikke er så påtrengende. Da er det mulig at behovet for en klar og konsis ordlyd bør stå sterkere, og bli avgjørende for hvordan pol. § 12 bør lyde.

I den nasjonale tilleggsreguleringen av biometriske personopplysninger, pol. § 12, blir ordlyden «identifisering» brukt. I praksis fra Personvernnemnda kan man se at det har skjedd en økende bevisstgjøring rundt skillet mellom identifisering og autentisering.[123] Det ble sist i 2011 avgjort at autentisering må falle utenfor ordlyden «identifisering».[124] Det har i etterkant av denne avgjørelsen ikke blitt avsagt noen avgjørelser som gir noen avklaring av hva som ligger i ordlyden, selv ikke etter personvernforordningen kom i 2016. Det kan dermed være usikkert hva som er rettstilstanden i dag.

Den usikre rettstilstanden underbygges av at det er klart at ordlyden innholdsmessig har endret seg siden vedtakelsen av personvernforordningen. Etter definisjonen av biometriske personopplysninger ble innført i personvernforordningen art. 4 nr. 14 er det nå klart at også autentisering ved bruk av biometriske personopplysninger vil falle innenfor.[125] Det vil dermed si at innholdet i det som nå er pol. § 12 har endret seg siden innføringen av personvernforordningen. En slik endring bør tydeliggjøres, for å skape et forutsigbart og lett anvendelig regelverk. Endringen kan for eksempel da være å skille ut reguleringen av biometriske personopplysninger i en egen bestemmelse, eller innføre en forskrift som presiserer at autentisering faller innenfor.

---

[122] Jfr. personvernforordningen art. 9 nr. 2 bokstav a.
[123] Se gjennomgang av praksisen i pkt. 5.3.2.
[124] Jfr. PVN-2011-11 og PVN-2011-12.
[125] Se nærmere om dette under pkt. 3.1.3.

5.4 Koblingen mellom identifikasjonsnummer og biometriske personopplysninger som et «entydig identifikasjonsmiddel»

Det må være en behandling av «fødselsnummer eller andre entydige identifikasjonsmiddel» for at pol. § 12 kommer til anvendelse. Dette er alternative vilkår, det vil si at det ikke stilles krav til at en personopplysning ikke trenger å være både et fødselsnummer *og* ett entydig identifikasjonsmiddel, jfr. ordlyden «eller». På bakgrunn av at vilkårene er alternative og således ikke henger sammen, er det naturlig å tenke at pol. § 12 oppstiller to forskjellige midler som ikke henger sammen med hverandre. Ser man nærmere på ordlyden, kan det dog argumenteres for at det foreligger en kobling mellom fødselsnummer og de entydige identifikasjonsmidlene. Dette kom blant annet til uttrykk i mindretallet fra Personvernnemndas avgjørelser. Mindretallet ga uttrykk for at ordlyden forutsatte at biometriske personopplysninger «… benyttes på en måte som har likhetstrekk med den måte fødselsnummer benyttes på …».[126] For d-nummer er dette trolig ikke problematisk, da det i praksis er det samme som et fødselsnummer, altså et identifikasjonsnummer som er tildelt individet for å identifisere vedkommende. Biometriske personopplysninger skiller seg dog ut fra fødselsnummer på flere måter, noe som kan medføre at koblingen mellom de to, og da ordlyden i pol. § 12, er uheldig. At det foreligger en kobling mellom identifikasjonsnummer og biometriske personopplysninger ble også fremmet av Datatilsynet, som høringsinstans ved forarbeidene til ny personopplysningslov i 2018.[127]

Biometriske personopplysninger skiller seg, rent fysisk, veldig fra identifikasjonsnummer. Som nevnt, er et fødselsnummer et identifikasjonsnummer med det formål at det skal identifisere vedkommende. Biometriske personopplysninger har sitt grunnlag i biometri, som er målinger av som er «automatiserte systemer for gjenkjenning ved å ta i bruk unike målbare biologiske kjennetegn».[128] Identifikasjonsnummer er noe konstruert som man er tildelt. Biometri er noe man er. Det er en rent fysisk ting ved menneske, som man har skapt en mulighet til å bruke til identifisering. Som utgangspunkt er det altså en personopplysning som er veldig forskjellig fra fødselsnummer, og d-nummer. Ettersom et identifikasjonsnummer er konstruert for å identifisere, har man i mye større grad kontroll over hva det brukes og kan brukes til. Man har ikke samme kontroll over bruken av biometriske personopplysninger. I

[126] Jfr. PVN-2006-11 REMA 1000 – fingeravtrykk ved registrering av timer pkt. 6.3.1.
[127] Jfr. Prop. 56 LS (2017-2018) s. 54–55.
[128] Se pkt. 3.1 i avhandlingen.

tillegg, som nevnt tidligere i avhandlingen, er biometriske personopplysninger trolig et begrep som kvalitativ kommer til å endre seg over tid.[129] Det samme kan ikke sies om identifikasjonsnummer, da dette er et fast avsatt begrep.

I tillegg vil behandlingen av identifikasjonsnummer skille seg fra biometriske personopplysninger, der det foreligger kravet til en «særskilt teknisk behandling».[130] Risikoene og konsekvensene ved behandling vil også stille seg annerledes for biometriske personopplysninger. For eksempel vil man i liten grad kunne endre sin biometri, noe som tilsier at dersom biometriske personopplysninger blir misbrukt, er dette særlig vanskelig å gjøre noe med.[131]

Som man kan se er altså fødselsnummer og biometriske personopplysninger veldig forskjellig. Dette er i seg selv et argument som taler i den retning at de ikke burde kobles sammen på en slik måte. Det kan muligens medføre at ordlyden kvalitativt har et forskjellig innhold utfra hvilken av de to kategoriene personopplysninger man vurderer. Det er for eksempel ikke nødvendigvis slik at man kan vurdere om det foreligger et saklig behov likt for fødselsnummer eller andre entydige identifikasjonsmidler. Det kan trolig være vanskeligere å argumentere for at behandling av biometriske personopplysninger har et «saklig behov» og er «nødvendig» når det som utgangspunkt er forbudt å behandle personopplysningen.[132]

Det kan fremstå som om man etter norsk rett ilegger disse to typene personopplysninger en lik verdi, når det i forordning er gjort et poeng i å skille ut biometriske personopplysninger. Dette kan fremstå som kontraproduktivt, fordi en type personopplysninger som er løftet frem i forordning «forsvinner» i det norske lovverket. Man kan således risikere å miste fokus på det vernet biometriske personopplysninger er gitt gjennom forordningen, når de sammenkobles med identifikasjonsnummer gjennom pol. § 12. Det er også vanskeligere å skille mellom hvilke forskjellige hensyn som gjør seg gjeldende, når det ikke finnes et skille mellom de to typene personopplysninger.

Til dette punktet må det også trekkes frem at formålet med en forordning er å få gjennomført et konsistent og ensartet regelverk på tvers av landegrensene. For at det skal være tilfelle, kan

---

[129] Se pkt. 3.1.4 i avhandlingen.
[130] Se pkt 4.2 i avhandlingen.
[131] Se pkt. 3.3 i avhandlingen.
[132] Jfr. personvernforordningen art. 9 nr. 1.

det fremstå som åpenbart at personopplysninger som det er gjort et skille mellom i forordningen, bør ha et tilsvarende og samsvarende skille i den nasjonale bestemmelsen.

Koblingen har dog en naturlig forklaring. Som nevnt tidligere kom bestemmelsen til som en del av reguleringen av fødselsnummer, som Norge var pålagt å innføre etter personverndirektivet. Ettersom det fremkommer av forarbeidene til den tidligere personopplysningsloven at fingeravtrykk vil falle innenfor ordlyden «entydige identifikasjonsmidler», er det klart at hvert fall dette hele tiden skulle reguleres av ordlyden. Når innføringen av konseptet biometriske personopplysninger, som da blant annet vil være fingeravtrykk, kan det fremstå som helt naturlig at ordlyden ble stående, fordi det allerede til en viss grad var gitt uttrykk for at biometriske personopplysninger skulle falle innenfor. Men når man nå vet at ordlyden innholdsmessig har endret seg, er det klart at skillet bør fremmes klarere.

Personvernnemda kom i PVN-2006-7 med en klar rettspolitisk uttalelse. Der ga nemnda klart uttrykk for at de var skeptiske til koblingen mellom fødselsnummer og fingeravtrykk, uten at det ble utredet mer rundt konsekvensene av dette. I 2008 foretok Dag Wiese Schartum en utredning om bruk av biometriske personopplysninger i pol. § 12, etter en oppfordring fra Justis- og beredskapsdepartementet.[133] Schartum konkluderer i utredningen at det er å foretrekke at man skiller fødselsnummer fra biometriske personopplysninger, og at de blir regulert i hver sin bestemmelse.[134] Han peker på at fødselsnummer og biometriske personopplysning er to forskjellige midler, som reiser forskjellige spørsmål.[135] Det er i etterkant ikke foretatt noen ytterligere vurdering av bestemmelsen, eller konsekvensen av å behandle fødselsnummer og biometriske personopplysninger under samme bestemmelse. Selv ikke etter at biometriske personopplysninger ble innført i personvernforordningen i 2016.

Identifikasjonsnummer og biometriske personopplysninger er to vidt forskjellige personopplysninger, som både skiller seg fra hverandre i utvikling. Når det i tillegg ikke foreligger noen rettsavklaring som klart kan gi uttrykk for at personopplysningene skal behandles som to helt individuelle vilkår uten sammenheng, kan det fremstå som mest

[133] Daværende Justis- og politidepartementet.
[134] Jfr. Schartum og Bygrave (2008) s. 60.
[135] Jfr. Schartum og Bygrave (2008) s. 60.

hensiktsmessig å fjerne koblingen mellom de to, gjennom å løse biometriske personopplysninger ut til en egen bestemmelse.

Departementet valgte å stå ved ordlyden slik den var i pol. § 12. Det ble begrunnet med at biometriske personopplysninger nyter et særlig vern, som de delvis får gjennom personvernforordningen art. 9, men at det likevel trengtes noe ytterligere regulering. Således trengtes det en særnorsk regulering, som finnes i pol. § 12. Dette ble begrunnet i at selv om det var en snever unntaksregel i personvernforordningen art. 9 nr. 2 at den registrerte kan samtykke til behandling.[136] Det skal med andre ord ikke så mye til for at forbudsregelen i første ledd ikke kommer til anvendelse. Dette ble tillagt vekt ved da departementet kom til at bestemmelsen skulle bli stående. Til dette argumentet må det dog også pekes på at kravet til samtykke skal tolkes strengt, slik at det likevel til en viss grad vil medføre en videreføring av beskyttelsene etter første ledd. Dette fremkommer av ordlyden i art. 9 nr. 2. bokstav a om at det må være et «uttrykkelig samtykke», i tillegg uttales det i fortalen til personvernforordningen at «samtykke bør gis i form av en tydelig bekreftelse der den registrerte på en frivillig, spesifikk, informert og utvetydig måte gir sitt samtykke til behandling av vedkommende sine personopplysninger».[137]

Det kan stilles spørsmål ved hvorfor ordlyden likevel ble stående, når departementet begrunner å beholde pol. § 12 med at biometriske personopplysninger skal få et særlig vern gjennom bestemmelsen, uten at dette nevnes i ordlyden. I tillegg må det stilles spørsmål ved hvilket særlig vern biometriske personopplysninger egentlig har etter pol. § 12.

6 Avsluttende bemerkninger

6.1 Oppsummering av de trendene vi har sett på

Nasjonalt reguleres biometriske personopplysninger i pol. § 12. Bestemmelsen er ikke oppdatert siden den ble vedtatt gjennom personopplysningsloven i 2000. Ordlyden er vid, og det kan være vanskelig å vite hva som faller innenfor ordlyden. Trolig har også innholdet i bestemmelsen endret seg, etter at personvernforordningen kom, slik at autentisering nå faller innenfor.[138] Når da i tillegg bestemmelsen ikke har fått noen form for rettsavklaring, fremstår

[136] Prop.56 LS (2017-2018) s. 56.
[137] Jfr. personvernforordningens fortale avsnitt 32.
[138] Se om dette i pkt. 3.1.3 i avhandlingen.

det som meget usikkert hva bestemmelsen favner om. I tillegg medfører ordlyden i pol. § 12 en kobling mellom identifikasjonsnummer, fødselsnummer og d-nummer, og biometriske personopplysninger. Dette kan være problematisk på bakgrunn av at dette er veldig forskjellige midler. Således vil vurderingene og vilkårene for behandling biometriske personopplysninger skiller seg fra behandling av identifikasjonsnummer.

Innledningsvis stilte jeg spørsmålet om hvorvidt den nasjonale lovreguleringen av biometriske personopplysninger fungerer godt nok. Etter det jeg har gjort rede for i avhandlingen mener jeg at svaret på dette spørsmålet er nei, den nasjonale reguleringen er ikke god nok. Videre i avslutningen skal jeg komme med et forslag til hvordan reguleringen av biometriske personopplysninger i nasjonal rett kan være utformet, utfra hvilke vilkår en slik bestemmelse bør oppfylle, og med de poengene jeg har gjort rede for i avhandlingen.

6.2 Hvordan bør den nasjonale reguleringen av biometriske personopplysninger være utformet?

6.2.1 Foreligger det et behov for en nasjonal regulering av biometriske personopplysninger?

At den nasjonale bestemmelsen ikke fungerer godt nok i dag, trenger dog ikke være ensbetydende med at man *trenger* en nasjonal regulering av biometriske personopplysninger.

I forarbeidene til personopplysningsloven av 2018 ble det fra flere av høringsinstansene påstått at det ikke foreligger et behov for å videreføre en nasjonal regulering av biometriske personopplysninger.[139]

Det til nå åpenbart sterkeste argumentet slik det fremkommer fra høringsinstansene, og som jeg også har gjort rede for i avhandlingen, er at det allerede foreligger en ganske snever adgang for behandling av biometriske personopplysninger. Biometriske personopplysninger, som en særlig kategori av personopplysninger, nyter således et tilstrekkelig og godt vern gjennom personvernforordningen, og ikke trenger en regulering i nasjonal rett.

Etter det jeg har vært gjennom, og med det poenget jeg trakk frem ovenfor, mener jeg likevel vi trenger en nasjonal regulering av biometriske personopplysninger, og at den bestemmelsen

[139] Jfr. Prop. 56 LS (2017-2018) s. 54.

vi har nå, ikke er tilstrekkelig. Dette underbygges jo også av at det i forarbeidene, tross motstand, ble konkludert med at man ønsket en regulering av biometriske personopplysninger.[140]

6.2.2 Hvordan bør en eventuell nasjonal regulering av biometriske personopplysninger se ut?

Ved utarbeidelsen av en nasjonal regulering til biometriske personopplysninger er det særlig to ting jeg mener man bør være bevisst på. For det første tror jeg man er best tjent dersom man prøver å sørge for at ordlyden i den nasjonale bestemmelsen har en ordlyd som samsvarer med ordlyden i personvernforordningen. På den måten sørger man for en lov som er lettere å anvende i samsvar med personvernforordningen. Men for å sørge for et konsistent lovverk bør man også sørge for at bestemmelsen er i samsvar med resten av personopplysningsloven. For det andre bør man, i likhet med personvernforordningen, søke å innføre en bestemmelse med en ordlyd som er teknologinøytral, for å sørge for en dynamisk utvikling. Med en teknologinøytral ordlyd kan man også unngå at tilfeller som bør reguleres under bestemmelsen faller utenfor.

Vi kan begynne med å ta utgangspunkt i hvordan biometriske personopplysninger reguleres per dags dato. Pol. § 12 lyder: «Fødselsnummer og andre entydige identifikasjonsmidler kan bare behandles når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering».

Nåværende pol. § 12 oppstiller to skjønnsmessige vilkår, «saklig behov» og «nødvendig for å oppnå slik identifisering». Som nevnt tidligere er biometriske personopplysninger et dynamisk begrep, som kan utvikle seg. Da bør man også holde muligheten for bruk åpen for utvikling. Jeg tenker at det er en god ide å videreføre disse vilkårene, fordi man på en slik måte passer på at behandlingen ikke avgrenser mot tilfeller som bør falle innenfor ordlyden. I tillegg åpner for at man til hvert tilfelle konkret kan vurdere hvordan behovet for behandling av biometriske personopplysninger er. Med tanke på den risikoen som kan foreligge ved behandling av biometriske personopplysninger, tenker jeg det er hensiktsmessig å kreve at det

[140] Se Prop. 56 LS (2017-2018) s. 56.

foretas en konkret vurdering av om det foreligger et «saklig behov», og metoden er «nødvendig».

Det første jeg mener man bør gjøre er å skille ut biometriske personopplysninger fra ordlyden «entydige identifikasjonsmidler» i pol. § 12. Et eksempel hadde vært å innføre ordlyden «biometriske personopplysninger» i pol. § 12. For eksempel slik:

«Fødselsnummer, andre entydige identifikasjonsmidler og biometriske personopplysninger kan bare behandles når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering».

Med en slik formuleringer får man for det første gjort det helt klart at biometriske personopplysninger skal falle innenfor ordlyden. På denne måten fjerner man også til en viss grad utfordringene som forelå ved koblingen mellom fødselsnummer og øvrige identifikasjonsnummer og biometriske personopplysninger, fordi det ikke forutsettes at biometriske personopplysninger anvendes på samme måte som fødselsnummer.

På samme tid vil en slik ordlyd fortsatt forutsette en bruk som har med identifisering å gjøre, gjennom ordlyden «saklig behov for *sikker identifisering*» og «oppnå slik *identifisering*». Jeg mener, etter det jeg har sett på i avhandlingen, at man må tolke ordlyden utvidende, slik at autentisering faller innenfor ordlyden.[141] For at man skal samsvare med innholdet i personvernforordningen er det mulig det burde unngå en nasjonal bestemmelse som bare viser til «identifisering» fordi det avgrenser mot autentisering. Dermed kan det være lurt å innføre ordlyden «autentisering».

I art. 4 nr. 14 brukes dog ordlyden «identifisering». Autentisering er ikke nevnt. Med tanke på at man gjerne ønsker at det skal være samsvar mellom ordlyden i personvernforordningen og personopplysningsloven, er det mulig man burde holde seg til ordlyden «identifisering», men da med den forutsetning at man tolker ordlyden utvidende slik at autentisering også faller innenfor.

Det vil dog være noe bakoverlent å vedta en ordlyd slik at den skal passe til en forordning som muligens ikke gir uttrykk for gjeldende rett, ved at man skal innfortolke autentisering i

---

[141] Se pkt. 3.1.3 i avhandlingen.

en ordlyd som ikke favner om det. Jeg tror også vi uansett vil være best tjent med å, der det er mulig, ha en ordlyd som er klarest mulig. Om det er tilfellet at ordlyden ikke skal tolkes utvidende slik at autentisering faller innenfor, er det heller ikke noe i veien for at man nasjonalt vedtar en bestemmelse som regulerer autentisering og. Det følger av personvernforordningen art. 9 nr. 4 medlemsstatene kan innføre «ytterligere vilkår, herunder begrensinger, med hensyn til behandling av … biometriske personopplysninger …». At det kan innføres ytterligere begrensninger medfører at det i nasjonal rett kan innføres en regulering av autentisering.

På bakgrunn av det jeg har nevnt ovenfor, foreslår jeg at biometriske personopplysninger løses ut til en egen bestemmelse i personopplysningsloven med følgende ordlyd:

§xx Behandling av biometriske personopplysninger

«Biometriske personopplysninger kan bare behandles der det foreligger et saklig behov for autentisering eller sikker identifisering, og metoden er nødvendig for å oppnå slik autentisering eller identifisering».

Kildeliste

Norske lover

Lov 17 mai 1814 Kongeriket Norges Grunnlov (Grl.)

Lov 14 mars 2000 nr. 31 om behandling av personopplysninger (opphevet ved lov 15 juni 2018)

Lov 17 juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven)

Lov 15 juni 2018 om behandling av personopplysninger (pol.)

Internasjonale lover og avtaler

Treaty on the Functioning of the European Union, 25 mars 1957, Roma (traktat om den europeiske unions virkemåte, TEUV)

Vienna Convention on the Law of Treaties, 23 mai 1969, Wien (Wien-konvensjonen)

The Agreement on the European Economic Area, 2 mai 1992, Porto (avtale om det europeiske økonomiske samarbeidsområde, EØS-avtalen)

Europaparlamentets- og rådsdirektiv (EF) 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personverndirektivet)

Europaparlamentet og Rådets forordning 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (personvernforordningen)

Norske forarbeider og utredninger

Ot.prp. nr. 92 (1998–1999) om lov om behandling av personopplysninger (personopplysningsloven)

Ot.prp. nr. 51 (2004-2005) om lov om mekling og rettergang i sivile tvister (tvisteloven)

Dag Wiese Schartum og Lee A. Bygrave, *Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12*,

Justis- og politidepartementet, (2008) (lest 09.12.2021) https://www.regjeringen.no/contentassets/daad3dbe61c74f5c9240d16478b088ba/g-0406.pdf

NOU 2009: 1 Individ og integritet: Personvern i det digitale samfunnet

Prop. 56 LS (2017-2018) lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen

Internasjonale veiledere og utredninger

Artikkel 29 – Gruppen vedrørende datasikkerhet, *Arbejdsdokument om biometri*, (2003), (lest 08.12.2021) hentet fra https://danishbiometrics.files.wordpress.com/2009/08/wp80_da.pdf

Personvernrådet, *Guidelines 3/2019 on processing of personal data through video,* edpb.europa.eu, (2019) (lest 11.11.2021) hentet fra https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

Tambiama Madiega og Hendrik Mildebrath, *Regulating facial recognition in the EU,* europarl.europa.eu, (2021) (lest 09.10.2021) hentet fra https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

Christiane Wenderhorst og Yannic Duller, *Biometric recognition and behavioural detection: assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces,* europar.europa.eu, (2021) (lest 09.10.2021) https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/697131/IPOL_BRI(2021)697131_EN.pdf

Rettspraksis fra Høyesterett, EFTA-domstolen og EU-domstolen

Rt. 1995 s. 54 A

E-7/97 Erla María Sveinbjörnsdóttir mot Island, (*Sveinbjørnsdottir)* [rådgivende uttalelse]

Rt. 2001 s. 428 A

Rt. 2002 s. 1500 U

Rt. 2004 s. 878 U

Rt. 2012 s. 1669 A

Rt. 2013 s. 143 (Avfallsservice) A

Dom 19. oktober 2016 [C5] *Breyer*, C-582/14, ECLI:EU:C:2016:779

HR-2021-966-A

HR-2021-2403-A

Forvaltningspraksis

PVN-2006-7 Tysvær kommune – fingeravtrykkspålogging

PVN-2006-8 Oxigeno Fitness – fingeravtrykk ved adgangskontroll

PVN-2006-9 Oslo trimsenter – fingeravtrykk ved adgangskontroll

PVN-2006-10 Esso Norge AS – fingeravtrykk ved adgangskontroll

PVN-2006-11 REMA 1000 – fingeravtrykk ved registrering av timer

PVN-2011-11 Visma Retail

PVN-2011-12 Adgangskontroll ubetjent treningssenter

20/01627-3 Vedtak om overtredelsesgebyr – Direktesending fra kameraovervåking fra offentlig område, datatilsynet.no (lest 09.12.2021) https://www.datatilsynet.no/contentassets/bb8618c1ce604468b3b478676bf196c5/vedtak-om-overtredelsesgebyr---dragefossen-as.pdf

20/02181-3 Vedtak om overtredelsesgebyr - Bergen kommune - Melding om avvik i Vigilo, datatilsynet.no (lest 09.12.2021) https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2020/endeleg-vedtak-om-gebyr-til-bergen-kommune/

20/03046-11 Varsel om vedtak om overtredelsesgebyr – TRUMF AS, datatilsynet.no (lest 10.12.2021)

https://www.datatilsynet.no/contentassets/1223c2b345334738b58ba46c7570346b/varsel-om-vedtak---trumf.pdf

Litteratur

Jarbekk, Eva, *Karnov lovkommentar: Personopplysningsloven 2018, Lovkommentar 1 til GDPR art. 4 1. ledd nr. 1*, lovdata.no (lest 01.12.2021)

Nasjonalt ID-senter, *Biometri og identitet: utfordringer og nye muligheter i utlendingsforvaltningen,* nidsenter.no (lest 08.12.2021) hentet fra https://www.nidsenter.no/globalassets/dokumenter/publikasjoner/nid-rapporter/rapport_biometri.pdf

Schartum, Dag Wiese, *Personvernforordningen – en lærebok,* 1.utg., Fagbokforlaget 2020

Sejersted, Fredrik, Finn Arnesen, Ole-Andreas Rognstad og Olav Kolstad, *EØS-rett,* 3. utg., Universitetsforlaget 2011

Skoghøy, Jens. Edvin A., *Rett og rettsanvendelse,* 1.utg., Universitetsforlaget 2018

Kilder hentet fra nett

Almås, Gry Blekstad, *Digitalt diktatur: Kina planlegger sosialt poengsystem,* nrk.no (lest 08.12.2021) https://www.nrk.no/urix/kinas-digitale-diktatur_-gar-du-pa-rodt-lys_-blir-du-uthengt-pa-storskjerm-1.14369439

Boe, Erik Magnus, *Legaldefinisjon,* snl.no (lest 05.10.2021) https://snl.no/legaldefinisjon

Datatilsynet, *Biometri,* datatilsynet.no (lest 11.10.2021) https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/

Datatilsynet, *Fødselsnummer,* datatilsynet.no (lest 04.09.2021) https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/fodselsnummer/

Nätt, Tom Heine, *Biometrisk autentisering,* snl.no (lest 11.10.2021) https://snl.no/biometrisk_autentisering

Skatteetaten, *D-nummer,* skatteetaten.no (lest 07.09.2021) https://www.skatteetaten.no/person/utenlandsk/norsk-identitetsnummer/d-nummer/

Skodvin, Knut Einar, *Dualisme*, snl.no (lest 30.08.2021) https://snl.no/dualisme_-_jus

Tillman, Maggie, *Amazon Go and Amazon Fresh: How the 'Just walk out' tech works,* pocket-lint.com (lest 10.09.2021) https://www.pocket-lint.com/gadgets/news/amazon/139650-what-is-amazon-go-where-is-it-and-how-does-it-work

Tranberg, Charlotte Bagger, *Persondata og biometri i Skandinavien*, lovdata.no (lest 13.09.2021) https://lovdata.no/pro/#document/LOD/lod-2007-090-1/KAPITTEL_1-1

Utenriksdepartementet, *Folkerett*, regjeringen.no (lest 14.11.2021) https://www.regjeringen.no/no/tema/utenrikssaker/folkerett/folkerett/id2076280/

Wikipedia, *IP-adresse*, wikipedia.no (lest 10.12.2021) https://no.wikipedia.org/wiki/IP-adresse